Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 10, pp 41-50, October, 2026

EFFECTIVENESS OF SECURITY MEASURES IN SELECTED POLYTECHNICS IN NORTHERN NIGERIA

Isah Balarabe*[1], Shamsuddeen Salihu Kamba[2]

[1] Department of General Studies, Kebbi State Polytechnic Dakingari. Nigeria.
isahbala4040@gmail.com
[2] Department of Public Administration, Kebbi State Polytechnic Dakingari. Nigeria.
shamsuddeenkamba@gmail.com

ABSTRACT :

This study evaluates the effectiveness of security measures in selected polytechnics in Northern Nigeria. The study examined existing security measures, their operational effectiveness, implementation challenges, the utilization of emerging security technologies, stakeholder perceptions of campus safety, collaboration with external security agencies, and strategies for improving security management. A descriptive survey design with a mixed-methods approach was adopted. From an estimated population of 18,500 stakeholders, 500 respondents were selected through a multi-stage sampling procedure, while 462 usable questionnaires were returned, representing a 92.4% response rate. Quantitative data were collected using the Questionnaire on the Effectiveness of Security Measures in Selected Polytechnics in Northern Nigeria (QESMSPNN) and analyzed using frequencies, percentages, means, standard deviations, Pearson correlation, and multiple regression in SPSS Version 29. Qualitative evidence was obtained through key informant interviews and analyzed thematically. The findings indicate that physical security infrastructure and personnel deployment were widely implemented, whereas emergency preparedness and advanced security technologies were less developed. Inadequate funding, shortages of trained personnel, obsolete equipment, and unstable electricity were major implementation challenges. The regression model explained 42% of the variance in perceived campus safety ($R^2 = .42$, adjusted $R^2 = .41$), with the overall model statistically significant, $F(6, 455) = 54.91$, $p < .001$. The study concludes that sustainable campus security requires coordinated investment in personnel, technology, infrastructure, and inter-agency collaboration.

Keywords: security measures; security management; polytechnics; Northern Nigeria; campus safety; security technologies

1. Introduction

Security is a fundamental condition for sustainable educational development because teaching, learning, research, innovation, and institutional engagement depend on an environment in which members of the academic community can operate without undue fear of violence, intimidation, or criminal activity. The effectiveness of an educational institution is therefore influenced not only by personnel, infrastructure, and instructional resources but also by the capacity of the institution to prevent, detect, and respond to security threats (UNESCO, 2021; Federal Republic of Nigeria [FRN], 2013). Where security is compromised, institutional productivity may decline, academic activities may be disrupted, staff morale may weaken, and confidence in the institution may be affected (Ogunode & Musa, 2023; World Bank, 2022).

In Nigeria, the security environment has become increasingly complex, with educational institutions operating within a broader context of insurgency, kidnapping, banditry, armed robbery, communal conflict, cybercrime, vandalism, and other forms of insecurity (Institute for Economics & Peace, 2024; National Bureau of Statistics [NBS], 2024). Northern Nigeria has experienced significant security pressures, and insecurity has affected educational continuity through disruptions to academic calendars, threats to institutional facilities, and risks to students and staff (UNICEF, 2023; UNESCO, 2022). These conditions make campus security management an important institutional and public-policy concern.

Security management in polytechnics is multidimensional. It includes physical protection, personnel deployment, access control, security policies, surveillance, emergency preparedness, technology adoption, information sharing, and collaboration with external security agencies. Contemporary approaches increasingly emphasize layered or defense-in-depth security, in which physical controls and human security personnel are integrated with surveillance technologies, communication systems, institutional policies, and coordinated response arrangements (ASIS International, 2022).

Despite the importance of these measures, evidence is needed on how effectively they operate within polytechnic environments in Northern Nigeria. In particular, there is a need to distinguish between the presence of security measures and their perceived effectiveness, while also examining the constraints that affect implementation. This study therefore evaluates security measures in selected polytechnics and examines the relationships between security management practices, technology adoption, institutional funding, personnel training, external collaboration, and perceived security effectiveness.

