International Journal of Innovative Finance and Economics Research 14(3):389-399, July-Sept, 2026
© SEAHI PUBLICATIONS, 2026 www.seahipublications.org ISSN: 2467-8473

DOI:10.5281/zenodo.22051672

Defence Procurement, Digital Accountability And Operational Readiness In Nigeria: Bridging The Acquisition-To-Battlefield-Effect GAP

[1]Chukwuemeka Ifegwu Eke, PhD
&
[2]Rear Admiral Sulaiman Haruna Abdullahi Psc+, RCDS, DSS, FCILT, FACSSM, FOSHA

[1]Department of Economics, University of Abuja, Abuja, Nigeria
chukwuemeka.eke@uniabuja.edu.ng | 08037889103

[2]Chief of Logistics, Naval Headquarters, Nigeria

ABSTRACT
Nigeria has devoted substantial public resources to defence acquisition in response to terrorism, insurgency, armed banditry, kidnapping, piracy and other violent threats. Yet the possession of newly acquired platforms, weapons, communication systems, vehicles, vessels and surveillance assets does not automatically translate into operational effectiveness. The decisive issue is whether appropriated funds and acquired equipment are converted into serviceable, deployable and sustainable military capability. This paper examines defence procurement as an integrated capability system involving threat assessment, budgeting, contracting, delivery, acceptance testing, training, maintenance, logistics, interoperability, digital communication and battlefield deployment. It argues that Nigeria faces an acquisition-to-battlefield-effect gap in which equipment may be purchased and formally delivered but remain unavailable, poorly supported, technically incompatible, inadequately crewed or disconnected from real-time intelligence and operational requirements. The paper develops a digital accountability framework linking procurement records, lifecycle costing, vendor performance, inventory, serviceability, spare-parts availability, personnel training and theatre-level readiness indicators. It further proposes a simple capability-conversion model showing that defence expenditure affects readiness through the combined influence of maintenance, training, logistics, interoperability, digital command systems and institutional accountability. The analysis demonstrates that legitimate secrecy and accountability are not mutually exclusive. Operational confidentiality can coexist with classified audit, parliamentary oversight, secure digital records and traceable internal controls. The paper concludes that procurement success should be measured not mainly by contract value or equipment count, but by serviceability, response time, deployment endurance, intelligence-to-action speed, force protection, territorial control and civilian protection.
Keywords: defence procurement, digital accountability, operational readiness, counterterrorism, armed banditry, lifecycle costing, logistics, Nigeria.

1. INTRODUCTION
Nigeria's contemporary security environment is complex, fluid and multidimensional (Adekoya et al., 2025). The Armed Forces are required to respond to insurgent groups, terrorist cells, armed bandits, kidnappers, pirates, oil thieves, violent separatist networks and other organised criminal actors. These

groups do not operate like conventional state armies (Ashe et al., 2026). They exploit forests, creeks, border communities, difficult terrain, informal economic networks and gaps in surveillance (Omar et al., 2025). They also change tactics rapidly, which means that procurement decisions based on static assumptions may become outdated before the acquired equipment is fully deployed (Salisu et al., 2026).

In such an environment, defence acquisition cannot be understood as the simple purchase of weapons or platforms. A helicopter, naval vessel, armoured vehicle or communication system becomes useful only when it is supported by trained personnel, fuel, ammunition, spare parts, maintenance facilities, secure data links and a clear operational doctrine. The mere physical presence of equipment is therefore different from actual capability. Equipment is an asset; capability is the dependable ability to use that asset at the required time, place and intensity to achieve a defined mission.

This distinction is particularly important in Nigeria because public debate often equates large defence budgets or newly commissioned equipment with improved security. Such a conclusion may be premature. Defence budgets may increase while equipment availability remains low. Contracts may be completed while operators remain insufficiently trained. Platforms may be delivered while maintenance contracts, secure communications, ammunition or software support are inadequate. In such cases, expenditure has produced acquisition outputs without producing corresponding operational outcomes.

