Al-Hikmah Journal of Pure and Applied Sciences
©2025
Volume: (5) Special Issue (1): 1-11

A Statistical Evaluation Of Artificial Intelligent (AI) And Big Data Analytics On National Security Performance Indicators In Nigeria: A Simulation-Based Analysis

[1]Alanamu, T., [2]Adetunji, K.O., [3]Muhammed M.O., [3]Adefila E.J. and [4]Adeyemi, B.T.

[1,2,3,]*Department of Mathematics, Kwara State College of Education, Ilorin, Nigeria.*
[4]*Department Computer, Kwara State College of Education, Ilorin, Nigeria*

ARTICLE INFO

Article history

Received: 01/12/2025
Revised: 16/12/2025
Accepted: 23/12/2025

Doi:
https://doi.org/10.5281/zenodo.18064443

Keywords:

Artificial intelligence,
Big data analytics,
National security,
Simulation
Modelling,
Operational performance.

Corresponding Author

Email:
taoheedatalanamu@yahoo.com

Phone:+234 8064002089

ABSTRACT

The rise in the security threats in Nigeria calls for the adoption of advanced technological systems capable of improving detection accuracy, cyber resilience, and operational responsiveness. While Artificial Intelligence (AI) and Big Data Analytics (BDA) are widely promoted as transformative tools for modern security operations, direct empirical evaluation within Nigeria remains constrained by restricted access to sensitive operational data. This study therefore adopts an operationally grounded simulation approach to examine how AI and BDA could influence key national security performance indicators. Using parameters that are informed by documented Nigerian security practices, policy frameworks, and international benchmarks, 180 paired observations were simulated to represent operational performance pre and post-AI integration across five selected indicators: threat detection accuracy, response time, cyber-attack interceptions, false alarm rates, and a composite operational efficiency index. The model outputs suggest that AI-enabled systems are associated with considerable improvements across all indicators under plausible institutional conditions. Although the findings are derived from simulated data, they are empirically anchored in real operational contexts and provide structured perception into how AI adoption could reform security performance in Nigeria. The study contributes a methodological bridge between empirical constraints and policy-relevant analysis, offering a foundation for pilot implementation and also future empirical validation.

Citation: Alanamu, T., Adetunji, K.O., Muhammed, M.O., Adefila, E.J. and Adeyemi, B.T. (2025). A Statistical Evaluation Of Artificial Intelligent (AI) And Big Data Analytics On National Security Performance Indicators In Nigeria: A Simulation-Based Analysis. *AJPAS.* 5: 1-12

1.0 Introduction

Africa's most populous country and with largest economy; Nigeria, faces a series of security challenges, ranging from terrorism and insurgency to cybercrime and communal conflicts to sophisticated digital threats [8]. There are pressing demands for a shift from traditional intelligence systems to technology-enhanced national security operations, due to rise in security threats ranging from terrorism, insurgency, cybercrime, transnational banditry, and organised criminal networks [2]. Today, there are enormous volume of data being faced by National security agencies from a variety of sources; surveillance systems, digital communications, social media, and cyber networks. When relying on traditional intelligence methods, detecting and responding so quickly to threats has become more difficult

The daily challenge of national security in the digital age has being on the increase, the threats are multiplying and becoming more complicated. Between 2018 and 2024, Nigeria saw an increase in security incidents, with kidnappings alone estimated at 2,235,954 between May 2024 and April 2024 [16]. Traditional intelligence methods simply can't keep pace with this scale of data, with the increase in the Nations level of reliance on Artificial Intelligence (AI) and Big Data Analytics (BDA). But with utilizing AI and big data, security organizations can identify potential threats.

In practical terms, Nigerian security agencies operate within an information-rich yet analytically constrained environment. Institutions such as the Nigeria Police Force, the Department of State Services, the Armed Forces, and cyber-focused agencies under the Office of the National Security Adviser generate and receive vast amounts of data from surveillance systems, telecommunications records, financial intelligence units, border monitoring platforms, and open-source intelligence. However, the extent of integrating, analysing, and acting upon these data streams remains uneven. Some of the challenges that continue to slow Intelligence cycles and constrain timely response are fragmented databases, limited analytic infrastructure, skills gaps, and inter-agency coordination.

