ournal of Philosophy, Policy and Strategic Studies, Vol. 1, No. 4 (2025)
ISSN: 1595 - 9457 (Online); 3043 - 4211 (Print)
Website: https://jppssuniuyo.com **Email:** jppssuniuyo@gmail.com
Received: April 14, 2025 **Accepted**: May 14, 2025 **Published**: June 30, 2025
Citation: Elekwachi, Chioma; Aliede, Jonathan E. & Orebiyi Taiwo P. (2025). "Radio as an Instrument for Creating Awareness on Cybersecurity and Crime Prevention among Nigerian Youths". *Journal of Philosophy, Policy and Strategic Studies*, 1 (4): 36-46.

Article **Open Access**

RADIO AS AN INSTRUMENT FOR CREATING AWARENESS ON CYBERSECURITY AND CRIME PREVENTION AMONG NIGERIAN YOUTHS

Chioma Elekwachi [1]
Jonathan E. Aliede [2]
Taiwo Philip Orebiyi [3]
Department of Peace and Conflict Resolution, National Open University of Nigeria [1 & 3]
Department of Mass Communication, National Open University of Nigeria [2]
Corresponding Email: chiomaelekwachi@gmail.com

Abstract

Cybersecurity threats are a growing concern in Nigeria, particularly among the youth, who are the most active users of digital technology. Radio, as a powerful and widely accessible medium, plays a critical role in raising awareness and educating the public on cybersecurity's best practices and crime prevention among the youth in Nigeria. These functions lean on the theory of social responsibility. This study examines the role of radio in promoting cybersecurity awareness among Nigerian youths, with a focus on Kapital FM (Radio Nigeria), Abuja. It highlights the current state of radio stations in supporting awareness, and its impact is fostering a culture of online morals and safety. Using a qualitative approach, data were gathered through a literature review and interviews with media officers at the radio station. The findings reveal that while radio is a powerful tool for public awareness, there is inadequate cybersecurity-related content on KFM Abuja, limiting its effectiveness in educating youths on cyber threats and preventive measures. This gap suggests a need for deliberate efforts to integrate cybersecurity programmes into radio broadcasts. The study recommended strategies for improving the effects of radio, which include, development of targeted content that addresses the growing challenges of cybercrime among Nigerian youths, and enhanced collaboration between radio stations, security agencies, cybersecurity experts, policymakers and educational institutions. By leveraging radio's reach and influence, the youths can be empowered to mitigate cybersecurity risks and reduce criminal activities in the digital space and by so doing, contribute to a safer online environment in Nigeria.

Keywords: Crime, Cybersecurity, Cyber threats, Radio, Youths.

Introduction

In today's world, the rapid growth of digital technologies has transformed how people work, live, and interact. However, this connectivity has also exposed individuals, especially youth, to various cyber threats and activities. Criminal activities such as cybercrime, online harassment, identity theft, credit card fraud, hacking, cyberbullying, cyberterrorism, and phishing are becoming increasingly prevalent, compromising the safety and security of Nigerian youth online.

Technology's rapid advancement has also transformed how information is disseminated, with every medium playing a focal role in shaping public awareness. In Nigeria, where access to the Internet may be a double-edged sword among the youth, radio remains a vital source of information for bridging the digital divide and fostering communication. This article delves into the important role of radio in enhancing cybersecurity awareness among Nigerian youths, who are increasingly vulnerable to cyber threats and also perpetrators of these crimes. By examining the effectiveness of radio programs in disseminating critical information about online safety, considering its wide reach, the study highlights the potential of this traditional medium to educate and empower a generation that traverses both digital and real-world challenges.