Modern military operations are also increasingly digital. Surveillance platforms, satellite systems, unmanned systems, secure communications, electronic procurement, predictive maintenance and real-time command networks all depend on data. The speed with which reliable information moves from detection to decision and from action decision can determine mission success. Eke and Osi (2023) emphasise the importance of time in digital economic processes (Olayinka-Agboola, Ismail & Eke, 2025). In military operations, delayed intelligence, delayed reinforcement and delayed maintenance can have even more serious consequences because they directly affect lives, territory and national security.

The central argument of this paper is that Nigeria faces an acquisition-to-battlefield-effect gap. This gap is the distance between what is purchased and what becomes usable, sustainable and effective in operations. The gap may arise from weak requirement definition, poor contracting, delayed funding, inadequate acceptance testing, fragmented fleets, limited training, absence of spare parts, poor maintenance or weak digital integration (Ismail, El-Yaqub & Eke, 2025). A procurement system that ignores these connections may spend heavily without creating a proportionate increase in readiness.

The paper therefore proposes that defence procurement should be treated as a complete capability chain. This chain begins with threat assessment and requirement definition, continues through budgeting, contracting, delivery and acceptance, and extends into training, maintenance, logistics, deployment and mission evaluation. Every link matters. Failure at one stage can neutralise investment at other stages. The purpose of digital accountability is to make each stage visible to authorised decision-makers without exposing sensitive operational information to the public.

2. Problem Statement And Research Purpose

The main problem addressed in this study is the gap between defence appropriation and operational capability. Public discussion frequently compares nominal defence expenditure across years and assumes that higher spending should automatically lead to better security. That assumption is unreliable because nominal figures do not reveal how much of the budget was released, how much purchasing power was lost through inflation or exchange-rate depreciation, how efficiently contracts were executed, or how much of the delivered equipment remained serviceable after deployment.

A more useful diagnosis begins with readiness failures that can be observed and measured. These include low serviceability rates, prolonged equipment downtime, inadequate night-fighting capability, weak counter-improvised-explosive-device support, insecure communications, delayed reinforcement, insufficient casualty evacuation, poor surveillance coverage, inadequate fuel or ammunition, and dependence on foreign maintenance. These indicators are closer to operational reality than headline

expenditure figures because they show whether procurement has improved the ability of forces to perform assigned missions.

The paper asks four related questions. First, how should defence procurement be redesigned around changing threat-based capability requirements? Second, what institutional and digital mechanisms can reduce leakages and improve traceability? Third, how do maintenance, training, logistics and interoperability influence the relationship between acquisition and readiness? Fourth, what practical indicators should be used to measure whether procurement has produced a battlefield effect? These questions are deliberately linked because procurement performance cannot be understood by examining any one stage in isolation.

The purpose is to develop an integrated framework suitable for Nigeria's counterterrorism, anti-banditry, maritime-security and other internal-security operations. The framework separates resources, acquisition outputs, capability outcomes, operational outcomes and strategic effects. Funds released are resources. Equipment delivered represents acquisition output. Serviceability, trained crews and ammunition availability are capability outcomes. Response time and deployment endurance are operational outcomes. The disruption of violent networks, protection of civilians and restoration of normal activity are strategic effects.

This sequence prevents a common analytical error. Counting equipment purchased as evidence of readiness confuses an intermediate output with a final result. The purchase of ten vehicles does not show that ten vehicles are serviceable, properly crewed or available in theatre. Similarly, the delivery of a surveillance system does not prove that intelligence reaches operational units quickly enough to shape decisions. Procurement success must therefore be traced through the full chain from appropriation to mission effect.

3. CONCEPTUAL FRAMEWORK

Defence acquisition is the complete process through which military requirements are identified, defined, budgeted, procured, delivered, tested, supported, upgraded and eventually retired. It is much broader than purchasing. It includes needs assessment, research, technical specification, lifecycle costing, vendor selection, contracting, quality assurance, training, infrastructure, maintenance, software support, upgrades and disposal. A narrow purchasing approach focuses on delivery; a capability approach focuses on whether the delivered asset remains useful throughout its intended service life.

