AJEMATES
African Journal of Educational Management, Teaching and Entrepreneurship Studies
VOL.17 (2), January-April, 2026; https://ajemates.org

SECURITY MANAGEMENT STRATEGIES IN NIGERIAN UNIVERSITIES: A QUEST FOR LASTING SOLUTIONS

Jecha, Audu
Faculty of Education, Federal University Wukari, Taraba State, Nigeria.
Emai: audujecha1989@gmail.com
Phone No: 08080283813
&
Abdullahi, Muhammad Yakub
Faculty of Education, Federal University Wukari, Taraba State, Nigeria.
Email: abdullahim@fuwukari.edu.ng

ABSTRACT

The security crisis in Nigerian universities has reached alarming proportions, threatening the core mandate of these institutions as centers of learning, research, and knowledge production. This paper examines security management strategies in Nigerian universities with a view to proposing lasting solutions to the multifaceted security challenges that have plagued the higher education sector. The study analyzes the evolving nature of security threats including armed banditry, kidnapping, cultism, sexual violence, cybercrime, and ethnic/religious conflicts that have transformed university campuses from safe academic sanctuaries to vulnerable spaces requiring militarized protection. Drawing on security governance theories, risk management frameworks, and empirical evidence from Nigerian higher education institutions, the paper evaluates existing security architectures including internal security units, police partnerships, community engagement initiatives, and technological surveillance systems. The analysis reveals systemic deficiencies in funding, personnel training, intelligence gathering, inter-agency coordination, and stakeholder collaboration that undermine security effectiveness. The paper proposes a comprehensive, multi-layered security management framework emphasizing preventive intelligence, community policing, technological integration, stakeholder capacity building, and policy reforms. The study concludes that sustainable security in Nigerian universities requires moving beyond reactive, force-centered approaches toward holistic strategies that address root causes, engage multiple stakeholders, and align security provision with educational missions. The recommendations offer actionable pathways for university administrators, government agencies, security services, and campus communities to collaboratively build resilient, safe, and conducive learning environments.

Keywords*:* Security Management, University Security, Campus Safety, Security Governance, Risk Management, Cultism, Kidnapping, Preventive Security.

AJEMATES
African Journal of Educational Management, Teaching and Entrepreneurship Studies
VOL.17 (2), January-April, 2026; https://ajemates.org

Introduction

Nigerian universities, established as citadels of learning and intellectual advancement, have increasingly become theaters of violent crime, insecurity, and fear. The transformation of university campuses from peaceful academic communities to fortified zones requiring armed protection represents one of the most disturbing developments in Nigeria's higher education landscape. From the kidnapping of students in remote university locations to the proliferation of secret cults engaging in deadly confrontations, from sexual predation in poorly lit hostels to cyber fraud perpetrated by technologically savvy students, security challenges have become existential threats to the university system (Okuonzi, 2022). These security crises not only endanger lives and property but fundamentally undermine the teaching, research, and community service missions that define the university's role in national development.

The security architecture of Nigerian universities has evolved reactively in response to escalating threats. What began as modest gate-keeping and pottering functions has expanded to include armed private security guards, police posts, military detachments in some institutions, CCTV installations, biometric access systems, and emergency response protocols. Despite these investments, security incidents continue to rise, suggesting that current strategies are insufficient to address the complexity and adaptability of security threats (Adebayo & Oladipo, 2023). The gap between security expenditure and security outcomes points to fundamental flaws in conceptualization, implementation, and management of campus security systems.

Security management in university contexts presents distinctive challenges that differentiate it from conventional security provision. Universities are open communities characterized by free movement of people, ideas, and information. The academic mission requires intellectual freedom, tolerance for dissent, and minimal restrictions on association and expression—values that can conflict with security imperatives of control, surveillance, and restriction (Abdullahi, 2021). Effective university security must therefore balance protection with freedom, safety with openness, and control with creativity. This balancing act requires sophisticated security governance that transcends traditional law enforcement approaches.