Makeri (2017) noted that cybercrimes have evoked mixed feelings of admiration and fear among people, especially the young ones, with a growing unease about cyber and personal security. Makeri asserted that Nigeria, among other countries, has acquired notoriety in internet-related criminal activities. For example, *The Punch* (2025) reported that the Police Special Fraud Unit, Lagos, arrested 14 persons, including four National Youth Service Corps members and eight students from Gateway Polytechnic, Sapaade, aged 18-28 years, for alleged involvement in Internet fraud across Lagos and Ogun states. Arum (2021) examined the role of the telecommunication sector in curbing hacking and cybersecurity, which affect a nation's lives, economy, and international reputation. Similarly, Ottah and Okpoko (2019) examined the collaboration of policymakers and the media to address national security. The Nigerian government has recently implemented various initiatives to promote cybersecurity awareness. However, these efforts have been largely focused on the formal education sector, leaving a significant gap in awareness among out-of-school youth and those in rural areas. There is a gap in the literature on exploring the role of radio in enhancing cybersecurity and crime prevention awareness among youths who are not exposed to education. To fill this gap, the study, therefore, conducted a review, relying on secondary data and interviews of a few officers in a media organisation – Kapital FM (Radio Nigeria), Abuja.

The study's objectives examine the current state of radio-based cybersecurity awareness initiatives, their impact, and potential strategies for improvement. This study aims to contribute to the existing body of knowledge on cybersecurity awareness and radio-based awareness initiatives. Its findings may also provide valuable insights for policymakers, educators, and non-governmental organisations, practitioners seeking to promote cybersecurity awareness among Nigerian youth.

Conceptualising Cybersecurity

Nwachukwu (2021) defines cybersecurity as the collection of policies, security concepts, tools, security safeguards, risk management approaches, guidelines, actions, best practices, training, assurance, and technologies that can be used to protect the cyber environment, organisation, and users' assets. Organisation and user assets include connected computing devices, personnel, applications, infrastructure, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. According to Hang & Coppel (2020), cybersecurity is the practice of protecting systems, networks, devices, and data for digital data from digital attacks, theft, damage, and unauthourised access. It involves implementing technologies, processes, and controls to ensure the confidentiality, integrity, and availability of information in the data space. Due to the nation's security, the issue of cybersecurity has recently caught the attention of some scholars.

In the article Hacking and Cybersecurity in Nigeria Telecommunication Industry: Implication for Teaching and Learning (Arum, 2021), the Internet was defined as a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of networks consisting of millions of private, public, academic, business, and government networks, of local to global scope, that is linked by a broad set of computer memory units, arranged in lines across electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the interlinked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

Youths are digital natives, growing up with the internet and mobile devices, making them more likely to be online and vulnerable to cyber threats. The youth has been defined in varying ways. The United Nations Population Fund defined youth as a period of transition from dependence of childhood to adulthood's independence. According to Uzoma, Bello and Falade (2016), the Nigeria Policy on Youth Development of 2009 considers youth to be persons between 18 and 35 years. The youths are individuals in the period of experimenting with roles and identities without the burden of social norms and responsibility. (Uzoma, *et al,* 2016). The youths spend a significant amount of time online, which makes them more susceptible to cyberbullying, online harassment, and other cyber threats. On the other hand, these youths are increasingly involved in cybercrimes, driven by greed, laziness, the quest for fast money, unemployment, and socio-economic challenges. Young individuals often exploit the anonymity of the internet to commit various offences like fraud and hacking (Ebelogu, Ojo, Andeh & Agu, 2019).

Cybercrime

Cybercrime is a series of organised crimes aimed at attacking cyberspace and cybersecurity. As computers became more widespread in the 1960s and 1970s, the first instances of computer hacking began to emerge. Baase (2013) notes that in 1971, a programmer named John Draper discovered a way to make free phone calls using a whistle that emitted a tone at the same frequency as a phone operator's dialling signal. The arrest of a German spy by West Germany's police in 1968 was acknowledged as the first case of cyber espionage (Warner, 2012). By the 1980s, cybercrime began to take a more malicious tone, with the emergence of computer viruses, worms and other forms of malware (Kizza, 2019). At the same time, individual criminals actively hacked data, targeting critical national infrastructures and financial organisations to steal money and sabotage (Mordi, 2019; Kshetri, 2019).

