



Nigerian Military Operational Adaptability: Outthinking, Outmanoeuvring and Outlasting Asymmetric Threats for Sustainable Operational Advantage

Muhammad Auwal Sule^{1*}

Centre for Civil-Military Cooperation (CIMICO), Abuja, Nigeria¹

*Corresponding author: albalagul@gmail.com

Received: 23 May 2026 | Revised: 24 June 2026 | Revised: 28 June 2026 | Published: 27 July 2026

Abstract

Purpose: This study examines Nigerian military operational adaptability as a strategic requirement for outthinking, outmanoeuvring, and outlasting asymmetric threats while sustaining operational advantage.

Research Methodology: The study adopts a qualitative documentary research design using reports, policy documents, and scholarly publications from 2021–2026. Evidence from Nigeria is comparatively analyzed alongside experiences from the United Kingdom, France, Kenya, and Ghana. The analysis is guided by the OODA Loop and Organizational Learning Theory.

Results: The findings show that sustainable operational advantage depends less on isolated technological acquisition than on the continuous integration of intelligence, doctrine, training, innovation, logistics, leadership, inter-agency coordination, and civil-military cooperation. Effective adaptability also requires institutional mechanisms that convert operational experience into doctrine, training, and capability development.

Conclusions: Nigeria requires an integrated institutional learning architecture that enables the military to anticipate, learn from, and continuously adapt to evolving asymmetric threats. Strengthening lessons-learned mechanisms, intelligence integration, technology adoption, readiness, and adaptive-force development is essential.

Limitations: The study relies on documentary evidence and comparative institutional analysis and does not establish statistical causality between adaptability measures and operational outcomes.

Contribution: The study integrates the OODA Loop and Organizational Learning Theory and proposes a Sustainable Operational Advantage Framework linking threat evolution, institutional learning, adaptive decision-making, capability innovation, and civil-military integration.

Keywords: *Asymmetric Threats, Military Innovation, Nigerian Military, Operational Adaptability, Operational Advantage*

How to Cite: Sule, M. A. (2026). Nigerian Military Operational Adaptability: Outthinking, Outmanoeuvring and Outlasting Asymmetric Threats for Sustainable Operational Advantage. *Advanced Studies in Law, Policy Innovation, and Institutional Reform (ASLPI)*, 1(3), 165-177.

1. Introduction

Contemporary armed conflict is increasingly characterized by rapid technological change, fluid adversary behavior, hybrid forms of violence, and the convergence of military, criminal, informational, and societal vulnerabilities. The distinction between conventional warfare and irregular conflict has consequently become less clear as non-state actors combine terrorism, organized crime,

local grievances, information operations, improvised technologies, and population-based networks ([Jakubiak, 2022](#)). The Global Terrorism Index 2025 recorded terrorist incidents in 66 countries in 2024, while the 2026 edition showed that more than 76% of terrorist attacks in 2025 occurred within 100 kilometers of an international border, highlighting the growing importance of mobility, border environments, and transnational linkages in contemporary asymmetric conflict ([Institute & Peace, 2026](#)). These developments increasingly favor military organizations capable of rapidly observing changes, interpreting emerging threats, making timely decisions, and continuously adapting their operational approaches.

Recent international experience further demonstrates that military effectiveness increasingly depends on institutional adaptability rather than conventional capability alone. The Russia–Ukraine war has reinforced the importance of technological adaptation, mission command, experimentation, interoperability, and the rapid integration of emerging technologies into established military capabilities ([Hackett & Nagl, 2024](#)). NATO Innovation Cooperation Roadmap with Ukraine similarly emphasizes rapid technological adoption, lessons learned, experimentation, and continuous refinement of operational concepts ([NATO, 2024a](#)). The United Kingdom has responded to these developments by promoting greater agility in defense acquisition and capability development, particularly through its Defence Drone Strategy and broader integrated defense approach ([UK, 2024](#)). France experience in the Sahel, however, demonstrates that adaptability involves more than acquiring new technologies; it also requires doctrine, local knowledge, institutional relationships, and operational approaches that correspond with political and social realities.

African security environments make such adaptability particularly important. Armed groups increasingly exploit porous borders, difficult terrain, local grievances, weak governance, and informal economic networks ([Bøås & Strazzari, 2020](#)). In 2026, fatalities linked to militant Islamist violence in Africa remained above 20,000 annually for the fourth consecutive year, with the Sahel, Lake Chad Basin, and Somalia accounting for substantial proportions of reported fatalities. Experiences from Kenya and Ghana further demonstrate that military responses to asymmetric threats increasingly require multi-agency coordination, regional cooperation, border surveillance, community engagement, and preventive approaches alongside conventional military capabilities ([Kapemba, 2025](#)). These experiences suggest that sustainable operational advantage depends on an institution's capacity to continuously learn and adapt as threats evolve.