Despite all odds, Artificial Intelligence and Big Data Analytics have globally emerged as prominent tools for addressing these kinds of analytic bottlenecks. AI-driven systems are increasingly deployed to support pattern recognition, predictive analysis, anomaly detection, and decision support within security and defence institutions. Big Data Analytics enables the integration of heterogeneous data sources, allowing security agencies to move beyond reactive responses toward more anticipatory and preventive strategies. In technologically advanced security environments, these tools have been associated with improvements in detection accuracy, response speed, and resource allocation.

In Nigeria, interest in data-driven security solutions has steadily grown, reflected in national digital economy strategies, cybersecurity policies, and institutional reforms aimed at strengthening intelligence coordination. Yet, the translation of these strategic aspirations into operational capability has been uneven. While pilot initiatives and isolated deployments exist, comprehensive AI-enabled security architectures remain limited. More importantly, systematic empirical evaluation of AI's impact on national security performance in Nigeria is constrained by restricted access to sensitive operational data and the classified nature of security operations.

This empirical constraint poses a significant challenge for researchers and policymakers. Behind the adoption of Artificial Intelligence and Big Data Analytics in security governance, there is strong normative and policy-driven momentum. On the other hand, the absence of accessible operational data limits the ability to rigorously assess performance impacts using empirical methods. In this context, simulation-based modeling offers a practical methodological alternative. By making assumptions clear and established parameters in documented institutional practices and policy benchmarks, simulation allows for structured exploration of reasonable outcomes without misrepresenting model outputs as observed reality.

This study is situated within this methodological space. Rather than measuring impacts of AI adoption, it develops an operationally grounded simulation model to examine how Artificial Intelligence and Big Data Analytics could reasonably influence selected national security performance indicators in Nigeria. The indicators considered are threat detection accuracy, response time, cyber-attack

interception, false alarm rates, and operational efficiency index. Each indicator reflects performance dimensions routinely referenced in security assessments and policy discourse [17].

Adopting this approach, the study seeks to contribute in three major ways. First, by bridging the gap between empirical constraint and policy relevance in national security research through the provision of a transparent modeling framework. Second, it offers context-sensitive perception into how data-driven technologies might connect with existing institutional structures within Nigeria's security architecture. Third, it generates structured expectations that can inform sample deployments, capacity-building efforts, and future empirical research as data access improves.

The existing literature on Artificial Intelligence, Big Data Analytics, and security performance are review in next section, with particular attention to developing and data-constrained contexts. This is followed by description of the simulation methodology and parameterization. The results section presents the statistical outputs generated by the model, while the discussion interprets these outputs within institutional and policy contexts.

1.1 Statement of the Problems

Nigeria security agencies continue to rely heavily on traditional, manual intelligence systems that are slow, disconnected, and reactive, despite increased in the country's security threats (terrorism, cybercrime, banditry, kidnapping, and cross-border crimes), The growing volume of digital data from mobile phones, social media, CCTV cameras, banking transactions, satellite imagery, and communication networks has affected existing analysis capabilities. Thereby, causing grave threats to often go undetected until after major damage has occurred. Although Artificial Intelligence (AI) and Big Data Analytics have globally proven effective for real-time threat detection, Nigeria's level of adoption, readiness, and actual impact still remain unclear.

1.2 Research Questions

1. To what extent does AI adoption improves key national security operational indicators in Nigeria?
2. What is the relationship between the level of AI adoption and overall operational efficiency in Nigeria's national security system?
3. Does operational efficiency differ across different levels of AI adoption power within Nigeria's national security operations?

1.3 Research Hypotheses

H_{o1}: There is no significant difference in key national security operational indicators before and after AI adoption in Nigeria

H_{o2}: There is no significant relationship between AI adoption and operational efficiency

H_{o3}: There is no significant difference in operational efficiency across levels of AI adoption intensity

1.3 Artificial Intelligence in National Security

Artificial Intelligence comprises computational systems capable of performing cognitive tasks such as pattern recognition, classification, prediction, and automated decision support [24]. In security operations, AI technologies include: predictive threat analytics, automated video surveillance, biometric and facial recognition, cyber-intrusion detection systems, anomaly detection in large datasets.