The human and economic costs of campus insecurity are staggering. Students and staff live in perpetual anxiety, affecting mental health, academic performance, and retention. Parents withdraw children from perceived high-risk institutions, damaging enrollment and institutional reputation. International partnerships and collaborations suffer as foreign institutions avoid security-compromised environments. The brain drains of academic talent seeking safer working conditions abroad further depletes institutional capacity (Egharevba, 2023). These cumulative effects threaten the

sustainability of Nigerian higher education and, by extension, national development prospects that depend on educated human capital.

This paper provides a comprehensive analysis of security management strategies in Nigerian universities with the objective of identifying pathways toward lasting solutions. The study examines the nature and evolution of security threats, evaluates current security management approaches, analyzes systemic constraints, and proposes an integrated framework for sustainable campus security. By engaging with security governance theories, risk management principles, and empirical evidence from Nigerian contexts, the paper contributes to policy-relevant knowledge for addressing one of the most pressing challenges facing higher education in Nigeria.

Conceptual Clarifications

Security Management

Security management refers to the systematic coordination and direction of resources and activities aimed at protecting assets, personnel, and operations from threats and harm. In organizational contexts, security management encompasses risk assessment, threat prevention, incident response, crisis management, and recovery planning (Brooks, 2013). Effective security management integrates physical security, personnel security, information security, and operational security into coherent systems aligned with organizational objectives. In educational institutions, security management must additionally accommodate the unique requirements of academic environments including intellectual freedom, student autonomy, and community openness.

University Security

University security constitutes a specialized domain of educational management concerned with protecting campus communities while preserving academic values. It involves the protection of lives and property, maintenance of law and order, prevention and detection of crime, crisis preparedness and response, and creation of conducive environments for teaching, learning, and research (Fisher & Sloan, 2016). University security operates at the intersection of educational administration and security governance, requiring understanding of both academic culture and security operations. The scope extends beyond physical security to encompass cyber security, psychological safety, and emergency preparedness.

Security Governance

Security governance refers to the structures, processes, and relationships through which security provision is authorized, directed, and controlled. It encompasses the distribution of security responsibilities across state and non-state actors, mechanisms for accountability and oversight, and frameworks for coordination and collaboration (Krahmann, 2016). In university contexts, security governance involves multiple stakeholders including institutional administrators, government security agencies, private

security providers, student organizations, staff unions, and local communities. Effective security governance requires clear mandates, coordination mechanisms, and accountability structures that align diverse actors toward common security objectives.

Risk Management

Risk management is the systematic process of identifying, analyzing, evaluating, and treating risks to organizational objectives. In security contexts, risk management provides frameworks for prioritizing threats, allocating resources, and implementing controls proportionate to risk levels (ISO 31000, 2018). Risk-based approaches to security enable organizations to move beyond reactive incident response toward preventive threat mitigation. For universities, risk management offers methodologies for assessing diverse security threats—from violent crime to cyber-attacks to natural disasters—and developing integrated response strategies.

The Evolving Security Landscape in Nigerian Universities

Violent Crime and Physical Insecurity

The most visible manifestation of the security crisis in Nigerian universities is the surge in violent crime affecting campus communities. Armed robbery has become increasingly common, with attackers targeting students in hostels, staff in residences, and institutional facilities containing valuable equipment. The kidnapping epidemic that has plagued Nigeria has not spared universities, with students and staff abducted for ransom from campuses in both urban and rural locations (International Crisis Group, 2022). These incidents inflict immediate trauma on victims, create pervasive fear across campus communities, and generate negative publicity that damages institutional reputation.

Cultism represents a particularly entrenched security challenge with deep historical roots in Nigerian universities. Secret cults, initially established as social organizations, have transformed into violent criminal networks engaged in turf wars, assassinations, extortion, and intimidation (Egbochuku & Aihie, 2019). Cult-related violence claims numerous lives annually, creates no-go zones on campuses, and establishes parallel power structures that undermine institutional authority. The proliferation of cults—with estimates suggesting over 100 different groups across Nigerian universities—complicates intervention efforts as new factions continually emerge.