In the 1990s, Nigeria joined other countries that faced cyber threats, and by 2003, former President Olusegun Obasanjo instituted the National Cyber Security Initiative to address the menace. The Nigeria Cybercrime Act was passed into law in 2015 to prohibit and prevent cybercrime in Nigeria. The act aims to provide an effective and unified legal framework for the prohibition, prevention, detection, prosecution, and punishment of crimes in cyberspace in Nigeria (Nigeria Cybercrime Act, 2015). The Nigerian Communications Commission (NCC), the Economic and Financial Crimes Commission (EFCC), and the Nigeria Police Force (NPF) are some of the organisations that prevent, detect and punish crimes in Nigeria. In 2024, the NCC reported over 219 million active mobile lines with about 134.27 million active mobile internet subscriptions. This shows the number of persons exposed to cyber threats. Cybercrime is complex and committed mostly from remote locations, making it difficult for the police to catch. Internet crimes occur daily, with victims showing naivety and gullibility when interacting with these fraudsters. Some of the risks young people face in cyberspace or engage in against their victims include:

Advanced Fee Fraud (419 or Yahoo-Yahoo): This is the most common type of cybercrime committed by youths in Nigeria. It involves tricking victims into paying upfront for non-existent services or goods, often facilitated through social media platforms like email, Facebook, WhatsApp (Udelue & Bentina, 2019).

Phishing: The National Cyber Security Centre (2020) described phishing as when a criminal attempts to trick people into doing the wrong thing, like clicking a link to a dodgy website. Phishing can be conducted through text messages, social media, or phone, but the term 'phishing' is mainly used to describe attacks that arrive by email. Some phishing emails may contain viruses disguised as harmless that become activated when opened.

Malware: Malware, according to Oyeyemi (2021), is a contraction of malicious software designed to destroy or exploit computer systems and programs. It has many forms such as viruses, worms, Trojans and spyware.

Identity Theft: This involves theft of an individual's personal information, such as a name, address and social security number, intending to use it for fraudulent activities like opening bank accounts, taking out loans or making purchases (Udelue & Bentina, 2019).

Hacking: This is an unauthorised access to computer systems or networks to steal data, disrupt operation or cause damage. According to Obinagwa, Ngoka, Uwaechia, Ezugwu, Okpala and Ayadiuno (2023), hacking is the process of attempting to gain or successfully gaining unauthorised access to computer resources. A hacker is a person who finds and exploits weaknesses in computer systems to gain access. They are classified into ethical hackers, crackers, and grey hats.

Cyberstalking: Oyeyemi (2021) views cyberstalking as involving the use of the internet or other electronic communication tools to harass, intimidate or threaten an individual. Though cyberstalking is a broad term for online harassment, it can include defamation, false accusations, teasing, and even extreme threats.

Cyberbullying: This involves the use of the internet or other electronic communication tools to bully, harass or humiliate an individual (Obinagwa *et al*., 2023).

Online Fraud: Obinagwa *et al* (2023) see online fraud to include various types of fraud carried out online. They could be investment scams, lottery scams, romance scams, etc.

Cyberterrorism: Cyberterrorism is a convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers and networks, and the information stored in them, to intimidate or coerce a government and its people into a political or social objective. Oyeyemi (2021) includes cyberterrorism as a type of cybercrime that occurs in Nigeria and involves the use of technology to carry out terrorist activities or spread terror and fear among people.

Causes and Effects of Cybercrime: Sheer curiosity, mischief, greed, laziness, corruption, poverty, internet porosity, unemployment, and ineffective laws on cybercrime can be seen as factors that motivate people to commit crime-related activities. The speed and power of modern information technology complicate the detection and investigation of computer crimes. For example, communications networks now span the globe, and a small personal computer can easily connect to sites located in different hemispheres or continents. Unfortunately, cybercrimes expose the vulnerability of information and communication technology, reduce productivity, and cause loss of funds, loss of national reputation, terrorism, and threats to national security (Ebelogu *et al*., 2019).