Operational readiness is the capacity of forces to perform assigned missions at the required time, place, intensity and duration. Readiness can be assessed through platform availability, serviceability, trained-crew availability, ammunition sufficiency, secure communication, reinforcement speed, casualty evacuation, intelligence-to-action time, deployment endurance and joint interoperability. These indicators make readiness a practical and measurable concept rather than a vague statement of preparedness.

Digital accountability refers to the use of secure digital systems to create traceable, verifiable and reviewable records of decisions, expenditures, assets and performance (Olayinka-Agboola, Eke & Ismail, 2025). In defence procurement, it may include electronic procurement, vendor databases, serial-number tracking, digital acceptance testing, maintenance-management systems, secure inventory records and classified performance dashboards. Digital accountability does not require public disclosure of operational secrets. It requires that properly authorised officers and oversight institutions can reconstruct what happened and identify where delays, defects or irregularities occurred.

Lifecycle capability refers to the useful military effect produced by an asset throughout its service life. The purchase price is only the beginning. Fuel, ammunition, software licensing, spare parts, infrastructure, crew training, maintenance, upgrades and disposal may cost more than the initial acquisition. Procurement that ignores these obligations creates stranded capability: equipment that has been paid for but cannot be sustained. Lifecycle costing is therefore not an optional accounting exercise; it is a core readiness requirement.

The acquisition-to-battlefield-effect gap describes the distance between what is purchased and what becomes effective in operations. The gap widens when planning is disconnected from field requirements, vendors underperform, funds are released late, acceptance testing is weak, maintenance ecosystems are absent or fleets become excessively fragmented. These concepts form an integrated chain. A system may contain excellent equipment yet perform poorly because a critical support link has failed.

4. THEORETICAL FOUNDATION

Systems Theory provides the primary foundation for the paper because military readiness emerges from the interaction of interdependent components. Procurement, training, intelligence, logistics, communications, maintenance and command must work together. Optimising one component while neglecting the others may reduce the performance of the whole. A sophisticated platform can even create additional vulnerability when the support system cannot provide the specialist maintenance, software access, technical documentation or trained personnel required to sustain it.

The Resource-Based View helps explain why strategic assets generate advantage only when they are valuable, usable and difficult to replace. In a military context, equipment has strategic value only when it is mission relevant, serviceable, deployable, interoperable and supported by trained personnel. Ownership alone is not capability. The true strategic resource is the combination of equipment, knowledge, personnel, maintenance, logistics, data and command competence.

Institutional Theory explains how formal rules, informal routines, secrecy, political influence, incentives and oversight affect procurement outcomes. A country may possess detailed procurement regulations while informal practices continue to shape vendor selection, contract variation, payment approval and equipment acceptance. Strong institutions improve the conversion of expenditure into capability by creating professional standards, clear sanctions, reliable documentation and independent review.

The digital-economy perspective adds the importance of information, speed and data control. Modern defence platforms are increasingly software defined and connected to digital supply chains. Data rights, cyber resilience, secure communication and rapid information exchange now influence both operational performance and accountability. Digital capability therefore serves two purposes: it improves command and control, and it creates a more reliable record of how public resources and military assets are managed.

5. AN INTEGRATED CAPABILITY-CONVERSION MODEL

The relationship between acquisition and operational readiness can be explained with a simple capability-conversion model. Let operational readiness be represented by R. Let A represent equipment that is actually available for operations, M maintenance capacity, T training quality, L logistics support, I interoperability, D digital command and information capability, and G governance or accountability quality. The model assumes that these factors complement one another rather than operate independently.

Equation 1: Multiplicative readiness model

The equation means that readiness depends on the combined strength of all the listed factors. The Greek letters above each factor simply show that some factors may have a stronger influence than others. The important idea is that the factors complement one another. If maintenance or training is extremely weak, a large quantity of equipment will still produce limited readiness. In simple terms, the whole system can be constrained by its weakest essential component.

Equation 2: Effective acquisition

In Equation 2, B is the amount appropriated for acquisition, u is the proportion actually released and cash-backed, e is procurement efficiency, and q is the proportion of delivered assets that pass proper acceptance testing. The multiplication sign is important. If any one of these factors is low, effective acquisition falls. For example, a large approved budget produces little capability if only a small portion is released or if delivered equipment fails acceptance tests.