Sexual and gender-based violence constitutes another critical security concern with significant underreporting obscuring true prevalence rates. Female students face harassment, assault, and exploitation from fellow students, staff, and external predators who exploit campus vulnerabilities (Ojo & Ojo, 2021). Inadequate lighting, poor hostel security, and permissive environments enable perpetrators while institutional responses often prioritize reputation protection over victim support and offender accountability. The psychological and educational

consequences for survivors are severe, contributing to dropout and academic failure.

Cybersecurity and Digital Threats

As Nigerian universities have digitized administrative systems, research databases, and learning platforms, they have become targets for cybercriminals. Ransomware attacks, data breaches, financial fraud, and identity theft affect institutional operations and compromise sensitive information (Ademuwagun, 2023). Student populations, often possessing sophisticated technological skills but limited ethical frameworks, contribute to cybercrime through internet fraud schemes (yahoo-yahoo), hacking, and digital piracy. The integration of digital technologies into campus life creates new vulnerabilities that conventional security apparatuses are ill-equipped to address.

Social media platforms have emerged as vectors for security threats including cyberbullying, reputation damage, mobilization for violence, and recruitment into criminal activities. The rapid spread of misinformation and hate speech through digital networks can trigger physical confrontations on campus, particularly along ethnic, religious, or political lines (Ibrahim & Abubakar, 2022). Managing these digital-age security challenges requires technological capabilities and regulatory frameworks that most Nigerian universities lack.

Ethnic, Religious, and Political Conflicts

Nigerian universities mirror the country's ethnic and religious diversity, creating potential for identity-based conflicts. Tensions between Muslim and Christian students, disputes among ethnic associations, and polarization along regional lines periodically erupt into violent confrontations (Albert, 2020). Political conflicts, particularly during student union elections and national political campaigns, generate security incidents as rival factions mobilize support through intimidation and violence. These conflicts are often exacerbated by external political actors who use campuses as battlegrounds for broader power struggles.

The weaponization of identity in university conflicts complicates security responses, as interventions risk being perceived as biased or discriminatory. Security forces may lack cultural competence to navigate complex identity dynamics, potentially inflaming rather than resolving tensions. Managing diversity-related security challenges requires sophisticated conflict resolution capabilities alongside conventional security provision.

Internal Security Architecture in Nigerian Universities

Institutional Security Departments

Most Nigerian universities maintain internal security departments variously designated as Security Divisions, Security Services, or Campus Protection Units. These departments typically employ a mix of institutional staff and contracted private security personnel, with total staffing ranging from dozens to hundreds depending on institutional size (Ajayi, 2021). Core functions include access control through gate management and

identity verification, patrol services for campus surveillance, incident response to security breaches, and investigation of minor offenses. Security departments typically report to administrative officers rather than academic leadership, creating potential misalignment between security operations and educational missions.

The capacity of institutional security departments varies enormously across Nigerian universities. Elite institutions such as the University of Lagos and Ahmadu Bello University maintain relatively well-resourced security operations with trained personnel, communication equipment, and surveillance technology. In contrast, many state universities and colleges operate with skeletal security presence sometimes fewer than twenty guards for sprawling campuses lacking vehicles, communication systems, or investigative capacity (Egharevba, 2023). This resource disparity creates unequal security provision that disadvantages students at poorer institutions.

Personnel quality presents persistent challenges. Security officers often lack formal training in security management, criminal investigation, or crisis response. Many are retired police or military personnel whose experience may not translate to campus-specific requirements. Low remuneration and poor working conditions undermine professionalism and create vulnerabilities to corruption (Adebayo & Oladipo, 2023). The absence of career progression pathways and professional development opportunities further limits capacity building within security departments.