Nigeria faces an especially complex asymmetric security environment. The country confronts terrorism in the North-East, banditry and kidnapping in the North-West and North-Central zones, communal violence, transnational organized crime, oil-related criminality, and other forms of insecurity. Between 2024 and 2025, 8,654 security incidents were recorded across Nigeria, including battles, explosions or remote violence, and violence against civilians, with particularly high levels of insecurity reported in Borno, Katsina, and Zamfara. Banditry has also become increasingly widespread and geographically dispersed, involving kidnapping, armed robbery, cattle rustling, murder, and attacks on communities ([European, 2026b](#)). In addition, the Global Terrorism Index 2026 recorded 171 terrorist incidents and 750 terrorism-related deaths in Nigeria during 2025, reflecting increases compared with the previous year and demonstrating the continuing adaptability of Boko Haram, the Islamic State West Africa Province, and emerging threats such as Lakurawa ([Onyejebu, 2025](#)).

The Nigerian military has undertaken several institutional responses to these evolving threats. These include the establishment of the Joint Doctrine and Warfare Centre, a dedicated Department of Training, expansion of special forces capabilities, restructuring of operational commands, development of forward operating bases, and greater emphasis on intelligence coordination, technology-enabled surveillance, and rapid response ([UK, 2024](#)). These initiatives demonstrate continuing efforts to improve military readiness and operational effectiveness. However, the persistence, mobility, and organizational adaptation of asymmetric threats suggest that the central challenge extends beyond the availability of military resources or technological capabilities. The critical issue is whether operational experience, intelligence, technology, and institutional resources

can be systematically transformed into doctrine, training, organizational learning, and sustainable capability development ([Schneider, 2019](#)).

Despite substantial investment in counterterrorism and counter-banditry operations, operational successes have not always translated into durable strategic advantage. The recurrence of attacks, emergence of new armed groups, expansion of criminal networks into new geographical areas, and continuing vulnerability of civilian communities indicate that adversaries retain the capacity to learn, reorganize, and exploit weaknesses in existing security arrangements. Military organizations may become increasingly reactive when lessons from operations are not systematically captured and incorporated into doctrine, training, procurement, intelligence, logistics, and institutional reform. Similarly, acquiring sophisticated technologies without corresponding improvements in information integration, maintenance, personnel development, command systems, civil-military cooperation, and organizational learning may strengthen short-term capability without ensuring long-term adaptability ([Dyson, 2019](#); [Boztosun-Çalışkan, 2025](#)).

This study therefore conceptualizes operational adaptability as a permanent institutional capability through which the Nigerian military can continuously understand, anticipate, and respond to asymmetric threats. The study is informed by the OODA Loop and Organizational Learning Theory. The OODA Loop provides an analytical basis for understanding how observation, orientation, decision, and action can support rapid adaptation, while Organizational Learning Theory explains how operational experience can be transformed into improved institutional behavior and capability. Combining these perspectives enables operational adaptability to be examined not simply as tactical flexibility, but as an institutional process connecting intelligence, doctrine, technology, training, logistics, leadership, inter-agency coordination, and civil-military cooperation ([Ryder & Downs, 2022](#)).

Accordingly, this study examines the evolving characteristics of terrorism and banditry confronting the Nigerian military, assesses the role of institutional learning and operational adaptability in sustaining military advantage, and analyzes the contribution of intelligence, technology, training, logistics, and civil-military cooperation to adaptive capability. It further develops an integrated framework for strengthening sustainable operational advantage within the Nigerian military. By focusing on how operational experience can be transformed into institutional knowledge and capability, the study seeks to explain how the Nigerian military can move beyond responding to emerging threats toward continuously anticipating, learning from, and adapting to changes in the asymmetric security environment.

2. Literature Review and Hypothesis/es Development

2.1 Operational Adaptability

Operational adaptability refers to the institutional capacity of a military organization to recognize changes in its operational environment, interpret emerging threats, modify doctrine and organizational arrangements, adjust capabilities, and incorporate lessons from experience. It extends beyond tactical flexibility because it involves systematic institutional processes through which operational experience is transformed into future preparedness. An adaptable military organization must therefore be capable of continuously reassessing its assumptions, procedures, and capabilities in response to changing security conditions. Such adaptability requires coordination among doctrine, leadership, training, intelligence, technology, logistics, personnel development, and organizational learning. Operational adaptability consequently represents an enduring institutional capability rather than a temporary response to a specific operational challenge ([Wujarso & Saputro, 2026](#)).

In asymmetric conflict environments, operational adaptability becomes particularly important because adversaries frequently change their tactics, locations, organizational structures, and methods of engagement. Military organizations that rely excessively on established procedures may struggle when threats evolve more rapidly than existing doctrine and command arrangements. Adaptability

therefore requires mechanisms for capturing field experience, evaluating operational outcomes, and translating lessons into revised doctrine, training, procurement, and force development. It also depends on the ability of commanders and institutions to balance strategic direction with sufficient flexibility for timely responses at the operational level. In this context, operational adaptability provides a foundation for maintaining effectiveness when conventional approaches alone are insufficient to address rapidly changing security threats ([Susilo, Wibisono, & Yanti, 2026](#); [Purba & Kusmiyanti, 2024](#)).