AI never gets tired, unlike humans that get tired, miss details, or make mistakes under pressure. By handling monitoring tasks (like scanning CCTV footage or filtering suspicious online activity) that are repetitive, AI frees human officers to focus on judgment and decision-making. Useful insight may be extracted by security agencies from large datasets to find patterns, spot abnormalities, and foresee possible threats by utilizing AI and big data analytics. AI, AI significantly improves operational

readiness, enables rapid data processing and enhances precision in detecting threats that may be difficult for human operators to identify [12].

Studies from technologically advanced nations show that AI significantly boosts national security performance. A 70% increase in real-time threat detection was reported by the U.S. Department of Homeland Security following AI deployment [6]. Israel's counterterrorism operations show improved precision through machine-learning-supported surveillance [25]. AI-driven intrusion detection uses by NATO reduces false alarms by more than half [17]. AI systems are not neutral tools; they embed assumptions and can reproduce existing biases if deployed uncritically.

1.4 Big Data Analytics in Security Operations

The term Big Data refers to large-scale information management and analysis technologies that exceed the capability of traditional data processing technologies [4]. Big Data analytics is the process of analyzing and mining Big Data, it can produce operational and business knowledge at an unprecedented scale and specificity [4].

Big Data Analytics involves techniques for analysing large, complex, and rapidly changing datasets to reveal hidden patterns and produce actionable insights [11]. Data originating from surveillance systems, telecommunications, cyber logs, social media intelligence, and crime databases are being relied on by Security agencies. Criminal pattern recognition, risk profiling, behaviour prediction, cyber-threat modeling, and real-time intelligence dissemination are all being assisted by BDA. For effective threat monitoring and situational awareness, the integration and analysis of these diverse data sources is widely regarded as essential.

The use of big data analytics to fight terrorism, insurgency, cyber threats, and other illegal activities gives a judicious advantage in Nigeria where we have varying and ever-changing security issues [21]. These potentials make it possible to minimise guesswork and improve precision in national security decisions [26].

AI and Big Data give Nigeria's security agencies the ability to spot danger earlier, connect the dots faster, and respond in smarter ways. Instead of being caught off guard, they can prepare, protect, and prevent. Lack of access to real-life data on security limits rigorous assessment [6] [7] [17]. However, scholars caution that data abundance does not automatically translate into analytic insight. Big Data initiatives can overwhelm institutions rather than enhance performance if adequate infrastructure, skilled personnel, and governance frameworks are not put in place.

1.5 Artificial Intelligence, Big Data, and Security in Developing Contexts

While much of the existing literature on AI and Big Data in security is drawn from technologically advanced contexts, a growing body of work examines their application in developing and data-constrained environments. These studies emphasise that institutional capacity, regulatory frameworks, and resource availability play a decisive role in shaping outcomes. In many developing countries, security agencies face fragmented data systems, limited analytic capacity, and uneven technological adoption.

Intelligence integration, cyber resilience, and inter-agency coordination are some of the challenges being pointed at by policy reports and institutional assessments in Nigerian context. Although national strategies increasingly reference digital transformation and data-driven security, implementation remains uneven. The literature suggests that gradual adoption, targeted pilot programmes, and context-sensitive modeling may be more appropriate than mass technology transfer.

1.6 Simulation and Modelling in Security Research

Simulation-based modelling holds an important place in security and defence research, especially where access to real operational data is restricted. Rather than serving as a replacement for empirical observation, simulations function as exploratory fact-finding tools that allow researchers to examine system behaviour under explicitly stated assumptions. This approach is especially valuable in national security research, where confidentiality constraints on data limits the availability.

As emphasized in methodological studies, transparent parameter selection and ground real operational contexts are being dependent upon by the credibility of simulation-based research. Models that are detached from institutional realities risk producing abstract or misleading conclusions. Conversely, operationally informed simulations can provide useful insight into reasonable system dynamics and support evidence-informed policy dialogue.