1.1 Statement of the Problem

The deteriorating security situation in Northern Nigeria poses serious challenges for tertiary institutions. Persistent insecurity can disrupt academic activities, increase institutional operating costs, and expose students, staff, and facilities to risk. Effective campus security also requires coordinated action among institutional management, security personnel, host communities, and conventional law-enforcement agencies. However, weak coordination may contribute to delayed emergency response, inadequate intelligence sharing, and ineffective implementation of security policies. The absence of comprehensive risk assessment and empirical evaluation further limits evidence-based security planning.

1.2 Aim and Objectives of the Study

The primary aim of the study is to evaluate the effectiveness of security measures in selected polytechnics in Northern Nigeria. The specific objectives are to:

1. Identify existing security measures implemented in the polytechnics;
2. Assess the effectiveness of existing measures in safeguarding lives, property, and facilities;
3. Examine major challenges affecting security implementation;
4. Determine the extent to which emerging security technologies are utilized;
5. Examine the relationship between security management practices and stakeholders' perception of campus safety;
6. Investigate the level of collaboration between campus security units and external security agencies; and
7. Formulate evidence-based strategies for strengthening campus security management.

1.3 Research Hypotheses

The following null hypotheses were tested at the 0.05 level of significance:

1. H01: There is no significant relationship between existing security management practices and stakeholders' perception of campus safety.
2. H02: There is no significant relationship between the adoption of modern security technologies and the effectiveness of campus security management.
3. H03: There is no significant relationship between institutional funding for security and the effectiveness of security management.
4. H04: There is no significant relationship between the training of security personnel and the effectiveness of campus security management.
5. H05: There is no significant relationship between collaboration with external security agencies and the effectiveness of campus security management.

2. Literature Review and Theoretical Framework

2.1 Concept of Security

Security is a multidimensional concept understood differently across disciplines, including political science, sociology, criminology, public administration, military studies, and education. Traditionally, it focused on protecting national territory from external aggression; however, contemporary perspectives extend it to the protection of individuals, institutions, infrastructure, information, and social systems from various threats and vulnerabilities. In educational institutions, security encompasses preventive, protective, and responsive measures that safeguard members of the academic community and ensure continuity of educational activities. Thus, institutional security requires an appropriate combination of physical, human, administrative, technological, and emergency-response measures.

2.2 Concept of Educational Security

Educational security refers to the protection of institutions, learners, personnel, facilities, information resources, and educational processes from physical, psychological, technological, environmental, and social threats that may hinder educational objectives. It involves measures that create safe environments for teaching, learning, research, innovation, and community engagement without undue fear of violence, intimidation, discrimination, or criminal activities (UNESCO, 2023). Effective educational security requires institutions to identify risks, implement preventive measures, maintain emergency-response mechanisms, and establish partnerships with relevant security stakeholders. It therefore involves not only protecting people and property but also maintaining institutional stability and continuity.

2.3 Security Management in Tertiary Institutions

Security management in tertiary institutions involves the systematic planning, coordination, implementation, monitoring, and improvement of policies,

procedures, personnel, technologies, and resources for preventing threats and protecting students, staff, visitors, facilities, information assets, and academic activities (ASIS International, 2022). It is a strategic institutional function that extends beyond security guards and physical barriers to include access control, surveillance, emergency preparedness, security policies, information management, and collaboration with external security agencies.

The effectiveness of institutional security depends on the adequacy, maintenance, funding, staffing, coordination, and utilization of security measures. Physical infrastructure alone may not guarantee adequate protection where personnel are insufficient, procedures are weak, equipment is poorly maintained, or emergency-response capacity is limited. Effective security management therefore requires an integrated and layered system capable of preventing threats, detecting risks, responding to incidents, and supporting institutional resilience.