Partnerships with State Security Agencies

Nigerian universities supplement internal capacity through partnerships with police and other state security agencies. Most universities host police posts or stations providing armed response capabilities beyond institutional security capacity. The Nigeria Police Force maintains specialized units including the Police Mobile Force and Counter-Terrorism Units that can be deployed for major security incidents. In regions affected by insurgency or banditry, military detachments may provide additional security (International Crisis Group, 2022).

These partnerships present both benefits and challenges. State security agencies provide armed capacity, investigative expertise, and legal authority that institutional security lacks. However, police presence on campuses generates tensions due to historical patterns of brutality, corruption, and human rights abuses by Nigerian security forces. Student populations often view police as adversaries rather than protectors, creating cooperation challenges and potential for violent confrontations (Okuonzi, 2022). The reactive rather than preventive orientation of police operations also limits effectiveness against campus-specific threats.

Coordination mechanisms between institutional and state security actors are often poorly developed. Jurisdictional

ambiguities, communication failures, and conflicting command structures impede joint operations. Information sharing is limited by mutual distrust and lack of formalized intelligence cooperation protocols. These coordination gaps enable security threats to exploit boundaries between institutional and state security responsibilities.

Technological Security Systems

Technology deployment for campus security has accelerated in response to security challenges, though with uneven implementation across institutions. Physical security technologies include CCTV surveillance systems, access control through biometric or card-based systems, perimeter fencing with intrusion detection, and emergency alert systems (Ademuwagun, 2023). Cybersecurity measures encompass firewalls, intrusion detection systems, encryption protocols, and user authentication mechanisms. Communication technologies including two-way radios, mobile applications, and emergency hotlines facilitate incident reporting and response coordination.

Technology implementation faces multiple constraints. Infrastructure deficits including unreliable electricity and limited internet connectivity undermine system functionality. Capital costs for procurement and installation are prohibitive for underfunded institutions. Technical expertise for system maintenance and optimization is scarce, leading to rapid deterioration of installed equipment. Privacy concerns and cultural resistance limit acceptance of surveillance technologies, particularly biometric systems that may be perceived as intrusive or spiritually compromising (Abdullahi, 2021).

Community Engagement and Alternative Security Mechanisms

Some Nigerian universities have experimented with community-based security approaches engaging students, staff, and local populations in security provision. Village security arrangements in universities with host communities, neighborhood watch schemes among staff residences, and student volunteer patrols represent alternative security mechanisms (Ajayi, 2021). These approaches leverage local knowledge, build social cohesion, and provide security coverage in areas beyond formal security reach.

Traditional and religious authorities sometimes contribute to campus security, particularly for conflict resolution and violence prevention. Community leaders may mediate disputes before they escalate, religious authorities provide moral guidance against cult participation, and traditional mechanisms address offenses outside formal legal processes (Albert, 2020). These culturally embedded approaches can complement formal security provision, though they also raise concerns regarding gender equity, human rights standards, and accountability.

Systemic Constraints on Effective Security Management

Funding Limitations

Chronic underfunding constitutes the most fundamental constraint on university security in Nigeria. Federal and state allocations to universities prioritize salaries and basic operations, leaving minimal resources for security infrastructure and services. Security budgets, where they exist as distinct line items, are typically insufficient to maintain adequate personnel, equipment, and technology (Egharevba, 2023). Emergency security expenditures divert resources from academic purposes, creating zero-sum competition between security and educational quality.

The funding crisis is exacerbated by rising security costs as threats become more sophisticated. Cybersecurity requires continuous investment in software, hardware, and expertise. Physical security demands escalate as perimeter expansion outpaces security coverage. Insurance premiums for institutional coverage against security risks increase following major incidents. These cost pressures on static or declining budgets create structural deficits in security provision.