2.2 Asymmetric Threats

Asymmetric threats arise when weaker actors employ unconventional strategies, organizational structures, technologies, or vulnerabilities to offset the conventional advantages of stronger military forces. Terrorist organizations, bandit groups, insurgents, and other non-state actors may deliberately avoid direct confrontation with conventional forces and instead rely on mobility, surprise, dispersed networks, difficult terrain, and civilian environments. Such actors can exploit social grievances, porous borders, weak governance, informal economic systems, and gaps in intelligence or institutional coordination. Their operational effectiveness is therefore not necessarily determined by conventional military strength or technological superiority. Instead, asymmetry enables weaker actors to impose significant costs by identifying and exploiting weaknesses within the stronger actor's operational and institutional systems ([Cohen, 2018](#)).

The changing nature of asymmetric threats further complicates military responses because these actors can reorganize, relocate, fragment, and adopt new technologies after experiencing operational pressure. Terrorism and banditry in Nigeria illustrate this challenge, as armed groups operate across different geographical areas and frequently adapt their organizational structures and operational techniques ([Ojo, Oyewole, & Aina, 2023](#)). Their ability to exploit local information, cross-border movement, digital communication, and relatively inexpensive technologies can reduce the effectiveness of standardized military responses. Consequently, successful responses require continuous intelligence gathering, contextual understanding, inter-agency coordination, and rapid institutional learning. Military effectiveness against asymmetric threats therefore depends not merely on superior force, but on the capacity to understand and adapt faster than adversaries can modify their own strategies ([Okoli & Nwangwu, 2023](#)).

2.3 Sustainable Operational Advantage

Sustainable operational advantage refers to the capacity of a military organization to maintain a relative advantage over adversaries across changing operational conditions. It differs from temporary battlefield superiority because operational success in a particular engagement does not necessarily translate into enduring strategic effectiveness. Sustainable advantage requires military institutions to preserve effective decision-making, intelligence, readiness, mobility, logistics, innovation, legitimacy, and organizational learning over time. It also requires the ability to regenerate capability when adversaries alter their tactics or when operational conditions change. Sustainable operational advantage should therefore be understood as a dynamic condition maintained through continuous adaptation rather than as a permanent state of military superiority ([Sołoducho-Pelc & Sulich, 2020](#)).

The sustainability of operational advantage is closely linked to institutional integration. Intelligence must inform operational planning, operational experience must influence training and doctrine, and technological acquisition must correspond with identified operational requirements. Logistics, personnel readiness, professional military education, leadership development, and inter-service coordination also determine whether military effectiveness can be maintained over prolonged periods ([Foresti, Rossi, Magnani, Bianco, & Delmonte, 2020](#)). Furthermore, legitimacy and civil-military cooperation are important because asymmetric threats often operate within communities where information and local support can influence operational outcomes. Sustainable advantage consequently emerges from the interaction of institutional capabilities rather than from dependence on a single technological, organizational, or tactical factor ([Shu, Zhao, Liu, & Lindsay, 2020](#)).

2.4 Intelligence, Technology, and Civil-Military Integration

Intelligence and technology are central components of operational adaptability because they influence how rapidly military institutions can identify, interpret, and respond to emerging threats. Intelligence should be understood not merely as information collection but as a process through which information from military units, security agencies, communities, technological systems, and other sources is transformed into operational understanding ([Ainslie, Thompson, Maynard, & Ahmad, 2023](#)). Technologies such as drones, satellite imagery, secure communications, data analytics, and geospatial intelligence can strengthen situational awareness and decision support. However, technological acquisition alone does not automatically produce operational advantage when systems are poorly integrated, personnel are inadequately trained, or information cannot be converted into timely decisions. Effective military adaptation therefore requires technology to be integrated with doctrine, intelligence analysis, training, command structures, and institutional learning ([Biswas, Hossain, & Comite, 2024](#)).

Civil-military integration further strengthens adaptive capability because asymmetric threats frequently operate within complex social environments. Local communities can provide contextual information, early warning, and knowledge of population movements or emerging threats that may not be available through conventional surveillance systems. Civil-military cooperation should therefore establish structured and responsible channels through which communities, traditional institutions, civil society organizations, local authorities, and security agencies can exchange relevant information ([Cook & Yogendran, 2020](#)). Such cooperation must remain institutionally coordinated and should not transfer military or intelligence responsibilities to civilians. When combined with intelligence and technological capabilities, effective civil-military integration can reduce information gaps, strengthen public confidence, improve situational awareness, and contribute to more responsive operational decision-making ([Liadi, 2024](#)).