2.4 Security Challenges in Northern Nigeria

Northern Nigeria has experienced persistent security challenges, including insurgency, armed banditry, kidnapping, cattle rustling, communal conflicts, farmer–herder clashes, trans-border crimes, organized criminal activities, and violent extremism. These challenges have implications for tertiary institutions because they can threaten the lives and property of students and staff, disrupt academic activities, damage infrastructure, and increase institutional security expenditure.

Consequently, polytechnics in the region require security systems capable of addressing both conventional and emerging threats. Physical protection, trained personnel, access control, surveillance, emergency preparedness, institutional policies, and collaboration with external security agencies are important components of such systems.

2.5 Existing Security Measures in Nigerian Polytechnics

Security management in Nigerian polytechnics involves physical, human, technological, procedural, and collaborative measures designed to protect lives, property, infrastructure, and academic activities. Physical measures include perimeter fencing, controlled entry and exit points, security gates, lighting, security posts, patrols, and protection of sensitive facilities. Human measures involve security personnel responsible for monitoring premises, regulating access, conducting patrols, and responding to incidents.

Administrative and procedural measures include security policies, visitor-management procedures, emergency protocols, incident-reporting systems, and coordination between management and security units. Collaborative measures involve cooperation among polytechnic authorities, campus security personnel, host communities, and external security agencies. Their effectiveness depends on adequate resources and proper integration. Thus, physical infrastructure may provide limited protection where personnel, procedures, maintenance, or emergency-response capacity are inadequate.

2.6 Emerging Security Technologies in Higher Education

Digital technologies have increasingly complemented traditional approaches to higher-education security. Common technologies include closed-circuit television (CCTV), biometric identification, cybersecurity systems, smart access-control systems, artificial intelligence (AI), Internet of Things (IoT) devices, and drones. These technologies can support real-time monitoring, access management, threat detection, information processing, and emergency response.

However, effective technology utilization depends on institutional conditions, including funding, electricity supply, ICT infrastructure, personnel capacity, maintenance arrangements, and institutional policies. Therefore, the availability of technology does not necessarily indicate effective utilization. Institutions must possess the technical and organizational capacity to operate, maintain, and integrate these technologies into their wider security-management systems.

2.7 Artificial Intelligence-Assisted Surveillance

Artificial intelligence-assisted surveillance is an emerging component of institutional security management. AI-enabled systems can process surveillance information, identify unusual activities, recognize patterns, monitor access points, and support early detection of potential threats. Such applications can complement security personnel through continuous monitoring and faster identification of incidents.

Nevertheless, effective AI implementation requires reliable ICT infrastructure, electricity, trained personnel, adequate funding, maintenance, and appropriate institutional policies. For polytechnics in Northern Nigeria, AI-assisted surveillance is therefore better understood as a complement to existing physical and human security measures. Its contribution depends on effective integration within the wider institutional security framework.

2.8 Routine Activity Theory

This study is anchored on Routine Activity Theory (RAT), developed by Cohen and Felson (1979). The theory proposes that predatory crime occurs when three elements converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian.

RAT provides a useful framework for understanding security in polytechnic environments. Students, staff, visitors, facilities, and information resources may constitute potential targets, while individuals intending to commit criminal acts represent motivated offenders. Security personnel, access-control systems, surveillance technologies, physical barriers, institutional policies, and emergency-response mechanisms can function as capable guardians. Strengthening guardianship can reduce opportunities for security incidents through improved surveillance, access control, detection, and institutional response. The theory therefore provides a basis for examining how different security measures contribute to campus safety and security effectiveness.

2.9 Empirical Studies on Security Measures in Tertiary Institutions

Empirical studies indicate that tertiary institutions increasingly combine physical infrastructure, administrative controls, security personnel, technological surveillance, and stakeholder collaboration to improve campus safety. Iwuamadi and Akuakanwa (2024) examined technological innovations in campus security management across public tertiary institutions in South-East Nigeria using 735 respondents. The study found that although institutions recognized the importance of modern surveillance technologies, implementation was constrained by financial limitations, poor maintenance culture, unstable electricity supply, and inadequate ICT infrastructure.