Let s represent the serviceability rate, meaning the proportion of accepted equipment that is actually available for use. Serviceable acquisition is therefore the product of effective acquisition and the serviceability rate. This step makes the model more realistic because equipment may be properly delivered yet become unavailable after deployment because of faults, accidents, lack of spares or maintenance delays.

Equation 3: Full capability-conversion model

Equation 3 combines budgeting, release, procurement efficiency, acceptance quality and serviceability with maintenance, training, logistics, interoperability, digital capability and governance. It explains why budget growth may coexist with weak readiness. If funds are delayed, contracts are poorly managed or serviceability is low, the contribution of the budget to operational performance is reduced. Maintenance and digital systems are therefore not secondary expenses; they help determine whether acquisition becomes usable capability.

6. THREAT-BASED PLANNING AND REQUIREMENT DEFINITION

Procurement should begin with threat analysis rather than platform preference. Terrorism and banditry require persistent surveillance, rapid mobility, secure communication, night capability, counter-IED support, casualty evacuation and endurance in remote environments. Maritime insecurity requires domain awareness, patrol endurance, interdiction capability, secure communications and reliable maintenance at sea. These mission requirements should guide the selection of equipment rather than prestige, vendor pressure or the attraction of a particular platform.

Field commanders, operators, maintainers, logisticians and intelligence officers should participate in requirement definition. Headquarters staff understand policy and contracts, but theatre personnel understand terrain, equipment failure and enemy adaptation. Their observations should be formally documented and incorporated into future procurement. A procurement plan that excludes field experience is likely to repeat avoidable mistakes.

Planning must also address lead time. Long procurement cycles may deliver equipment designed for yesterday's threat. Modular systems, framework agreements and prequalified suppliers can improve responsiveness, but emergency procurement must retain safeguards. Urgency should not become a permanent excuse for opaque contracting, poor documentation or weak acceptance testing.

Lifecycle costing should be compulsory. Every proposal should state the purchase price, annual operating cost, training cost, infrastructure requirement, spare-parts plan, software obligations, expected service life and disposal cost. Decision-makers should compare the total cost of ownership, not only the headline price. An apparently cheaper platform may become more expensive if it requires imported spares, foreign technicians or costly software support.

Standardisation is equally important. Excessive diversity of platforms increases the number of technicians, spare parts, diagnostic tools, software systems and training programmes required. Nigeria should therefore prefer families of systems with common components where operationally feasible. Technology transfer and local maintenance should be treated as practical capability requirements rather than ceremonial additions to contracts.

7. PROCUREMENT, VENDOR MANAGEMENT AND CONTRACT PERFORMANCE

Vendor management begins before contract award. Technical competence, financial strength, ownership structure, delivery history, sanctions exposure, manufacturing capacity, after-sales capability and local support should be independently verified. Prequalification should be evidence based and periodically reviewed because a vendor's technical or financial condition may change over time.

Contracts should contain clear specifications, milestones, acceptance criteria, warranties, training obligations, spare-parts packages, software-update commitments, data rights and penalties for non-performance. Ambiguous contracts transfer risk to government and create disputes that delay capability. A contract should not merely state what will be delivered; it should explain how the asset will be supported and how satisfactory performance will be demonstrated.

Acceptance testing must be independent of vendor influence. Delivered platforms should be tested against the contract specification, environmental conditions, endurance requirements, safety standards and interoperability needs. Payment milestones should be linked to verified acceptance rather than physical arrival alone. An item that has arrived but cannot perform as required should not be treated as completed capability.

A secure vendor-performance system should record delivery timeliness, quality defects, warranty response, spare-parts availability, technical support and user-unit feedback. Repeated failure should lead to debarment or reduced eligibility. Strong performance should improve future ratings, but concentration risk must also be considered so that the defence system does not become excessively dependent on one supplier.

Digital procurement can improve traceability by linking the requirement, approval, tender, evaluation, contract, payment, delivery and acceptance records. Authorised auditors should be able to reconstruct the complete transaction chain. Classified technical details can remain protected while financial and procedural integrity is preserved.