Cybersecurity Awareness

According to Blackwood-Brown (2018), cybersecurity awareness is educating internet users about cybersecurity issues, benefits, threats and attacks that can jeopardise their activities on the web, mitigate against the attack and prevent unauthorised users. In other words, cybersecurity awareness refers to the knowledge and understanding of potential cyber threats and the best practices to mitigate them. Aliede (2015) found out that students' use of information and communication technologies in their studies also comes with inadequate digital literacy and negative application by unscrupulous users. The necessity of cybersecurity awareness among Nigerian youths has become increasingly important due to the proliferation of online activities and the corresponding rise in cyber threats. As digital technologies transform communication and commerce, they also expose users to various cybercrimes, such as fraud, theft, and harassment, thereby necessitating robust education on cybersecurity (Ray, 2014). In Nigeria, the growing engagement of the youth on social media platforms and electronic commerce sites amplifies the role of awareness in safeguarding their digital lives. Makeri (2017) and Bouraff & Hui (2024) assert that these risks not only challenge individuals but also jeopardise broader societal structures through the malicious misuse of information communication technologies. However, the youths may not be fully aware of the potential cyber threats and the measures to prevent them. Youths may engage in risk-taking behaviour online, such as sharing sensitive information or clicking on suspicious links. They may also be more vulnerable to social engineering tactics like phishing or online scams.

It is therefore pertinent to empower young individuals to navigate these threats through fostering a culture of cybersecurity awareness. This educational initiative can be achieved through radio, which can reach and promote essential strategies for digital safety among the youth. The awareness can help individuals protect their sensitive data from being breached or compromised. It can also prevent financial fraud and protect sensitive financial information. Cybersecurity awareness is essential for national security as it helps prevent cyberattacks that can compromise critical infrastructure, development and economy (Erondu & Erondu, 2023).

The History and Evolution of Radio as a Medium of Communication in Nigeria

The media is generally regarded as the fourth estate of the realm, with the executive, the legislature and the judiciary as the three other estates (Ibrahim & Jamri, 2022). Radio is a traditional medium that uses electromagnetic waves to transmit audio content to listeners. Radio was invented in the late 19th century by Guglielmo Marconi, and by the 1920s, it became a staple of modern life, with millions of people tuning in to listen to news, music, and dramas. Radio's influence extended beyond entertainment, as it played a critical role in disseminating news and information during war and crisis. All through the 20th century, radio continued to evolve and adapt to changing technological and societal trends. The rise of FM radio in the 1960s and 1970s brought better sound quality and more diverse programming, and in the 1980s and 1990s, an era of interactive and opinion-driven content was enabled. Radio, as a mass medium, is saddled with the responsibility of protecting public interest, creating public awareness, and serving as the intermediary between the government and the people. In essence, radio has an all-embracing role of possibly senitising people against possible injustice, oppression and misdeeds in society (Chirunga & Mbwirire, 2020). Radio is regarded as the most powerful mass medium due to its penetrative, propagative, persuasive and socialising nature.

The evolution of radio in Nigeria is intricately linked to the socio-political landscape of the nation, serving as both a communication tool and a cultural artefact. According to Adeeko (2023), radio broadcasting in Nigeria began in the 1930s, profoundly influencing the dissemination of information and shaping public opinion. This medium became particularly significant during the struggle for independence, as it provided a platform for national discourse and unity. As the digital age emerged, the radio landscape transformed, adapting to contemporary issues such as cybersecurity. This evolution is crucial in understanding how radio can enhance cybersecurity awareness among Nigerian youths, who are increasingly vulnerable to online threats.