The study demonstrates that technology adoption depends not only on awareness and availability but also on financial, infrastructural, technical, and human-resource capacity. The present study extends this focus by examining physical security infrastructure, personnel deployment, access control, security policies, surveillance, emergency preparedness, inter-agency collaboration, and perceived campus safety in selected polytechnics in Northern Nigeria. This broader approach treats security as an integrated institutional system rather than a technology-specific issue.

3. Methodology

3.1 Research Design and Sampling

The study adopted a descriptive survey research design complemented by a mixed-methods approach. The target population comprised approximately 18,500 stakeholders across public polytechnics in Northern Nigeria. A sample of 500 respondents was selected using a multi-stage procedure incorporating purposive, stratified, and simple random sampling techniques. Respondents were drawn from principal officers, chief security officers, security personnel, academic staff, non-academic staff, students, and external security agencies.

Area of the Study

The study will be conducted in selected public polytechnics located in Northern Nigeria. Northern Nigeria comprises the North-West, North-East, and North-Central geopolitical zones, accounting for nineteen states and the Federal Capital Territory.

For this study, six public polytechnics will be purposively selected to ensure adequate geographical representation across the three geopolitical zones. The proposed institutions include:

Waziri Umaru Federal Polytechnic, Birnin Kebbi (North-West)

Hassan Usman Katsina Polytechnic, Katsina (North-West)

Federal Polytechnic, Bauchi (North-East)

Federal Polytechnic, Damaturu (North-East)

Federal Polytechnic, Bida (North-Central)

These institutions were selected because they represent different ownership structures (federal and state), geographical contexts, student population sizes, and security environments. They have also experienced varying degrees of security challenges, making them suitable for evaluating the effectiveness of campus security measures.

3.2 Instrumentation and Data Collection

Quantitative data were collected using the structured Questionnaire on the Effectiveness of Security Measures in Selected Polytechnics in Northern Nigeria (QESMSPNN). Qualitative evidence was obtained through key informant interviews with principal officers, chief security officers, and police commanders. The questionnaire clusters reported Cronbach's alpha coefficients exceeding 0.80, indicating acceptable internal consistency for the study.

3.3 Data Analysis

Quantitative data were analyzed using SPSS Version 29. Descriptive statistics included frequencies, percentages, means, and standard deviations. Pearson correlation and multiple regression were used to examine relationships among the study variables and to test the stated hypotheses. Qualitative interview data were analyzed using thematic analysis. Statistical decisions were made at the 0.05 significance level.

4. Results

4.1 Response Rate and Respondent Characteristics

Of the 500 questionnaires distributed, 462 were retrieved, properly completed, and considered usable, yielding a response rate of 92.4%.

Table 1. Questionnaire Distribution and Response Rate

Questionnaire Status	Frequency	Percentage (%)
Questionnaires distributed	500	100.0
Questionnaires returned and usable	462	92.4
Questionnaires not returned/unusable	38	7.6
Total	500	100.0

Table 2. Distribution of Respondents by Category

Respondent Category	Frequency	Percentage (%)
Principal Officers	22	4.8
Chief Security Officers	6	1.3
Security Personnel	57	12.3
Academic Staff	84	18.2
Non-academic Staff	64	13.9
Students	204	44.2
External Security Agencies	25	5.4
Total	462	100.0

4.2 Existing Security Measures

Table 3. Mean Ratings of Existing Security Measures

Security Measure	Mean	SD	Decision
Physical security infrastructure	3.74	0.86	Accepted
Security personnel deployment	3.68	0.91	Accepted
Access control measures	3.61	0.89	Accepted
Security policies and procedures	3.42	0.94	Accepted
Surveillance systems	3.27	1.02	Accepted
Emergency preparedness	3.15	1.01	Accepted
Grand Mean	3.48	0.94	Accepted