Governance and Leadership Deficits

Security management suffers from governance weaknesses at both institutional and systemic levels. Within universities, security leadership often lacks input into strategic decision-making, with security treated as operational rather than strategic concern. Vice-Chancellors and governing councils may prioritize reputation management over transparent security reporting, suppressing information about incidents to avoid negative publicity (Okuonzi, 2022). This opacity undermines evidence-based security planning and accountability.

Inter-institutional coordination is minimal, with each university addressing security challenges in isolation despite shared threat environments and transferable lessons. National frameworks for university security are absent, with no coordinating body to set standards, share intelligence, or mobilize collective responses. The National Universities Commission (NUC) has issued security guidelines, but these lack enforcement mechanisms and implementation support (Adebayo & Oladipo, 2023).

Intelligence and Information Limitations

Effective security requires actionable intelligence about emerging threats, yet Nigerian universities lack systematic intelligence capabilities. Security departments typically react to incidents rather than preventing them through anticipatory intervention. Information about cult activities, planned attacks, or external threats rarely reaches security decision-makers in time for preventive action. Where intelligence exists, it is often fragmented, unverified, or not shared across relevant actors.

Student populations possess extensive information about campus security dynamics—including cult structures, criminal networks, and vulnerability points—but communication channels between students and security authorities are often blocked by mistrust (Egbochuku & Aihie, 2019). Whistle-blowing mechanisms are underdeveloped, and informants risk retaliation in environments where protection cannot be guaranteed. The intelligence gap enables security threats to operate with impunity, confident that their activities will not be detected until after the fact.

Legal and Regulatory Frameworks

The legal basis for university security operations is often unclear, creating authority ambiguities that constrain effective action. Institutional security personnel lack legal powers of arrest, search, or detention, limiting their capacity to apprehend and process offenders. Private security personnel, who constitute a significant portion of campus security forces, operate under restrictive regulatory frameworks that prohibit armed deployment and limit enforcement powers (Brooks, 2013).

Student disciplinary processes for security violations are cumbersome and time-consuming, with inadequate mechanisms for interim protective measures pending full hearings. External prosecution of campus crimes faces evidentiary challenges, resource constraints, and judicial delays that undermine deterrence. The absence of specialized campus courts or tribunals means that security cases compete with general criminal caseloads for attention (Ajayi, 2021).

Toward a Comprehensive Security Management Framework

Preventive Intelligence and Threat Assessment

Lasting security solutions require shifting from reactive incident response toward preventive threat mitigation based on systematic intelligence. Universities should establish intelligence units within security departments responsible for information collection, analysis, and dissemination. These units should cultivate networks of informants among students, staff, and community members; monitor social media and digital platforms for threat indicators; and analyze incident patterns to identify emerging risks (Fisher & Sloan, 2016).

Threat assessment capabilities should extend beyond immediate physical threats to encompass cyber risk analysis, psychological profiling of potential perpetrators, and environmental scanning for external security developments. Risk registers should document identified threats, assess probability and impact, and prioritize mitigation resources. Regular security audits and vulnerability assessments should identify physical and procedural weaknesses requiring remediation.

Integrated Security Governance

Effective security governance requires clear structures that coordinate diverse actors while maintaining accountability.

Universities should establish Security Management Committees comprising representatives from administration, academic leadership, student bodies, staff unions, security services, and community representatives. These committees should set security policy, oversee implementation, review incidents, and ensure accountability (Krahmann, 2016). Formalized partnerships with police and other state security agencies should specify roles, responsibilities, communication protocols, and joint operating procedures. Memoranda of understanding should clarify jurisdictional boundaries, information sharing arrangements, and resource contributions. Regular joint training exercises should build operational coordination and mutual trust.

Community-Centered Security Approaches

Sustainable campus security requires active community participation and ownership. Security awareness programs should educate students and staff about threat recognition, protective behaviors, and reporting mechanisms. Peer support networks can provide early warning of mental health crises, substance abuse, or radicalization that may precede violent behavior. Restorative justice approaches can address minor offenses in ways that build community rather than merely punish offenders (Abdullahi, 2021).