1.7 Gaps in the Existing Literature

Despite the growing attention to studies on AI and Big Data, several gaps remain. First, there is limited work that patently links AI-enabled analytics to measurable multiple performance indicators within national security systems, mostly in developing contexts. Second, few studies attempt to bridge empirical constraints through simulation frameworks that are transparently grounded in institutional realities. Finally, few studies assesses AI's operational impact on Nigeria's security indicators, causing under-representation of the Nigerian security context in systematic and methodologically explicit analyses of data-driven security transformation.

This study responds to those gaps by developing a simulation model that is operationally grounded and explores how Artificial Intelligence and Big Data Analytics could plausibly influence national security performance indicators in Nigeria.

2.0 Materials and Method

2.1 Research Design

The research design adopted by the study is a quasi-experimental, simulation-based design. Two operational conditions were being modeled: a baseline pre-AI condition representing conventional security operations, and a post-AI condition showing the integration of AI and Big Data Analytics into analytic and response processes.

Due to limited access to sensitive operational datasets (which is a common challenge in security research), simulation was used [25]. This approach aligns with best practice in national security research, where simulation-based analytics are widely used to evaluate system performance under controlled conditions. Without compromising national security protocols, simulation enables measurable and testable outcomes, when real intelligence data remain confidential and unavailable.

This study provides a replicable framework for future research where real life data cannot be accessed publicly on national security, using simulation to model classified data

3.2 Operational Grounding and Parameterisation

By the combination of Nigerian policy documents, institutional reports [18], and international security benchmarks [6], [7], [17], simulation parameters were informed. Baseline performance levels used were aligned with documented challenges in threat detection, response coordination, and cyber defense reported by Nigerian security agencies and regulatory bodies. International benchmarks were used cautiously as upper-bound references rather than direct comparators.

Parameter shifts for the post-AI condition were deliberately conservative. The modeling choice reflects the reality that AI adoption in Nigeria is likely to be incremental, uneven across agencies, and shaped by infrastructure and capacity constraints. This decision prioritises plausibility over statistical contrast.

The pre-AI condition represents traditional largely manual operations, which is consistent with the operational realities of many country's security agencies; Nigeria as a developing country inclusive. Below is the table of mean and standard deviation for pre-AI data simulation

Table 1: Mean and standard deviation used to generate for Pre-AI security performance data

Variables	Mean(μ)	Standard deviation(δ)	Distribution	Source
Threat Detection Accuracy (%)	42.11	8.50	Normal	[7] [18]
Response time(minutes)	92.44	18.30	Normal	[6] [10]
Cyber- Attack Interceptions (count)	210.87	14.52	Poisson	[18] [4]
False Alarm Rate (%)	27.22	6.70	Poisson-Normal Approximation	[7]
Operational Efficiency Index	0.00	1.00	Standard Normal	[9] [22]

Normal distribution parameters with means and standard deviation reflecting pre-AI performance indicators in Nigeria security systems were used to generate the baseline (pre-AI). This is consistent with simulation practices in applied security analytics [9], [7], [18].

3.2.1 Intervention Model

The structure of the intervention model follows a Pretest-Posttest Simulation Framework. It is expressed as $O_1 \rightarrow X \rightarrow O_2$, where

O_1 is the security performance indicators pre-AI Adoption

X is the AI intervention

O_2 is the security performance indicators post-AI Adoption

With operational pathway of the intervention as grounded in information processing theory [8] as AI Adoption→Balanced information processing→ improved decision quality →operational performance gains.

3.2.2 Model representation [10] [7] [6][9]

$Y_{it} = \propto + \beta AI_t + \varepsilon_{it}$, where

Y_{it} =Security performance indicator ^{i} at time t

AI_t=Binary intervention variable (0=pre-AI, 1 = post-AI)

β =estimated effect of AI intervention

ε_{it} = error term

3.2.3 Assumptions

- Data availability constraint[8][23]
- Baseline performance validity[6][18]
- Distributional assumption[9][3]
- AI directional effect assumption[10][7][6]
- Mean shift assumption[10][9]
- Indicator independence assumption[12]
- Variance reduction assumption
- Homogeneity assumption of intervention[25]
- Sample representative assumption
- Statistical test assumption[3]

The study operates under many assumption that could influence the outcome.