Physical security infrastructure recorded the highest mean rating (M = 3.74, SD = 0.86), followed by security personnel deployment (M = 3.68, SD = 0.91) and access control measures (M = 3.61, SD = 0.89). Security policies and procedures recorded M = 3.42, while surveillance systems and emergency preparedness recorded M = 3.27 and M = 3.15, respectively. The grand mean of 3.48 indicates broad implementation of basic security measures, with greater emphasis on conventional physical controls than on emergency preparedness and electronic surveillance.

4.3 Effectiveness of Existing Security Measures

Table 4. Effectiveness of Existing Security Measures

Indicator of Effectiveness	Mean	SD	Decision
Protection of lives and property	3.69	0.84	Effective
Improvement of campus safety	3.63	0.86	Effective
Prevention of security-related incidents	3.56	0.88	Effective
Institutional resilience	3.38	0.92	Effective
Emergency response	3.21	0.97	Effective
Overall Mean	3.49	0.89	Effective

Respondents generally rated existing security arrangements as effective (M = 3.49, SD = 0.89). Protection of lives and property received the highest rating (M = 3.69), followed by improvement of campus safety (M = 3.63) and prevention of security-related incidents (M = 3.56). Emergency response had the lowest mean (M = 3.21), suggesting that response speed and coordination represent a comparatively weaker component of existing arrangements.

4.4 Challenges Affecting Security Implementation

Table 5. Challenges Affecting Security Implementation

Challenge	Mean	SD	Rank
Inadequate funding	4.21	0.79	1st
Shortage of trained security personnel	4.05	0.86	2nd
Obsolete security equipment	3.98	0.91	3rd
Unstable electricity supply	3.91	0.95	4th
Poor ICT infrastructure	3.83	0.97	5th
Weak implementation of security policies	3.71	0.99	6th
Inadequate training	3.66	1.01	7th

Inadequate funding was identified as the highest-rated challenge (M = 4.21, SD = 0.79), followed by shortage of trained security personnel (M = 4.05, SD = 0.86) and obsolete security equipment (M = 3.98, SD = 0.91). Unstable electricity supply (M = 3.91) and poor ICT infrastructure (M = 3.83) were also substantial constraints.

4.5 Utilization of Emerging Security Technologies

Table 6. Utilization of Emerging Security Technologies

Security Technology	Mean	SD	Decision
CCTV surveillance	3.35	1.04	Moderate
Biometric systems	3.08	1.08	Moderate
Cybersecurity systems	3.02	1.03	Moderate
Smart access-control systems	2.87	1.07	Moderate
Artificial intelligence systems	2.41	1.10	Low
Internet of Things (IoT) systems	2.36	1.09	Low
Drone technology	2.18	1.06	Low
Overall Mean	2.75	1.06	Moderate

Technology utilization was moderate overall (M = 2.75, SD = 1.06). CCTV surveillance recorded the highest utilization mean (M = 3.35), followed by biometric systems (M = 3.08) and cybersecurity systems (M = 3.02). Artificial intelligence (M = 2.41), IoT systems (M = 2.36), and drone technology (M = 2.18) recorded low levels of utilization.