How, then, do radio stations function in cybersecurity awareness? Education and media are considered to be more structural and feasible actions for cybersecurity awareness, far better and easier to manage than other complex agents of information. Montasari (2024) notes that the educational goals of radio and information literacy in responding to cyberspace unfold in a three-pronged process: information, analysis and action. Information seeks to raise awareness about cybersecurity and its consequences, convey and disseminate information about it and communicate the relevant legal frameworks to deal with it. Analysis entails identifying and assessing cybersecurity, analysing common causes and underlying assumptions, recognising tricks and reporting and exposing cybercrimes. Action capacitates the individual to respond to cybersecurity, change the discourse on crimes, and monitor the radio on cybersecurity awareness. Radio stations have the potential to educate the public by focusing on their reach and accessibility (Heywood, 2020).

Radio's pervasive influence as a medium of disseminating information cannot be overemphasised, especially in the context of enhancing cybersecurity awareness among Nigerian youths. Despite the growth in new communication media, such as social media platforms, radio remains the most important communication tool to reach large segments of the population in Nigeria (Aondover, Okuneye & Onyejelem, 2024). Given the high penetration of radio, this platform can effectively reach diverse demographics, educating them about the complexities of cyber threats and preventive measures. For example, radio programmes that incorporate discussions on current trends in cybercrimes can significantly demystify the behaviours and motivations of offenders. Moreover, the interactive nature of radio allows the audience to engage with experts and provide feedback, thereby fostering a participatory environment for knowledge sharing. As demonstrated via various initiatives, radio broadcasts that focus on cybersecurity issues can bridge the gap in technological literacy, equipping youth with the skills necessary to navigate the digital landscape safely and responsibly (Upadhyaya, 2024). Furthermore, by employing engaging narratives and expert commentary, these programs can demystify complex cybersecurity concepts and promote best practices among young listeners. The interactive nature of radio facilitates community engagement, fostering discussions that reinforce learning and collective responsibility in cybersecurity. Ultimately, the strategic use of radio can catalyse a broader cultural shift towards proactive cybersecurity practices.

The study of communication and mass media has led to the formulation of many theoretical frameworks and methodologies. McQuail (2005) notes that Social Responsibility Theory is one of the normative theories of the media, which was postulated by F.S. Siebert, T.B. Peterson and W. Schramm in 1956. The theory goes beyond "objective" reporting to interpretive reporting; and calls for responsibility more than freedom on the part of the media. In following the principles of social responsibility, radio broadcasting has a public mandate to inform, educate, and entertain, which aligns with the principles of social responsibility.

Case Study of Kapital FM (Radio Nigeria), Abuja

Radio Nigeria, officially called Federal Radio Corporation of Nigeria (FRCN) is a government-owned broadcast institution that is headquartered in Abuja, and has a network of 36 FM stations across the nation, with six Zonal Stations in Kaduna, Enugu, Ibadan, Bauchi (North-East Zone), Port-Harcourt (South-South Zone) and Lafia (North-Central Zone) as well as two Operations in Lagos and Abuja. Radio was owned, controlled, and fully government-funded until the deregulation and commercialisation of broadcast media in Nigeria in 1996. The various stations of Radio Nigeria have a format of radio programme production that provides information, education, and entertainment to their audience. Radio Nigeria, as a public service organisation has the mandate to provide impartial radio broadcasting services within Nigeria to inform, educate, and entertain the public through up-to-date and well-researched news and programmes. Its key mandate by the law setting is to ensure that the services it provides, when considered as a whole, shall reflect the unity of Nigeria as a federation, and at the same time, give adequate expression to the culture, characteristics, affairs, and opinions of each part of the federation. Thus, its slogan, "Uplifting the People and Uniting the Nation". Radio Nigeria strives to balance divergent opinions. This means that in a given discourse, it is expected that every individual concerned is given space to air their opinions (www.radionigeria.gov.ng). Considering that the study cannot cover all the FM stations of Radio Nigeria within the given period, Kapital FM Abuja is chosen as a case study. KFM was established as an urban-based FM station in 2002 to cater for the upward residents of the Federal Capital Territory. KFM became the second station of the Radio Nigeria family, streaming on a frequency of 92.9.