3.3 Simulated Dataset and Procedure

180 paired observations in total were simulated across all indicators, representing performance pre and post-AI integration. Data were drawn from normal distributions using parameters derived from established ranges as reported in Nigeria security literature, performance indicators and global cyber defence framework from [6], [7], and [17]. The indicators include: threat detection accuracy, response time, cyber-attack interceptions, false alarm rate, and operational efficiency index. Realistic means and standard deviations were embedded to replicate actual operational environments. The indicators selected reflect the performance measures used by:

The Nigeria Police Force (NPF) for monitoring response time and threat detection during patrols and emergency dispatches, the Department of State Services (DSS) for intelligence screening and false alarm reduction, the Office of the National Security Adviser (ONSA) and ngCERT for cyber-attack interception and digital threat monitoring, the Armed Forces of Nigeria (AFN) for operational coordination and efficiency assessments. Thus, the variables represent measurable performance outcomes that Nigerian agencies actively track or should track under Nigeria's National Cyber security Policy and Strategy (NCPS, 2021).

3.3 Variables and Measurement

The independent variable was AI adoption, operationalised as pre- and post-integration conditions and as ordinal adoption intensity levels. Dependent variables included threat detection accuracy, response time, cyber-attack interceptions, false alarm rate, and a composite operational efficiency index. Each indicator corresponds to performance metrics routinely referenced in Nigerian security operations and cybersecurity assessments [6] [7] [17].

3.0 Result (Simulation Output)

This section presents the statistical outputs generated by the simulation model. All results reported here are derived from simulated data parameterized using operationally grounded assumptions. They illustrate how performance indicators respond under specified AI adoption and not represent observed security operations but illustrate how performance indicators respond scenarios.

3.1 Descriptive Statistics

Table 2: Descriptive Statistics of Security Performance Indicators Pre and Post-AI Adoption.

Indicator	Before AI (Mean)	After AI(Mean)
Threat Detection Accuracy (%)	42.11	78.63
Response Time (Minutes)	92.44	41.27
Cyber-Attack Interceptions	210.87	529.33
False Alarm Rate (%)	27.22	9.83
Operational Efficiency Index	-	0.71

Across all indicators, higher detection accuracy was exhibited by the post-AI condition, as well as greater cyber-attack interception, lower response time, reduced false alarm rates, and improved composite efficiency. These differences reflect the structural assumptions immersed in the simulation rather than measured operational change.

3.2 Paired Sample t-Tests

Within the simulation, paired sample t-tests were conducted to examine whether observed mean differences between pre-AI and post-AI conditions are statistically distinguishable. The results are as presented in Table 3.

Table 3: Result of paired samples t-Test for pre and post-AI operational metrics

Indicator	Mean Difference	T	Df	p-value
Threat Detection Accuracy	+36.52	14.21	179	< 0.001
Response Time	–51.17	11.45	179	< 0.001
Cyber-Attack Interceptions	+318.46	16.33	179	< 0.001
False Alarm Rate	–17.39	9.72	179	< 0.001

All paired comparisons indicate statistically significant differences in the expected direction. These results only demonstrate internal statistical separation between the two simulated conditions, but should not be interpreted as empirical causal effects.

3.3 Correlation Analysis

Pearson correlation coefficients were determined to examine relationships between AI adoption intensity and performance indicators.

Table 4: Pearson correlation analysis between AI adoption and operational efficiency

Variables	AI Adoption Score	Operational Efficiency
AI Adoption Score	-	.63
Operational Efficiency	.63	-

Note. P-value < .01

Higher levels of simulated AI adoption are associated with improved security performance indicators and reduced inefficiencies, as indicated by the result. The results align with theoretical expectations. These relationships reinforce the internal consistency of the model without implying empirical validation.

3.4 Analysis of Variance (ANOVA)

One-way ANOVA tests were conducted to assess performance differences across varying levels of AI adoption intensity. Where AI adoption was modelled at three levels: low, moderate, and high integration.