4.6 Security Management Practices and Perceived Campus Safety

Table 7. Multiple Regression Analysis of Security Management Practices and Perceived Campus Safety

Predictor	B	SE	β	t	p
Constant	0.82	0.15	—	5.47	< .001
Physical security infrastructure	0.18	0.06	0.17	3.00	.003
Security personnel	0.21	0.07	0.18	3.14	.002
Access control	0.16	0.06	0.15	2.67	.008
Surveillance	0.14	0.05	0.14	2.80	.005
Security policies	0.19	0.06	0.17	3.17	.002
Emergency preparedness	0.12	0.05	0.11	2.40	.017

$R^2 = .42$; adjusted $R^2 = .41$; $F(6, 455) = 54.91$; $p < .001$.
The multiple regression model explained 42% of the variance in stakeholders' perception of campus safety ($R^2 = .42$; adjusted $R^2 = .41$). The overall model was statistically significant, $F(6, 455) = 54.91$, $p < .001$. All six predictors had positive and statistically significant coefficients at the 0.05 level. Security personnel deployment had the largest standardized coefficient in the model ($\beta = .18$, $p = .002$), followed by physical security infrastructure ($\beta = .17$, $p = .003$) and security policies ($\beta = .17$, $p = .002$).

4.7 Collaboration with External Security Agencies

Table 8. Institutional Collaboration with External Security Agencies

Collaboration Indicator	Mean	SD	Decision
Information sharing	3.72	0.91	High
Regular communication	3.69	0.88	High
Joint security operations	3.54	0.95	High
Emergency coordination	3.47	0.98	Moderate
Joint training and capacity building	3.12	1.02	Moderate
Overall Mean	3.51	0.95	High

Overall collaboration between institutional security units and external law-enforcement bodies was rated high (M = 3.51, SD = 0.95). Information sharing recorded the highest mean (M = 3.72), followed by regular communication (M = 3.69) and joint security operations (M = 3.54). Joint training and capacity building recorded a lower mean of 3.12.

4.8 Strategies for Improving Security Effectiveness

Table 9. Strategies for Improving Security Effectiveness

Improvement Strategy	Mean	SD	Rank
Increased security funding	4.48	0.65	1st
Security personnel capacity building	4.35	0.71	2nd
Adoption of modern security technologies	4.31	0.74	3rd
Strengthening inter-agency collaboration	4.27	0.76	4th
Security policy reforms	4.22	0.79	5th
Increased community participation	4.08	0.83	6th

Increased security funding recorded the highest mean rating (M = 4.48, SD = 0.65), followed by security personnel capacity building (M = 4.35), adoption of modern security technologies (M = 4.31), and strengthening inter-agency collaboration (M = 4.27). Security policy reforms and increased community participation also received high ratings.

4.9 Test of Null Hypotheses

All five null hypotheses were tested at the 0.05 level of significance. The results are presented below.

Table 10. Test of Hypothesis One

Statistic	Value
Multiple correlation (R)	0.65
Coefficient of determination (R^2)	0.42
F-value	54.91
Degrees of freedom	6, 455
p-value	< .001
Decision	Reject H01

H01 was rejected because the multiple regression model was statistically significant, $F(6, 455) = 54.91$, $p < .001$. The results indicate a statistically significant relationship between security management practices and stakeholders' perception of campus safety.

Table 11. Test of Hypothesis Two

Statistic	Value
Standardized beta (β)	0.29
t-value	6.42
p-value	< .001
Decision	Reject H02

H02 was rejected. Linear regression indicated a statistically significant positive relationship between technology adoption and security effectiveness ($\beta = .29$, $t = 6.42$, $p < .001$).

Table 12. Test of Hypothesis Three

Statistic	Value
Standardized beta (β)	0.31
t-value	6.88
p-value	< .001
Decision	Reject H03

H03 was rejected. Regression analysis indicated a statistically significant positive relationship between security funding and security effectiveness ($\beta = .31$, $t = 6.88$, $p < .001$).

Table 13. Test of Hypothesis Four

Statistic	Value
Standardized beta (β)	0.27
t-value	5.95
p-value	< .001
Decision	Reject H04

H04 was rejected. Personnel training had a statistically significant positive relationship with security effectiveness ($\beta = .27$, $t = 5.95$, $p < .001$).