Current State of Cybersecurity and Crime Prevention Awareness on Radio

In an interview with one of the Presenters of KFM, Participant 1 said:

> We have a 30-minute programme called City Watch that discusses matters of security, any kind of security, be it land, sea, internet, and so on. It is broadcast in English every Thursday at 6:30 pm. There is no particular time scheduled for cybersecurity because various topics around security are discussed depending on the availability of experts. Our stations in the zones have similar programmes across the country.

Going by the participant's response, there is no regular or scheduled topic on cybersecurity awareness. The lack of regular cybersecurity awareness discussions on the radio program may indicate a limited focus on this critical issue. The response provides insight into the current state of radio-based programmes on cybersecurity and crime prevention, specifically highlighting the inconsistent coverage of cybersecurity awareness, contributing to a lack of public awareness and education on the issue. (Kur, Melladu, Agodosy & Orhewere*,* 2013) asserted that community radio projects can foster engagement and promote discussions around security issues, which in turn empower youths to navigate the digital landscape safely. This multifaceted approach is vital for building a resilient cyber-conscious generation in Nigeria.

Radio's Challenges of Delivering Education on Cybersecurity and Crime Prevention

In another conversation with a Producer, Participant 2 revealed that:

> City Watch is a security awareness programme that educates and informs our listeners how to be security conscious and be well informed about what is going on in the security space in our country. Cybersecurity is very important, but not discussed too often on City Watch. It crops up at any time security is discussed, but going forward, its broadness will be looked at. Knowing that the

> youths need to be educated to prevent getting engaged in cybercrimes and being hacked, there will be more awareness, starting from every quarter. The fear is that there may not be enough materials to run cybersecurity as a programme, which can lead to repetition of topics. Sponsorship is needed to support a programme like this.

Radio seems not to be effective in discussing cybersecurity due to various challenges. The literature by Hawkridge and Robinson (2023) suggested that radio has inadequate funding to produce consistent and high-quality educational content, which corroborated with the response of Participant 2. The response highlighted a significant challenge in radio broadcasting for promoting cybersecurity awareness: perceived lack of content. Sustaining a programme with adequate content exposes a broader issue in the radio broadcasting industry, where stations struggle to create engaging and informative content on cybersecurity awareness. This challenge, therefore limits their ability to effectively promote awareness.

Implications of a Lack of Radio's Awareness on Cybersecurity

In an interaction with a good number of students for Industrial Work Experience Scheme (SIWES) in the News Room, a 300-level student of Mass Communication at Nasarawa University, Keffi (Participant 3) observes that:

> Since I have been on Industrial Attachment for about two months. I have not
> heard of any programme on cybersecurity. That does not mean that I do not
> know anything about Internet activities. I know my mates who do yahoo-yahoo.
> And I know it is wrong. I can tell when someone wants to swindle me because
> I read about other people's ordeals through social media. So, by God's grace,
> I will not commit or be a victim of cybercrime.

The student's response shows a lack of awareness of cybersecurity and crime prevention through radio, indicating a lack of exposure to the issue among Nigerian youths, leading to reliance on alternatives such as social media integrations or peer-led discussions. The student's statement reveals a knowledge gap in cybersecurity awareness, which is not being addressed through traditional radio broadcasting. This highlights the potential consequences of radio stations' lack of engagement in this area, such as youths may not be fully aware of the potential cyber threats and the measures to prevent them. This gap affects even more those youths in the rural areas who do not have access to the Internet or those who are out of school.

The Way Forward

The literature underscores the critical role of radio in creating awareness about cybersecurity and crime prevention among youths. However, findings from interviews with media officers at KFM (Radio Nigeria), Abuja, revealed a gap in cybersecurity-related content. This suggests a disconnect between the potential of radio as highlighted in the literature and its actual implementation. This aligns with previous studies indicating that while radio is a powerful tool for information dissemination, limited specialised programming on cybersecurity hinders its effectiveness in raising awareness. The lack of adequate content at KFM Abuja reflects broader challenges identified in the literature, such as insufficient media prioritisation of cybersecurity issues and a lack of targeted programming for young audiences. The study, therefore, proposes the following recommendations as potential strategies for improvement:

Creation of dedicated cybersecurity radio shows/jingles: Radio stations should understand the importance of improving education on cybersecurity to enable them to develop a program to address it. Radio stations could benefit from exploring innovative formats, sponsorship and collaborations with relevant organisations to enhance their cybersecurity awareness initiatives. A dedicated program to be aired once a week could be created, and with time, could become participatory where young ones share their idea on cyber issues.