2.5 Theoretical and Analytical Framework

This study employs the OODA Loop and Organizational Learning Theory as complementary theoretical lenses for explaining military operational adaptability. The OODA Loop, associated with John Boyd, conceptualizes competitive effectiveness through four interconnected processes: observation, orientation, decision, and action. Observation involves identifying relevant changes in the operational environment, while orientation concerns interpreting information according to existing knowledge, experience, and contextual understanding. Decision and action subsequently translate this interpretation into operational responses that can be evaluated through further observation. The OODA Loop is therefore best understood as a continuous and adaptive cycle rather than a rigid sequential process, particularly in asymmetric environments where information and adversary behavior change rapidly.

Organizational Learning Theory complements the OODA framework by explaining how military institutions transform operational experience into improved organizational behavior and capability. The distinction between single-loop and double-loop learning is particularly relevant because the former focuses on correcting performance within existing assumptions, whereas the latter questions whether existing doctrine, policies, structures, and assumptions remain appropriate. Persistent asymmetric threats may require military organizations not only to improve existing procedures but also to reconsider the institutional assumptions underlying training, procurement, command arrangements, and force employment. When combined, the two perspectives suggest that military adaptation begins with changes in the threat environment, which are identified through observation and intelligence and subsequently interpreted through institutional orientation. This process supports organizational learning, informs decision-making and innovation, and enables operational adaptation that can ultimately contribute to sustainable operational advantage. The framework therefore emphasizes that sustainable advantage emerges when information is systematically transformed into institutional knowledge, knowledge informs decisions, decisions generate adaptive capabilities, and operational experience is continuously reintegrated into organizational learning ([Johnson, 2023](#)).

3. Research Methodology

The study adopted a qualitative documentary research design. Data were obtained from recent reports and policy documents of international organizations, government institutions, military authorities, research organization and scholarly publications covering the period 2021–2026. Particular attention was given to contemporary evidence concerning terrorism, asymmetric warfare, military innovation, operational learning, technology, training, civil-military cooperation and security-sector adaptation. Selected experiences from the United Kingdom, France, Kenya and Ghana were used comparatively to identify institutional lessons relevant to Nigeria. Documentary evidence was subjected to thematic analysis around five analytical themes: threat evolution, institutional learning, intelligence and technology, force readiness, and civil-military integration. The study does not claim statistical causality; rather, it interprets documentary evidence to identify institutional patterns and policy implications ([Morgan, 2022](#)).

4. Results and Discussions

4.1 Evolving Asymmetric Threat Environment in Nigeria

Nigeria's asymmetric threat environment is characterized by fragmentation, geographical mobility, organizational adaptation, and the convergence of terrorism with other forms of criminality. Terrorist organizations such as ISWAP and Boko Haram continue to operate particularly in the North-East, while Lakurawa represents an emerging dimension of violent extremist activity. At the same time, banditry and kidnapping have expanded across several states, creating an operational environment in which the military must respond to diverse threat structures operating within overlapping geographic and social spaces. The EUAA's 2026 assessment indicates that bandit groups are highly fragmented and vary considerably in organization, operational capacity, and geographic reach, making standardized responses increasingly difficult ([European, 2026b](#)). These characteristics require security institutions to develop flexible and context-sensitive approaches rather than rely on uniform operational responses.

The threat environment is further complicated by the growing significance of border areas. The Global Terrorism Index reports that more than three-quarters of terrorist attacks globally in 2025 occurred within 100 kilometers of international borders, while Nigeria's security environment remains closely connected to the wider Lake Chad Basin and Sahel security complex ([Institute & Peace, 2026](#)). This regional dimension allows armed groups to exploit porous borders for mobility, logistics, financing, recruitment, and the movement of weapons and information. Consequently, operational adaptability must incorporate regional intelligence cooperation, inter-agency information sharing, border surveillance, and cross-border security coordination. A purely territorial conception of military operations is therefore increasingly inadequate in an environment where threats can rapidly move across national and regional boundaries.

The threat is also becoming increasingly technologically adaptive. Low-cost drones, digital communications, satellite imagery, open-source intelligence, and other commercially available technologies are transforming how armed groups communicate, gather information, coordinate activities, and evade detection. These developments create additional challenges for military organizations because technological advantages can quickly shift as new tools become widely accessible. International experience demonstrates that operational advantage increasingly depends on the ability to identify useful technologies, test them rapidly, integrate them into doctrine and operational practice, and discontinue ineffective applications. NATO's innovation roadmap similarly connects technological innovation with experimentation, lessons learned, interoperability, and the continuous adaptation of concepts of operations ([NATO, 2024a](#)). For Nigeria, this reinforces the need to integrate technological innovation with intelligence, training, doctrine, and organizational learning in responding to evolving asymmetric threats.