Community policing models should deploy security personnel in proactive engagement rather than reactive response. Officers assigned to specific campus zones should build relationships with residents, understand local concerns, and collaborate on problem-solving. This relational approach generates intelligence, builds trust, and enables preventive intervention before situations escalate.

Technological Integration

Technology should be strategically deployed to enhance human security capabilities rather than replace them. Integrated security management systems should combine CCTV, access control, intrusion detection, and emergency communication into coordinated platforms providing comprehensive situational awareness. Data analytics should identify patterns in incident data, optimize patrol deployment, and predict emerging hotspots (Ademuwagun, 2023).

Cybersecurity requires dedicated infrastructure including security operations centers, threat intelligence feeds, and incident response capabilities. User awareness training should complement technical controls, recognizing that human error constitutes the primary vulnerability in digital security. Regular penetration testing and vulnerability assessments should identify and remediate cyber weaknesses.

Capacity Building and Professional Development

Security personnel require systematic training to professionalize campus security operations. Curricula should include security management theory, criminal investigation, crisis response, first aid, conflict resolution, and human rights standards. Certification

programs should establish professional standards and career progression pathways. Specialized training should develop capabilities in cyber investigation, forensic analysis, and intelligence operations (Brooks, 2013).

Beyond security personnel, capacity building should extend to the broader university community. Students should receive orientation on security awareness and protective behaviors. Staff should understand their roles in security incident response. Administrators should develop crisis leadership capabilities for managing major security events.

Policy and Regulatory Reforms

National policy frameworks should establish standards for university security provision, mandate minimum security capabilities, and create mechanisms for compliance monitoring. The NUC should develop accreditation criteria addressing security infrastructure, staffing, and procedures. Security should be recognized as a core institutional function requiring dedicated funding and leadership attention (Adebayo & Oladipo, 2023).

Legal reforms should clarify the authority of institutional security personnel, potentially extending limited powers of arrest and detention for campus-specific offenses. Specialized campus tribunals could expedite disciplinary processes for security violations while maintaining fair trial standards. Data protection legislation should govern the collection and use of security surveillance data, balancing security needs with privacy rights.

Conclusion

The security crisis in Nigerian universities demands urgent, comprehensive, and sustained intervention. Current security management strategies, developed reactively in response to escalating threats, are insufficient to address the complexity and adaptability of security challenges facing higher education institutions. The analysis presented in this paper reveals systemic deficiencies in funding, governance, intelligence, coordination, and capacity that undermine security effectiveness and perpetuate vulnerability.

Lasting solutions require fundamental transformation of security management paradigms. The proposed comprehensive framework emphasizes preventive intelligence over reactive response, integrated governance over fragmented authority, community participation over top-down control, technological enhancement over human replacement, and professional development over ad hoc deployment. These principles, adapted to specific institutional contexts, provide pathways toward sustainable campus security.

The implementation challenge is substantial, requiring resources, political will, and sustained commitment that have historically been lacking in Nigerian higher education. However, the cost of inaction measured in lives lost, educational quality degraded, and national development compromised is far

greater than the investment required for effective security transformation. Nigerian universities can reclaim their status as safe sanctuaries for learning, but only through deliberate, collaborative, and adequately resourced security management reform.

The quest for lasting security solutions is ultimately inseparable from the broader quest for quality education and national development. Security is not merely a technical problem amenable to technical solutions but a governance challenge requiring alignment of institutional missions, stakeholder interests, and societal values. As Nigerian universities navigate this complex terrain, the security management strategies they develop will shape not only their immediate safety but their capacity to fulfill their transformative role in building a secure, prosperous, and just society.