8. MAINTENANCE, LOGISTICS AND HUMAN CAPABILITY

Maintenance is the bridge between acquisition and readiness. A platform that cannot be repaired quickly becomes a sunk cost during operations. Maintenance planning should begin before contract award and include manuals, tools, test equipment, spares, technician training, depot requirements, software access and repair-turnaround targets. Where these elements are omitted, equipment may become unavailable after minor faults.

Predictive maintenance can use sensor and usage data to identify likely failures before breakdown. A secure digital maintenance-management system should record service history, faults, parts replaced, technician action, downtime and return-to-service date. Aggregated data can reveal recurring vendor or design problems and help commanders decide whether a fleet is becoming too costly or unreliable to sustain.

Logistics determines whether forces can remain in operation. Fuel, ammunition, food, medical supplies, transport and communications must reach units under difficult conditions. Procurement analysis should therefore include deployment endurance and resupply reliability, not merely equipment availability. A platform that can operate for only a short period before resupply may have limited value in remote theatres.

Human capability is equally decisive. Training should cover operators, maintainers, commanders, logisticians and communications personnel. The number of trained crews must be sufficient for rotation, leave, illness and attrition. Simulators can reduce cost and risk, but live exercises remain necessary to test how equipment, personnel and command systems work together under realistic conditions.

Interoperability should be treated as a contractual requirement. Platforms and communication systems must exchange information across the Army, Navy, Air Force and relevant security agencies. Where systems are incompatible, commanders lose time translating information or coordinating through insecure channels. In fast-moving operations, this delay can erase the advantage created by expensive equipment.

9. DIGITAL ACCOUNTABILITY ARCHITECTURE

Nigeria requires a classified Defence Acquisition and Readiness Information System that integrates requirements, budgets, contracts, assets, maintenance, inventories, training and operational readiness. Access should be role based and limited to security-cleared personnel. The objective is to create one reliable chain of information from the first statement of need to the final assessment of operational performance.

A digital asset registry should assign each major platform a unique identifier linked to its contract, delivery date, location, configuration, warranty and maintenance history. Transfers between units and eventual disposal should be recorded. Serial-level tracking reduces diversion, duplication and the possibility that an asset is reported in more than one location.

An electronic contract and payment trail should link approvals, milestones, invoices, certificates and payments. Contract variations should require documented technical and financial justification. Automated exception reports can flag unusual timing, repeated vendors, split payments, repeated variations, deliveries without inventory records and payments made outside agreed milestones.

A serviceability dashboard should allow authorised commanders and auditors to see platform availability, causes of unserviceability, maintenance backlogs, spare-parts shortages, trained-crew availability and average repair time. Such a dashboard creates a direct connection between procurement and readiness. It shifts attention from what was bought to what is available for missions.

Secure audit analytics can identify duplicate assets, abnormal spare-parts consumption, unusual maintenance patterns, persistent vendor defects and inventory discrepancies. Audit can therefore become continuous rather than episodic. This does not remove human judgement; it gives decision-makers faster and more complete evidence.

Cybersecurity and data sovereignty must be built into the architecture. Contracts for software-dependent platforms should address source-code access, data ownership, encryption, patching, remote access and supply-chain cyber risk. Nigeria should not depend on systems that foreign vendors alone can inspect or control. Critical defence data must remain protected under national authority.

10. ACCOUNTABILITY, SECRECY AND PUBLIC VALUE

Defence procurement requires confidentiality, but secrecy should be specific and justified. Technical specifications, operational plans, deployment locations and intelligence methods may require protection. Contract value, procedural compliance, lifecycle obligations and audit findings can still be reviewed by authorised institutions. Accountability does not require that every detail be made public; it requires that someone with lawful authority can examine the evidence.

A layered accountability model is appropriate. Internal military audit should examine detailed operational records. The Ministry of Defence and procurement institutions should review compliance and performance. Parliamentary committees should receive classified briefings, while supreme audit institutions should conduct secure financial and value-for-money reviews. Public summaries can disclose aggregate findings without compromising missions.