4.2 Institutional Learning and the Need to Outthink the Threat

To outthink asymmetric threats at the institutional level means developing superior understanding rather than relying solely on greater firepower. Intelligence should therefore be viewed as an organizational learning function rather than merely as a process of information collection. The critical issue is whether information from soldiers, communities, intelligence agencies, police, border institutions, and technological systems can be effectively integrated, analyzed, and translated into timely operational understanding. This requires reliable information-sharing mechanisms, analytical capacity, and institutional processes that enable decision-makers to identify emerging patterns and anticipate changes in adversary behavior. Superior understanding consequently depends on the ability to transform diverse information sources into actionable knowledge ([Ainslie, Thompson, Maynard, & Ahmad, 2023](#)).

Nigeria's current emphasis on intelligence-driven operations reflects this requirement. In 2026, the Minister of Defence highlighted satellite-enabled surveillance, radar imaging, and signal analytics as capabilities capable of improving situational awareness and identifying criminal routes and locations. However, the strategic challenge extends beyond the acquisition and use of technology. Intelligence superiority also depends on analytical capacity, interoperability, information assurance, human intelligence, institutional trust, and mechanisms for rapidly converting information into operational decisions. Technology therefore becomes most effective when it is integrated with human judgment, organizational processes, and coordinated intelligence structures.

Outthinking asymmetric threats also requires a stronger lessons-learned culture. Every major operation generates information about what worked, what failed, and why particular outcomes occurred. When such information is not systematically captured, analyzed, and incorporated into training and doctrine, military institutions may repeatedly encounter similar problems without developing corresponding organizational knowledge. Institutional learning therefore requires structured mechanisms for recording operational experience, evaluating outcomes, identifying recurring weaknesses, and disseminating validated lessons across relevant commands and training institutions. NATO's establishment of mechanisms to capture lessons from the Ukraine war demonstrates how military organizations can institutionalize learning to influence training, capability development, and strategic posture.

For Nigeria, a comparable institutional approach would involve the systematic collection of observations from military operations, structured analysis of operational outcomes, doctrinal review, incorporation of validated lessons into professional military education, and subsequent testing through exercises. Such processes would help ensure that knowledge gained in one operational theater is not lost when personnel or commanders change. They would also strengthen the connection between field experience, doctrine, training, force development, and future operational planning. The objective should be to make learning a routine and continuous institutional function rather than an occasional response to major operational setbacks. In this way, organizational learning can strengthen the military's capacity to anticipate, understand, and adapt to evolving asymmetric threats.

4.3 Outmanoeuvring Through Operational Flexibility and Innovation

Outmanoeuvring asymmetric threats should be understood primarily as the capacity to remain organizationally and intellectually flexible when adversaries change their behavior. This includes the ability to modify operational concepts, adjust command relationships, reorganize resources, and integrate new capabilities without prolonged bureaucratic delay. It also requires an appropriate balance between central coordination and decentralized initiative, allowing commanders to respond to changing circumstances while remaining within strategic intent and legal authority. Such flexibility is particularly important in asymmetric environments where adversaries can rapidly alter tactics, locations, and methods of operation. Operational effectiveness therefore depends on institutional arrangements that allow military organizations to adapt more quickly than the threats they confront.

The United Kingdom's experience demonstrates the importance of acquisition systems that can respond effectively to operational change. Its Defence Drone Strategy recognized that emerging technologies were transforming battlefield conditions and that defense procurement therefore needed to become more agile and resilient ([UK Ministry of Defence, 2024](#)). NATO's Ukraine Innovation Roadmap similarly emphasized responsiveness, agility, speed, interoperability, and continuous experimentation as important principles of military innovation ([NATO, 2024a](#)). These approaches demonstrate that innovation requires more than acquiring new technologies; it also depends on the institutional capacity to test, evaluate, integrate, and scale useful capabilities. Military innovation is therefore most effective when procurement, doctrine, training, and operational requirements are closely aligned.

For Nigeria, operational innovation should not be equated solely with expensive or sophisticated technology. Innovation may involve modifying organizational structures, improving intelligence fusion, redesigning training, strengthening maintenance systems, enhancing communications, using commercially available technologies responsibly, and improving medical and logistics support. It may also include developing more effective civil-military information channels and refining command processes to support faster decision-making. These measures can improve operational responsiveness without necessarily requiring large-scale technological acquisition. The central objective is to ensure that organizational processes can adapt at a speed compatible with the changing threat environment.

The Nigerian military has already demonstrated progress in this direction through the Joint Doctrine and Warfare Centre, dedicated training structures, special forces development, and changes to operational command arrangements ([Defence Headquarters Nigeria, 2025](#)). These initiatives provide an institutional foundation for strengthening operational flexibility and innovation. However, their long-term effectiveness depends on whether they are integrated into a broader system of organizational learning and capability development. Doctrine, training, equipment, intelligence, logistics, and operational experience should reinforce one another rather than function as separate institutional activities. The next challenge is therefore to consolidate these initiatives into an integrated adaptive system capable of responding continuously to evolving asymmetric threats.