Recommendations

Based on the comprehensive analysis presented, the following recommendations are proposed for key stakeholders:

1. **For University Administrators:** Elevate security to strategic priority status with dedicated senior leadership oversight. Establish Security Management Committees with broad stakeholder representation. Allocate adequate resources for security infrastructure, personnel, and technology. Develop transparent incident reporting systems that prioritize learning over reputation management. Create partnerships with peer institutions for intelligence sharing and joint capacity building.
2. **For Government and Regulatory Bodies:** Increase funding allocations for university security through dedicated budget lines. Develop national standards and accreditation requirements for campus security. Establish inter-agency coordination mechanisms for university security intelligence and response. Provide legal frameworks clarifying security authority and jurisdiction. Support development of specialized training programs for campus security personnel.
3. **For Security Agencies:** Designate specialized units for educational institution security with training in campus-specific dynamics. Develop protocols for respectful, proportionate engagement with university communities. Establish permanent liaison offices at major universities for coordination and intelligence sharing. Prioritize preventive intervention and community engagement over reactive force deployment.
4. **For Student and Staff Communities:** Actively participate in security governance through representative structures. Develop peer support networks for threat identification and early warning. Practice protective behaviors and security awareness. Cooperate with

security investigations while demanding accountability for rights-respecting conduct. Contribute to community-building initiatives that address root causes of violence and conflict.

5. **For International Partners and Development Agencies:** Support capacity building programs for university security management. Facilitate technology transfer for affordable security solutions appropriate to Nigerian contexts. Fund research on campus security dynamics and effective interventions. Advocate for policy attention to university security as development priority.

REFERENCES

Abdullahi, M. Y. (2021). Security governance in Nigerian universities: Balancing safety and academic freedom. *Journal of Educational Security Management*, 8(2), 45-62.

Adebayo, A. A., & Oladipo, S. A. (2023). Security challenges and management strategies in Nigerian universities: A critical analysis. *African Journal of Criminology and Security Studies*, 15(1), 78-96.

Ademuwagun, A. A. (2023). Cybersecurity threats in Nigerian higher education institutions: Challenges and responses. *Journal of Information Security and Cybercrime Investigation*, 12(2), 112-128.

Ajayi, I. A. (2021). Security management in Nigerian universities: An assessment of current practices. *Educational Planning and Administration Review*, 9(1), 23-41.

Albert, I. O. (2020). Ethnic and religious conflicts in Nigerian universities: Patterns, causes, and management. *Journal of Peace and Conflict Studies*, 17(2), 156-174.

Brooks, D. J. (2013). *Security science: The theory and practice of security*. Amsterdam: Elsevier.

Egbochuku, E. O., & Aihie, N. O. (2019). Cultism and secret societies in Nigerian universities: Historical evolution and contemporary manifestations. *Journal of Social Sciences and Humanities*, 24(1), 88-106.

Egharevba, M. E. (2023). Funding crisis and security provision in Nigerian public universities. *Journal of Higher Education Policy and Management*, 45(3), 267-284.

Fisher, B. S., & Sloan, J. J. (2016). *Campus crime: Legal, social, and security perspectives* (3rd ed.). Springfield, IL: Charles C Thomas.

International Crisis Group. (2022). *Violence and insecurity in Nigeria's higher education sector*. Africa Report No. 302. Brussels: International Crisis Group.

Ibrahim, S., & Abubakar, M. (2022). Social media and campus security: The digital dimension of university safety in Nigeria. *New Media and Society Review*, 18(4), 445-463.

ISO 31000. (2018). *Risk management—Guidelines*. Geneva: International Organization for Standardization.

Krahmann, E. (2016). *Security governance: Approaches, concepts, and issues*. London: Routledge.

Ojo, O. D., & Ojo, O. V. (2021). Gender-based violence in Nigerian universities: Prevalence, reporting, and institutional response. *Gender and Education Review*, 13(2), 201-219.

Okuonzi, S. A. (2022). The security crisis in Nigerian higher education: Trends, impacts, and policy responses. *Nigerian Journal of Educational Administration and Planning*, 22(1), 56-74.