The distinction between secrecy and impunity is essential. Blanket secrecy can shield inflated contracts, poor-quality equipment, non-delivery and unjustified variations. Careless disclosure can endanger personnel and expose vulnerabilities. The answer is not total secrecy or total openness, but professional classification rules, controlled access and clear responsibility for misuse.

Value-for-money audit should examine economy, efficiency and effectiveness. Economy asks whether inputs were acquired at a reasonable cost. Efficiency asks how well resources were converted into serviceable capability. Effectiveness asks whether the capability improved mission outcomes such as response time, surveillance persistence, force protection and civilian protection.

Public value also requires attention to opportunity cost. Wasteful defence procurement reduces the funds available for education, health and infrastructure. Effective acquisition therefore protects both national security and fiscal sustainability. Olasode, Eke and Olaleye (2022) show that aggregate economic growth

does not automatically reduce poverty. In the same way, aggregate defence expenditure does not automatically produce security; the transmission institutions matter.

11. MEASUREMENT AND EMPIRICAL STRATEGY

A rigorous assessment of defence acquisition should separate perceptions from objective operational performance. Questionnaires can measure views about planning quality, vendor management, transparency, maintenance support and training adequacy. However, claims about battlefield effectiveness require operational indicators such as serviceability, downtime, delivery delay, mission-response time, deployment duration, ammunition availability, casualty-evacuation time and trained-crew ratios.

These variables can be anonymised and aggregated where security requires it. The purpose is not to reveal the location or vulnerability of a specific unit, but to determine whether procurement is improving performance. For example, the average repair time for a class of vehicles can be reported without identifying the exact unit or operational theatre.

The qualitative strand should include field commanders, operators, maintainers, logistics officers, procurement officials, auditors and intelligence personnel. Interviews should identify where delays occur and how equipment failure affects missions. Sampling should extend beyond headquarters because field experience may differ sharply from administrative perceptions.

A mixed-method design must explain how the quantitative and qualitative strands are integrated. Quantitative results may show that accountability is associated with readiness, while qualitative evidence explains the mechanisms. Divergent findings should be reported rather than hidden. Where structural-equation modelling is used, the study should report reliability, validity, collinearity, path coefficients, confidence intervals, effect sizes and predictive relevance. Significant coefficients alone do not prove causation.

Ethical and security approval are essential. Researchers should protect identities, avoid operationally sensitive disclosure and use secure data storage. Methodological transparency should be maximised within legitimate security limits. The objective is to produce evidence that is useful to policy-makers without creating additional security risks.

12. POLICY RECOMMENDATIONS

Nigeria should adopt a threat-based capability-planning framework that begins with mission requirements and incorporates field-command input, lifecycle costing and periodic review against changing terrorist and criminal tactics. Every procurement proposal should explain the specific capability gap it addresses and the measurable readiness improvement expected from the investment.

Procurement proposals should include complete support packages covering training, ammunition, spare parts, maintenance tools, infrastructure, software updates, data rights and disposal plans. No major platform should be approved without a funded sustainment concept. This would reduce the risk of acquiring expensive equipment that cannot be maintained after the initial warranty period.

The Ministry of Defence should establish an integrated vendor-performance system covering due diligence, delivery milestones, acceptance testing, warranty response, after-sales support, sanctions and debarment. Vendor history should follow the supplier across contracts so that poor performance in one programme affects eligibility in future programmes.

Performance-based budgeting should link funds to readiness indicators such as serviceability, downtime, trained crews, response time, deployment endurance and interoperability. Contract value and quantity delivered should not be the principal measures of success. Budget discussions should ask what capability improved and whether the improvement can be demonstrated.

A secure digital asset, inventory and maintenance platform should be implemented across the Services with common data standards. The system should support continuous audit and classified readiness dashboards. Common standards are important because different Services must be able to share relevant information during joint operations.

Nigeria should strengthen domestic maintenance, repair, overhaul and manufacturing capacity. Technology transfer should be measured by local skills, tooling, documentation and actual reduction in foreign dependence. A contract should not be described as involving technology transfer merely because a small number of personnel attended a short training programme.