4.4 Outlasting the Threat: Readiness, Logistics and Institutional Endurance

The third component of sustainable operational advantage is the capacity to outlast asymmetric threats. Terrorist and bandit organizations often exploit the assumption that military operations are temporary. They can disperse, regenerate, relocate or change methods while security forces face fatigue, resource constraints and competing national priorities. Sustained advantage therefore depends on endurance, including personnel readiness, equipment availability, maintenance, medical support, logistics, rotation systems, professional education and institutional morale.

Outlasting should also be understood as a whole-of-system concept. Military effectiveness becomes difficult to sustain when civilian institutions cannot provide complementary governance, policing, justice, development and community-security functions. Kenya's experience demonstrates the importance of multi-agency approaches, community-level prevention, regional cooperation and socio-economic measures alongside security operations.

The Nigerian context similarly requires the Armed Forces to operate within a wider national security ecosystem. Military pressure can disrupt armed groups, but lasting security requires police and intelligence capacity, effective justice processes, border management, local governance, economic opportunities and community cooperation. Civil-military cooperation is particularly important because local communities frequently possess information unavailable to conventional surveillance systems. Such cooperation should remain rights-respecting and institutionally coordinated, ensuring that civilian participation enhances security without exposing communities to retaliation or inappropriate security responsibilities.

4.5 Technology as an Enabler of Operational Adaptability

Technology is increasingly central to operational adaptability, but its value depends on institutional integration. Artificial intelligence, drones, satellite imagery, geospatial intelligence, secure communications, data analytics and other emerging technologies can improve situational awareness and decision support. However, technology can also create vulnerabilities when personnel are insufficiently trained, systems are incompatible or procurement is disconnected from actual operational requirements.

The Ukraine experience demonstrates the importance of rapid experimentation and continuous adaptation. NATO's 2024 roadmap stresses that emerging technologies should be integrated with doctrine, concepts of operations and lessons learned rather than treated as isolated technical projects ([NATO, 2024a](#)). Similarly, recent military analysis identifies emerging multi-use technology and mission command as major lessons from the Russia-Ukraine war ([Bolton & Nagl, 2026](#)).

Nigeria should consequently approach military technology through an operational-problem-solving model. Technology acquisition should begin with clearly defined operational gaps, followed by testing, evaluation, training, integration and institutional review. This would reduce the risk of acquiring sophisticated systems that are difficult to maintain, insufficiently integrated or poorly matched to Nigeria's operational environment.

4.6 Training, Leadership and the Human Dimension

No operational concept can remain adaptive without personnel capable of learning and exercising informed judgment. Training should therefore move beyond repetition toward realistic problem-solving, inter-service cooperation, technological familiarity, ethical decision-making and continuous professional development. The objective is to prepare personnel to operate in conditions where information is incomplete and threats evolve faster than standard operating assumptions.

Leadership is particularly important. Military organizations need commanders and non-commissioned leaders capable of interpreting changing circumstances, encouraging disciplined initiative and transmitting operational lessons upward and downward. Evidence from the Ukraine conflict has highlighted the importance of mission command, empowered leadership and professional non-commissioned officers in improving battlefield adaptability ([Dyson, 2019](#)).

For the Nigerian military, this suggests the need to connect professional military education with real operational experience. Officers and soldiers returning from operational theatres should contribute systematically to training institutions, doctrine reviews and lessons-learned processes. Such a system would reduce the gap between what is taught in training institutions and what personnel encounter in actual operations.

4.7 Civil-Military Cooperation as a Source of Operational Advantage

Civil-military cooperation should form an important component of Nigeria's operational adaptability because asymmetric threats frequently operate within social environments. Communities are not merely recipients of security; they are important sources of contextual information, early warning and social resilience. Ghana's experience of combining border patrols with community engagement illustrates how military presence can be complemented by local information and trust-building ([Boztosun-Çalışkan, 2025](#)).

In Nigeria, civil-military cooperation should be institutionalized without transferring military or intelligence responsibilities to civilians. The objective should be to establish reliable channels through which communities, traditional institutions, civil society organizations, local authorities and security agencies can exchange information, communicate concerns and strengthen early warning. Such mechanisms can help reduce information gaps and improve public confidence while preserving the professional responsibilities of security institutions.

The concept also aligns with a whole-of-society approach to security. Terrorism and banditry are not exclusively military problems because their persistence can be influenced by unemployment, local grievances, criminal economies, weak governance, social exclusion and cross-border networks. The military therefore gains greater strategic endurance when its operational activities are connected to appropriate civilian institutions that address non-military dimensions of insecurity.

4.8 Discussion

The evidence indicates that sustainable operational advantage is fundamentally a function of institutional adaptability. Nigeria's security environment changes continuously, while terrorist and criminal organizations demonstrate capacity for fragmentation, mobility and tactical adjustment. The appropriate institutional response is not simply to increase the intensity of military operations, but to create a force capable of learning and adapting faster than the threat environment changes.