Table 5: One-Way Analysis of Variance (ANOVA) results for efficiency across all levels of AI Adoption

Source	SS	df	MS	F	p-value
Between Groups	1.832	2	0.916	13.47	< 0.001
Within Groups	12.098	177	0.068		
Total	13.930	179			

The results indicate statistically significant differences across AI adoption levels for all indicators. Post-hoc test reveals a repetitive pattern, as performance improves incrementally as AI integration intensity increases.

4.0 Discussion

Using an operationally grounded simulation framework, the study examines how Artificial Intelligence and Big Data Analytics could plausibly influence some selected national security performance indicators within the Nigerian context. The statistical outputs are cautiously interpreted, pointing out the fact that they are generated under stated assumptions rather than derived from observed operational data. The emphasis, therefore, is not on empirical verification, but understanding directional tendencies, institutional implications, and policy relevance. The simulation outputs suggest

that AI-enabled analytic systems are associated with notable improvements in threat detection accuracy and cyber-attack interception rates.

The observed decline in false alarm rates under the post-AI condition further highlights the potential value of data-driven systems. High false alarm rates place a very significant strain on limited operational resources and can ruin the confidence in intelligence systems. By modelling AI-assisted filtering and cross-validation of data sources, the simulation suggests a plausible pathway through which analytic precision could improve.

Beyond individual indicators, the composite operational efficiency index captures the cumulative effect of these simulated improvements. The increase in this index reflects not a single transformative gain but the interaction of modest enhancements across multiple operational dimensions. This aligns with the reality that security performance improvements are often incremental and system-wide rather than dramatic and isolated. The ANOVA results indicate that performance gains follow a consistent pattern across varying levels of AI adoption, rather than being an artefact of a simple pre- and post-AI dichotomy. Correlation analysis reveals relationships that align with theoretical expectations.

The parameters used, although grounded in policy documents and operational reports, cannot fully capture informal practices, political constraints, or adaptive behaviour by adversaries; these happen to be the limitation of the study. As suggested by the model, the findings should not be interpreted as evidence that AI adoption will automatically yield the improvements. Real-world outcomes will depend on human capacity, organisational culture, legal frameworks, and sustained investment.

However, under plausible conditions, the study offers a structured way of thinking about how AI and Big Data Analytics could interact with existing security systems. By making assumptions explicit and results transparent, the model provides a useful starting point for pilot studies, controlled trials, and mixed-methods research. In this sense, the contribution of the study lies not in prediction but in informed exploration, supporting evidence-based dialogue on the future of data-driven national security in Nigeria.

5.0 Conclusion and Recommendation

Using an operationally grounded simulation framework, this study set out to examine how Artificial Intelligence and Big Data Analytics could plausibly influence national security performance indicators in Nigeria. The study deliberately adopted a modelling approach that balances analytical rigor with methodological caution in a context where access to detailed security data is restricted. The objective was not to claim empirical measurement of impact, but to provide a structured and transparent exploration of how data-driven technologies might interact with existing security systems under realistic institutional conditions.

Importantly, the findings should not be interpreted as evidence that AI and Big Data Analytics will automatically yield the improvements suggested by the model. Real-world outcomes will depend on a range of factors that extend beyond technology itself, including data quality and human capacity. Without sustained investment in these supporting conditions, the potential benefits of AI systems may remain unrealized or unevenly distributed across security institutions.

The study also underscores the risks associated with uncritical adoption of automated analytic tools. Issues such as algorithmic bias, system vulnerability, and over-reliance on machine-generated outputs pose genuine challenges for national security governance. These concerns reinforce the need for strong oversight mechanisms, continuous evaluation, and the retention of human judgement at the centre of security decision-making.

Despite these limitations, the modelling framework developed in this study provides a useful foundation for future research and policy experimentation. It offers a means of generating informed expectations, identifying priority areas for pilot deployment, and designing empirical studies that can test specific components of AI-enabled security systems as data access improves. In this sense, the study contributes not definitive answers, but a disciplined way of asking the right questions about the role of Artificial Intelligence and Big Data Analytics in Nigeria's evolving security architecture.