Procurement fleets should be standardised where operationally feasible. Reducing unnecessary platform diversity will lower training, inventory and maintenance costs. Emergency procurement should remain time limited and subject to post-award classified audit. Urgency should not remove acceptance testing, end-user verification or vendor accountability.

Parliamentary and supreme-audit oversight should be strengthened through secure access to relevant records and technical expertise. Oversight bodies must understand lifecycle capability, not merely financial compliance. Defence research should also incorporate objective theatre-level evidence and field personnel so that policy is not based only on headquarters perceptions or vendor claims.

13. IMPLEMENTATION FRAMEWORK

Implementation should begin with an institutional and regulatory review of existing procurement rules, approval processes, classification practices, audit arrangements, vendor databases and asset-recording procedures. This review should identify gaps, duplication and areas where responsibility is unclear. Reform will be difficult if several institutions believe that another institution is responsible for the same stage of the process.

The second stage should develop the digital architecture for the Defence Acquisition and Readiness Information System. The system should begin with major platforms and high-value contracts, where the financial and operational risks are highest. It should then expand gradually to other asset categories. A phased approach will allow technical and security problems to be corrected before full-scale implementation.

Pilot implementation should take place in selected units and procurement programmes. The pilot should test asset registration, contract tracking, maintenance reporting, vendor scoring and readiness dashboards. The results should be independently evaluated. User feedback is important because a system that is too complicated may encourage officers to maintain parallel paper records or enter incomplete information.

Following successful evaluation, the system should be expanded across the Armed Forces with common data standards and secure inter-service connectivity. Training should be provided for procurement officers, auditors, logisticians, maintainers and commanders. Cybersecurity testing should be continuous because the system itself will become a high-value target.

The final stage should involve continuous evaluation through classified audit, technical inspection, field-user feedback and readiness measurement. The reform should remain adaptable because threats, technologies and operational requirements will continue to change. A digital system that is not regularly updated may reproduce old weaknesses in a more sophisticated form.

14. CONCLUSION

Nigeria's struggle against terrorism, armed banditry, piracy, kidnapping and other violent threats requires modern equipment, but equipment alone does not fight. Capability emerges when acquisition is connected to intelligence, training, maintenance, logistics, interoperability, digital communication and effective command. The critical policy problem is therefore not simply how much Nigeria spends on defence, but how effectively resources are converted into battlefield effect.

This paper has reframed defence procurement as a capability system. It distinguishes appropriation, release, contracting, delivery, acceptance, serviceability, deployment and mission outcomes. Each stage can fail, and failure at one stage may neutralise investment elsewhere. The capability-conversion model shows that acquisition works together with maintenance, training, logistics, interoperability, digital systems and accountability. The weakest component may become the binding constraint.

Digital accountability offers a practical response. Secure asset registers, electronic contract trails, maintenance systems, inventory records, vendor scores and readiness dashboards can improve timeliness and traceability. Technology must, however, be combined with professional audit, classified oversight, clear sanctions, skilled personnel and field-level feedback.

The central conclusion is straightforward. Procurement success should be measured by usable capability and mission outcomes. Nigeria should move from counting equipment to measuring serviceability, deployment endurance, response speed, intelligence-to-action time, force protection, territorial control and civilian protection. When these indicators improve, acquisition has become capability. When they do not, expenditure has not achieved its full strategic purpose.

Table 1: Meaning of the Variables in the Capability Model

Symbol	Meaning	Simple interpretation
R	Operational readiness	Ability to perform assigned missions effectively
B	Approved defence resources	Budget made available for acquisition
U	Release rate	Share of the approved budget actually released
E	Procurement efficiency	How well the procurement process converts funds into value
Q	Acceptance quality	Share of delivered equipment that passes proper testing
S	Serviceability rate	Share of equipment that is ready for use
M	Maintenance capacity	Ability to repair and sustain equipment
T	Training quality	Competence of operators and maintainers
L	Logistics support	Fuel, ammunition, transport, food and medical support
I	Interoperability	Ability of systems and Services to work together
D	Digital capability	Quality of command, data and communication systems
G	Governance quality	Accountability, oversight and institutional discipline

REFERENCES

Acemoglu, D., & Robinson, J. A. (2012). Why nations fail: The origins of power, prosperity, and poverty. Crown.