The comparative evidence reinforces this proposition. The United Kingdom illustrates the importance of agile capability development and procurement, while France demonstrates the necessity of adapting doctrine to local political and social environments. Kenya highlights the value of multi-agency and regional approaches, whereas Ghana demonstrates the preventive importance of border surveillance and community engagement. None of these experiences should be mechanically transplanted into Nigeria. Their relevance lies in the institutional principles they reveal, including continuous learning, integrated intelligence, flexible structures, technology adoption, inter-agency cooperation, and attention to the social environment.

Nigeria has already taken important steps toward these principles through joint doctrine structures, training reforms, special forces development, restructuring of operational commands and greater emphasis on technology and intelligence. The central requirement now is integration. Doctrine should inform training; training should reflect operational experience; operational experience should shape doctrine; intelligence should inform technology acquisition; technology should be evaluated through operational use; and civil-military engagement should feed relevant information into security planning.

The study consequently proposes the Sustainable Operational Advantage Framework (SOAF), which explains how changes in the threat environment should be identified through integrated observation, interpreted through institutional orientation, and transformed into rapid organizational learning. This learning process should then inform adaptive decision-making, capability innovation, and stronger joint and civil-military integration. Through this sequence, military institutions can progressively develop sustainable operational advantage rather than depend on isolated capabilities or temporary operational successes. The framework places institutional learning at the center because no single capability can permanently guarantee advantage against evolving asymmetric threats. Sustainable operational advantage instead emerges from the interaction of personnel, intelligence, doctrine, technology, logistics, leadership, and societal partnerships.

5. Conclusions

Nigeria's asymmetric security environment requires a military institution capable not only of fighting effectively but also of learning continuously. Terrorism and banditry are adaptive threats whose organizational forms, geographic patterns, technologies, and social relationships change over time. Consequently, a military response based primarily on established routines risks becoming progressively less effective as threats evolve.

Operational adaptability provides a framework for addressing this challenge. Outthinking asymmetric threats requires superior institutional understanding and intelligence, while outmaneuvering them requires organizational flexibility, innovation, and timely decision-making. Outlasting such threats requires sustained readiness, logistics, personnel development, legitimacy, and national partnerships. The objective is not to achieve permanent superiority in every encounter, but to develop the institutional capacity to regenerate operational advantage as circumstances change.

Nigeria's existing reforms provide a foundation for building a more integrated adaptive system. The strategic priority should therefore be to institutionalize lessons learned, integrate intelligence and technology, strengthen professional military education, improve logistics and readiness, and deepen civil-military cooperation. Such an approach would enable the Nigerian military to move beyond merely responding to threats as they emerge and toward continuously anticipating, learning from, and adapting to the changing character of asymmetric conflict.

Acknowledgement

The author would like to acknowledge the contributions of international organizations, government institutions, military authorities, research organizations, and scholars whose reports, policy documents, and academic publications provided valuable evidence for this study. The author also appreciates the broader academic and professional communities engaged in security studies, military innovation, and organizational learning, whose knowledge and insights supported the development of this research.

Conflict of Interest

The author declares that there is no conflict of interest regarding the publication of this article. The research was conducted independently, and no financial, institutional, or personal relationships influenced the research design, data interpretation, analysis, or preparation of the manuscript.

References

- Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 132, 103352. <https://doi.org/10.1016/j.cose.2023.103352>
- Biswas, T. R., Hossain, M. Z., & Comite, U. (2024). Role of management information systems in enhancing decision-making in large-scale organizations. *Pacific Journal of Business Innovation and Strategy*, 1(1), 5-18. <https://doi.org/10.70818/pjbis.2024.v01i01.03>
- Bolton, S., & Nagl, J. A. (2026). Innovation and adaptation: Lessons from the Russia-Ukraine War, 2024. *Parameters*, 56(3). <https://doi.org/10.55540/0031-1723.3406>
- Boztosun-Çalışkan, E. M. (2025). Digital command in irregular warfare: NATO military leadership communication adaptation during Crisis operations (2019–2024). *Small Wars & Insurgencies*, 1-37. <https://doi.org/10.1080/09592318.2025.2557618>
- Bøås, M., & Strazzari, F. (2020). Governance, fragility and insurgency in the Sahel: A hybrid political order in the making. *The International Spectator*, 55(4), 1-17. <https://doi.org/10.1080/03932729.2020.1835324>
- Cohen, E. (2018). Technology and warfare. *Strategy in the contemporary world: an introduction to Strategic Studies*, 127-143. <https://doi.org/10.1093/hepl/9780198708919.003.0008>
- Cook, A. D., & Yogendran, S. (2020). Conceptualising humanitarian civil-military partnerships in the Asia-Pacific:(Re-) ordering cooperation. *Australian Journal of International Affairs*, 74(1), 35-53. <https://doi.org/10.1080/10357718.2019.1693498>
- Dyson, T. (2019). The Military as a learning organisation: Establishing the fundamentals of best-practice in lessons-learned. *Defence Studies*, 19(2), 107-129. <https://doi.org/10.1080/14702436.2019.1573637>
- European Union Agency for Asylum. (2026b). *Nigeria: Security situation—Banditry and kidnappings*.