Full engagement of young people: The youth represent the next generation, and therefore need credible and up-to-date information on cybersecurity. Duchi and Orebiyi (2024) agreed that the lack of educational access to the growing number of young people presents a crisis, calling for effective and efficient actions. Radio should therefore incorporate social media elements such as live tweets and Instagram stories, to extend the reach and youth's engagement in cybersecurity awareness. Host interactive programmes, such as call-in shows, quizzes, or games, should be initiated to educate and engage the youths and other diverse listeners. This will go a long way in raising awareness and promoting safe online behaviours.

Training: Radio stations should provide training and workshops for radio staff and presenters on cybersecurity awareness to ensure they can effectively communicate complex information.

Conclusion

The few lessons arising from the engagement with radio's role in cybersecurity awareness and crime prevention are significant and instructive. The discussion acknowledges that radio, with its wide range, can help to educate a large audience, particularly Nigerian youths, on issues concerning cybersecurity. Youths can benefit from cybersecurity education and awareness programs that teach them about online safety and security best practices. However, the study shows a limited awareness of cybersecurity awareness among youths due to a lack and limited of content in the programme, and a lack of sponsorship and staff training. The convergence of evidence underscores the relevance and validity of the research objectives within the context of the study. Documenting the findings and recommendations of the study serves as a possible model for radio stations and relevant stakeholders like the NCC, EFCC, the NPF, Non-profits, and educational institutions, to create a call-in segment to enhance cybersecurity education.

References

Adeeko, T. I. (2023). *Nigerian Media: A Comparative Media Analysis*, Master's thesis, Northern Illinois University.

Adenike, O., & Raliat, A. (2023). Awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria. *Journal of Library Services and Technologies,* 5(3), 90-104. DOI: http://doi.org/10.47524/jlst.v5i3.91

Aliede, J. E. (2015). Challenges and prospects of information and communication technologies application among mass communication students of tertiary institutions in Lagos, Nigeria, *New Media and Mass Communication, 39*. IISTE, 86-106

Aondover, E. M., Okuneye, A. P., & Onyejelem, T. E. (2024). Application of new media in peace building and conflict resolution in Nigeria. *Journal of African Conflicts and Peace Studies*, 6(1), 8.

Arum, B. U. (2021). Hacking and cybersecurity in Nigeria's telecommunication industry: Implication for teaching and learning. *SIST Journal of Religion and Humanities, 1*(1).

Baase, S. (2013). *A gift of fire: Social, legal and ethical issue for computing and the Internet.* Pearson.

Blackwood-Brown, G. (2018). An empirical assessment of senior citizens' cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, attitude, and motivation to acquire cybersecurity skills.

Bouraff, T., & Hui, K. (2024). *Regulating information and network security: Review and challenges.* Association for Computing Machinery. Computing Surveys. https://doi.org/10.1145/371112.

Chirunga, T., & Mbwirire, J. (2020). The role of media in peacebuilding: A case study of both public and private media in Harare. *International Journal of Humanities, Art and Social Studies (IJHAS),* 5(3).

Duchi E. M., & Orebiyi, T. P. (2024). Banditry and forced migration: Implication for children education and peacebuilding in Kaduna State (2017-2022). *IJMGS, 4*(1)

Ebelogu, C. U., Ojo, S. D., Andeh, C. P., & Agu, E. O. (2019). Cybercrime, its adherent negative effects on Nigerian youths and the society at large: Possible solutions.