Adekoya, A. A., Magaji, S., & Ismail, Y. (2025). Impact of Insecurity on Economic Growth in Nigeria: 1990-2023. *International Journal of Research and Scientific Innovation (IJRSI)*, 12(4), 1258-1271. DOI: https://doi.org/10.51244/IJRSI.2025.12040146

Ashe, M.A. Magaji, S. & Ismail, Y. (2026) Evaluating the Contribution of Police Reform Initiatives to National Security and Economic Stability. *International Journal of Innovative Finance and Economics Research 14(1):266-276,* doi:10.5281/zenodo.18527217

Bitzinger, R. A. (Ed.). (2009). The modern defense industry: Political, economic, and technological issues. Praeger Security International.

Eke, C. I., & Osi, M. U. (2023). The gathering clouds: The case of time and digital economics. East African Journal of Business and Economics, 6(1), 226-232. https://doi.org/10.37284/eajbe.6.1.1310

International Organization for Standardization. (2018). ISO 31000:2018 risk management-Guidelines. ISO.

Ismail, Y., El-Yaqub, A.B. & Eke, C. I., (2025) Impact of Digital Payment Technologies on Selected Banking Institutions in Nigeria. *MSI Journal of Economics and Business Management.* 2(4), 1-10. DOI: 10.5281/zenodo.15173057

North Atlantic Treaty Organization. (2018). NATO logistics handbook. NATO.

Olasode, T., Eke, C. I., & Olaleye, O. O. (2022). Has economic growth reduced poverty in Nigeria? A critical analysis of the last two decades. Journal of Enterprise and Development, 4(2), 232-256. https://doi.org/10.20414/jed.v4i2.5506

Olayinka-Agboola, M., Eke, C.I., & Ismail, Y., (2025) Effect of Corporate Entrepreneurship on Organizational Performance at United Africa Company of Nigeria. *International Journal of Spectrum Research in Social and Management Sciences (IJSRSMS)*, 1(2), 93-102. https://doi.org/10.5281/zenodo.15601528

Olayinka-Agboola, M., Ismail, Y., & Eke, C.I., (2025) Impact Of Digitalization On Public Service Delivery In Nigeria: A Case Study Of Federal Civil Service In Nigeria. *International Journal of Innovative Information Systems & Technology Research* 13(2):132-142, doi:10.5281/zenodo.15601615

Omar, A.I.S., Magaji, S., & Jafaru, Y. (2025). Insecurity and Women's Livelihoods in Borno State, Nigeria: A Socioeconomic Analysis of Conflict Impacts. *Global Journal of Economic and Finance Research*. 2 (7), 643-650

Organisation for Economic Co-operation and Development. (2016). Preventing corruption in public procurement. OECD Publishing.

Osi, M., & Eke, C. (2023). Households and 1-world economy: A mathematical discourse. Asian Journal of Economics, Business and Accounting, 23(15), 44-48. https://doi.org/10.9734/ajeba/2023/v23i151014

Pugh, P. G. (2007). Retrospect and prospect: Trends in cost and their implications for UK aerospace. Defence and Peace Economics, 18(1), 25-37.

Salihu, A., Musa, I., & Magaji, S. (2026). Effects of Boko Haram Activities on Trans-Border Migration in North-East Nigeria. Sciences (UKRJAHSS), 2(2), 7-21

SIPRI. (2024). SIPRI yearbook 2024: Armaments, disarmament and international security. Stockholm International Peace Research Institute.

Technical Critique. (2026). Technical critique of the paper 'Defence equipment acquisition strategies and operational effectiveness of the Nigerian Armed Forces': Assessment against Nigeria's war on terrorism and armed banditry. Unpublished manuscript.

United Nations Office on Drugs and Crime. (2013). Guidebook on anti-corruption in public procurement and the management of public finances. United Nations.

World Bank. (2016). World development report 2016: Digital dividends. World Bank.