Table 14. Test of Hypothesis Five

Statistic	Value
Pearson correlation (r)	0.34
t-value	7.72
p-value	< .001
Decision	Reject H05

H05 was rejected. Pearson correlation analysis showed a statistically significant positive relationship between collaboration with external security agencies and security management effectiveness ($r = .34$, $p < .001$).

5. Discussion

The findings indicate that selected polytechnics rely substantially on physical infrastructure and human security personnel. This pattern is consistent with Routine Activity Theory because perimeter walls, controlled access points, patrols, and security personnel provide forms of capable guardianship. The comparatively lower rating for emergency preparedness suggests that the presence of guardianship does not necessarily translate into equally strong response capacity.

The overall effectiveness rating of 3.49 indicates that respondents generally considered the existing arrangements effective. Protection of lives and property received the highest rating, while emergency response recorded the lowest. This difference is important because effective security management involves not only preventing unauthorized access but also the capacity to communicate, mobilize, and respond when an incident occurs.

The technology findings show a distinction between established technologies and more advanced systems. CCTV, biometric systems, and basic cybersecurity recorded moderate utilization, whereas artificial intelligence, IoT systems, and drones recorded low utilization. This pattern suggests that technology adoption is uneven and that advanced applications remain less integrated into campus security operations. The finding is consistent with the study's emphasis on funding, infrastructure, and personnel capacity as enabling conditions for technology use.

Inadequate funding was the highest-rated implementation challenge. This finding is consistent with the observation that limited resources can affect equipment maintenance, personnel development, power availability, and the acquisition of newer security technologies. The relationship between funding and effectiveness was also statistically significant in the hypothesis test ($\beta = .31$, $t = 6.88$, $p < .001$).

The regression model provides evidence that the combined security management practices were significantly associated with perceived campus safety. The model explained 42% of the variance in the dependent variable, with $R^2 = .42$ and adjusted $R^2 = .41$. The overall model was statistically significant, $F(6, 455) = 54.91$, $p < .001$. Because the analysis is based on survey data and the design is descriptive, these relationships should be interpreted as statistical associations rather than proof of causation.

Collaboration with external security agencies was also statistically significant ($r = .34$, $p < .001$), while the descriptive results showed high overall collaboration. Nevertheless, the lower rating for joint training and capacity building compared with information sharing and communication indicates that collaboration may be stronger in routine communication than in systematic preparedness and joint professional development.

Taken together, the findings support a layered approach to campus security in which physical controls, personnel, technology, institutional policies,

emergency preparedness, and external collaboration are treated as interconnected components. This interpretation is consistent with contemporary security-management principles and the study's theoretical framework.

6. Managerial and Policy Implications

Polytechnic managers should treat security as an integrated institutional management function rather than as a narrow guarding activity. Planning should connect infrastructure, personnel, technology, emergency response, information management, and external partnerships.

Security budgets should be aligned with identified operational needs, including equipment maintenance, personnel training, power reliability, ICT infrastructure, and technology upgrades. The findings provide empirical support for treating funding as a central component of security management.

Technology investments should be accompanied by personnel development and maintenance arrangements. The low utilization of AI, IoT, and drone technologies indicates that technology acquisition alone would not address security gaps without the institutional capacity to operate and sustain such systems.

Inter-agency collaboration should move beyond routine communication toward structured joint training, emergency coordination, information sharing, and preparedness exercises. Such arrangements can strengthen institutional capacity while maintaining clear roles and responsibilities.

7. Conclusion

Based on the findings, the selected polytechnics have established basic physical security measures and personnel deployments, and respondents generally perceive these arrangements as effective. However, the effectiveness of campus security is constrained by inadequate funding, shortages of trained personnel, obsolete equipment, unstable electricity, ICT limitations, and relatively low utilization of advanced security technologies. The regression analysis shows that the combined security management practices explain 42% of the variance in perceived campus safety, with a statistically significant overall model, $F(6, 455) = 54.91$, $p < .001$. The hypothesis tests also show statistically significant relationships involving technology adoption, funding, personnel training, and external collaboration. The findings therefore support a coordinated, layered security-management approach.