- Foresti, R., Rossi, S., Magnani, M., Bianco, C. G. L., & Delmonte, N. (2020). Smart society and artificial intelligence: Big data scheduling and the global standard method applied to smart maintenance. *Engineering*, 6(7), 835-846. <https://doi.org/10.1016/j.eng.2019.11.014>
- Hackett, M. T., & Nagl, J. A. (2024). A long, hard year: Russia-Ukraine war lessons learned 2023. *The US Army War College Quarterly: Parameters*, 54(3), 6. <https://doi.org/10.55540/0031-1723>
- Institute for Economics & Peace. (2026). *Global Terrorism Index 2026: Measuring the impact of terrorism*.
- Jakubiak, E. (2022). Hybrid warfare as a new type of armed conflict in the modern world. *Studia Bezpieczeństwa Narodowego*, 24(2), 71-82. <https://doi.org/10.37055/sbn/151015>
- Johnson, J. (2023). Automating the OODA loop in the age of intelligent machines: Reaffirming the role of humans in command-and-control decision-making in the digital age. *Defence Studies*, 23(1), 43-67. <https://doi.org/10.1080/14702436.2022.2102486>
- Kapemba, R. K. (2025). From Guns to Governance: Rethinking Responses to Hybrid Security Threats Beyond the Battlefield: Global, Regional and Kenyan Perspectives. *National Security: A Journal of the National Defence University-Kenya*, 3(2), 84-97. <https://doi.org/10.64403/n26w7d18>
- Liadi, K. O. (2024). Designing a cross-border security cooperation model: Nigeria's foreign policy response to regional terrorism. *Gyanshauryam, International Scientific Refereed Research Journal*, 7(3), 311-338. <https://doi.org/10.32628/GISRRJ247324>
- Morgan, H. (2022). Conducting a qualitative document analysis. *The qualitative report*, 27(1), 64-77. <https://doi.org/10.46743/2160-3715/2022.5044>
- NATO. (2024a). Summary of the NATO-Ukraine Innovation Cooperation Roadmap. *North Atlantic Treaty Organization*.
- Ojo, J. S., Oyewole, S., & Aina, F. (2023). Forces of terror: Armed banditry and insecurity in North-west Nigeria. *Democracy and Security*, 19(4), 319-346. <https://doi.org/10.1080/17419166.2023.2164924>
- Okoli, A. C., & Nwangwu, C. (2023). Organized crime-terror nexus: Interrogating the linkage between banditry and terrorism in Northern Nigeria. *Journal of Asian and African Studies*, 58(5), 766-778. <https://doi.org/10.1177/00219096211069650>
- Onyejebu, D. C. (2025). Faith-Based Violence: Exploring the Nexus between Religious Extremism and Crime in Nigeria. *African Journal of Religion Philosophy & Culture (AJRPC)*, 6(4), 111. <https://doi.org/10.31920/2634-7644/2025/v6n4a6>
- Purba, A., & Kusmiyanti, K. (2024). Pengaruh Manajemen Pengetahuan terhadap Kinerja Organisasi Berdasarkan Balance Scorecard pada Lembaga Pemasyarakatan Wilayah Banten. *Jurnal Akuntansi, Keuangan, Dan Manajemen*, 6(1), 263-278. <https://doi.org/10.35912/jakman.v6i1.3672>
- Ryder, M., & Downs, C. (2022). Rethinking reflective practice: John Boyd's OODA loop as an alternative to Kolb. *The International Journal of Management Education*, 20(3), 100703. <https://doi.org/10.1016/j.ijme.2022.100703>
- Schneider, J. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies*, 42(6), 841-863. <https://doi.org/10.1080/01402390.2019.1627209>
- Shu, C., Zhao, M., Liu, J., & Lindsay, W. (2020). Why firms go green and how green impacts financial and innovation performance differently: An awareness-motivation-capability perspective. *Asia Pacific Journal of Management*, 37(3), 795-821. <https://doi.org/10.1007/s10490-018-9630-8>

- Sołoducho-Pelc, L., & Sulich, A. (2020). Between sustainable and temporary competitive advantages in the unstable business environment. *Sustainability*, 12(21), 8832. <https://doi.org/10.3390/su12218832>
- Susilo, S., Wibisono, C., & Yanti, S. (2026). Human Resource Competence, Technology Utilization, and Safety Culture on Organizational Performance through Operational Effectiveness. *Global Academy of Multidisciplinary Studies*, 3(1), 37-48. <https://doi.org/10.35912/gams.v3.n1.p37-48.2026>
- UK Ministry of Defence. (2024). *Defence Drone Strategy: The UK's approach to defence uncrewed systems*.
- Wujarso, R., & Saputro, G. E. (2026). Evaluation of Intelligence Management Strategies in Improving National Security and Resilience Preparedness. *Annals of Human Resource Management Research*, 6(2), 447-461. <https://doi.org/10.35912/ahrmr.v6i2.3826>