In conclusion, while simulation-based analysis cannot substitute for empirical evaluation, it remains a valuable tool in data-constrained environments. By combining methodological transparency, operational grounding, and cautious interpretation, this study put forward understanding of how emerging technologies might shape national security performance in Nigeria. It is hoped that the perceptions offered here will support evidence-informed dialogue, responsible innovation, and future empirical inquiry into data-driven security governance.

Declaration of generative AI and AI assisted technologies in the writing process

To improve readability and language, the authors used AI tool for editing the content during the preparation of this paper. We hereby declare that we have reviewed and edited the content as required and take full responsibility for the content of the paper.

Reference

1. Afolabi, T., & Omotola, J. (2022). Digital capacities and the future of Nigeria's security operations. *African Security Review, 31*(2), 145–159.
2. Adegboyega, L. (2022). Contemporary security threats in Nigeria: Challenges for internal security management. *Journal of Security Studies, 14*(1), 33–48.
3. Cameron, A. C., & Trivedi, P. K. (2013). *Regression analysis of count data* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139013567
4. Cloud, R. (2013). Big data: Issues, challenges, tools, and good practices. In *Proceedings of the International Conference on Emerging Trends & Applications in Computer Science* (pp. 404–409).
5. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.
6. Department of Homeland Security. (2022). *Artificial intelligence applications in homeland security*. U.S. Department of Homeland Security.
7. Europol. (2021). *European Union security annual report*. Europol Publications Office.
8. Federal Government of Nigeria. (2019). *National security strategy of the Federal Republic of Nigeria*. Office of the National Security Adviser.
9. Field, A. (2018). *Discovering statistics using SPSS* (5th ed.). Sage.
10. Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces, 4*(3), 28–36.
11. Katal, A., Wazid, M., & Goudar, R. (2013). Big data: Issues, challenges, tools and good practices. In *Emerging trends & applications in computer science* (pp. 404–409). IEEE.
12. Law, A. M. (2015). *Simulation modeling and analysis* (5th ed.). McGraw-Hill Education.
13. Li, X., & Zhao, H. (2021). Machine learning for intelligent security surveillance: A review. *Expert Systems, 38*(2), e12645.
14. Lim, K., Tan, J., & Wong, Y. (2021). Smart city emergency response: Big data analytics for crisis management in Singapore. *Journal of Urban Technology, 28*(1), 55–73.
15. Ministry of Defence. (2022). *Defence artificial intelligence strategy*. Government of the United Kingdom.
16. Moyo, M. (2020). Emerging technologies in Africa's security landscape. *African Journal of Criminology, 8*(1), 79–95.
17. National Bureau of Statistics. (2024). *Crime statistics: Kidnapping, homicide, and armed robbery report (May 2023–April 2024)*. NBS.
18. NATO. (2021). *Cyber defence enhanced by artificial intelligence*. NATO Cooperative Cyber Defence Centre of Excellence.
19. National Information Technology Development Agency. (2022). *Nigeria cyber threat landscape report*. NITDA.
20. Okoro, E., & Odoemelam, C. (2021). Digital transformation challenges in Nigeria's security agencies. *International Journal of Security Studies, 9*(2), 88–104.
21. Onifade, C., & Ogunleye, R. (2021). Limitations of traditional intelligence gathering in Nigeria. *Journal of Peace and Conflict Studies, 6*(3), 102–119.

22. Onazi, P., Musa, A., & Shittu, Y. (2025). Big data analytics and national security intelligence in Nigeria. *Nigerian Journal of Security Studies, 12*(1), 44–61.
23. Pallant, J. (2020). *SPSS survival manual* (7th ed.). McGraw-Hill Education.
24. Provost, F., & Fawcett, T. (2013). *Data science for business*. O'Reilly Media.
25. Russell, S., & Norvig, P. (2020). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
26. Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Houghton Mifflin.
27. Shapiro, B. (2021). AI-enabled counterterrorism systems: Evidence from Israel. *Security Informatics, 10*(1), 1–12.
28. Wang, Z., & Liu, Y. (2020). Big data policing and predictive models: Evidence from China. *Policing and Society, 30*(6), 639–654.