8. Recommendations

1. Polytechnic management and relevant funding bodies should establish dedicated security budgets that support equipment modernization, infrastructure maintenance, emergency preparedness, and technology integration.
2. Institutions should progressively modernize security systems by integrating appropriately selected CCTV networks, biometric access controls, automated visitor management, and other technologies suited to institutional needs and available infrastructure.
3. Security units should implement regular training in intelligence gathering, emergency response, crisis management, communication, and technology operation.
4. Polytechnics should formalize collaboration with relevant external security agencies through structured coordination mechanisms, joint training, intelligence sharing, and emergency-response exercises.
5. Host-community engagement should be incorporated into institutional security planning through regular communication and appropriate local information channels.

9. Limitations of the Study

The study used a descriptive survey and mixed-methods approach across selected polytechnics. The findings therefore reflect the perceptions and experiences represented in the sampled institutions and should not automatically be generalized to every tertiary institution in Northern Nigeria. In addition, the regression findings establish statistical associations rather than causal effects. Future research may incorporate longitudinal designs, incident records, comparative institutional data, and broader geographic coverage.

REFERENCES :

- Adebayo, O., & Abdulhamid, S. M. (2014). E-Exams system for Nigerian universities with emphasis on security and result integrity. arXiv. https://arxiv.org/abs/1402.0921
- American Psychological Association. (2020). Publication manual of the American Psychological Association (7th ed.). American Psychological Association.
- ASIS International. (2022). Protection of assets: Security management handbook. ASIS International.
- Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide. Sage.

- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608.
- Creswell, J. W., & Creswell, J. D. (2023). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). Sage.
- Federal Emergency Management Agency. (2021). Guide for developing high-quality emergency operations plans for institutions of higher education. FEMA.
- Federal Republic of Nigeria. (2013). National policy on education (6th ed.). NERDC Press.
- Field, A. (2024). Discovering statistics using IBM SPSS Statistics (6th ed.). Sage.
- Institute for Economics & Peace. (2024). Global terrorism index 2024: Measuring the impact of terrorism. IEP.
- International Association of Campus Law Enforcement Administrators. (2023). Standards and best practices for campus public safety. IACLEA.
- Iwuamadi, C. K., & Akuakanwa, E. O. (2024). Technological innovations and campus security management in public tertiary institutions in South-East Nigeria. Journal of Educational Administration and Policy Studies, 16(1), 22–35.
- Kothari, C. R. (2004). Research methodology: Methods and techniques (2nd ed.). New Age International.
- National Bureau of Statistics. (2024). Crime statistics publication 2023. NBS.
- National Board for Technical Education. (2023). Guidelines for the administration of polytechnics in Nigeria. NBTE.
- National Institute of Standards and Technology. (2024). Cybersecurity framework (Version 2.0). NIST.
- Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.
- Ogunode, N. J., & Musa, A. (2023). Security challenges in Nigerian tertiary institutions: Implications for educational administration. International Journal of Development and Public Policy, 3(2), 11–24.
- Olanipekun, S. O., et al. (2024). Campus safety arrangements and administrative efficiency in Nigerian higher education. Educational Planning and Practice, 12(1), 45–58.
- OECD. (2023). OECD digital education outlook 2023: Push conditions and modern technologies. OECD Publishing.
- UNESCO. (2021). Education under attack 2021. UNESCO.
- UNESCO. (2022). Protecting educational institutions from attack: Global synthesis report. UNESCO.
- UNESCO. (2023). Ensuring safe learning environments: Global guidance for education systems. UNESCO.
- UNICEF. (2023). The impact of conflict and insecurity on children's education in West and Central Africa. UNICEF.
- United Nations Development Programme. (2022). Human development report 2021/2022. UNDP.
- World Bank. (2022). Nigeria development update: Responding to economic and security shocks. World Bank.