International Journal of Advances in Scientific Research and Engineering, 5(12). DOI: https://doi.org/10.31695/IJASRE.201933658.

Erondu, C. I., & Erondu, U. I. (2023). The role of cyber security in a digitalizing economy: A development perspective. *International Journal of Research and Innovation in Social Science*, *7*(11), 1558-1570

Hang, L. H., & Coppel, I. A. (2020). Cybersecurity: Concepts, challenges and practices. *Journal of Information Security and Cybercrimes Research, 3*(1), 1-12.

Hawkridge, D., & Robinson, J. (2023). *Organizing educational broadcasting*. Taylor & Francis.

Heywood, E. (2020). Radio journalism and women's empowerment in Niger. *Journalism Studies*, *21*(10), 1344-1362.

Ibrahim, M. A., & Jamri, B. (2022). From the fourth estate of the realm to the third party in the relationship: Public education role of the media in setting agenda for cordial civilian-military and principal-agency relations. *Медиаобразование*, (2), 232-252.

Kshetri, N. (2019). Cybercrime and cybersecurity I Africa. *Journal of Global Information Technology Management.* DOI:10.1080/1097198X.2019.1603527.

Kizza, J. M. (2019). *Guide to computer network security.* Springer.

Kur, J. T., Melladu, B. B., Agodosy, F. I., & Orhewere, J. A. (2019). Community radio and Nigeria's national security exigencies: fears and promises. *New Media and Mass Communication, 17.*

Makeri, Y. A. (2017). Cyber security issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering, 7*(4).

McQuail, D. (2005). *Mass communication theory.* Sage Publications.

Montasari, R. (2024). *Cyberspace, cyberterrorism and the international security in the fourt industrial revolution: Threats, assessment and responses*. Springer Nature.

Mordi, M. (2019). Is Nigeria the headquarters of cybercrime in the world? *Guardian.* https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/

National Cyber Security Centre (NCSC). (2021). Making the UK the safest place to live and work online. *NCSC Annual Review.* https://ww.ncsc.gov.uk/collection/ncsc-annual-review.

Nigeria Cybercrime Act 2015. (2015). The Federal Republic of Nigeria Official Gazette.

Nigerian Communications Commission. (2024). Subscriber data. *Report* https: // ncc.gov.ng>statistics.

Nwachukwu, (2021, May 19). Nigeria: A failing state teetering on the brink. *The Punch.*

Obinagwa, C. E., Ngoka, R. O. Uwaechia, O. G., Ezugwu, I. H., Okpala, J. C., & Ayadiuno, R. U. (2023). Youth unemployment and cybercrime in Nigeria. *African Renaissance, 20*(2).

Ottah, P. O., & Okpoko, A. I. (2019) Assessment of cybersecurity among Nigerian youths. *International Journal of Cybersecurity Intelligence and Cyberforensics, 2*(1), 1-12.

Oyeyemi, J. A. (2017). Addressing the challenges of cybersecurity in Nigeria. A collaborative approach. *International Journal of Advanced Computer Science and Applications, 8*(2), 150-156.

Ray, J. R. (2014). Training programs to increase cybersecurity awareness and compliance in non-profits. *Interdisciplinary Studies Program.*

Salami, U. (2025, January 21). Four NYSC members, and eight poly students were arrested for Internet fraud. *Punch.*

Upadhyaya, H. (2024). *Digital education and economic transformation: Bridging the gap*. Meadow Publication.

Udulue, M. C., & Bentina, M. (2019). Prevalence of cybercrimes among youths in Onitsha South local government area of Anambra State, Nigeria. *International Journal of Health and Social Inquiry,* 5(1).

United Nations Department of Economic and Social Affairs. (2014) Definition of youth, 1-7.

Uzoma, C. W., Bello, R., & Falade, M. O. (2016). Background paper on the Nigerian youth. *The Centre for Public Policy Alternatives.* DOI:10.13140/RG.2.2.27860.40324