NIGERIA'S INTELLIGENCE REVIEW

SPECIAL EDITION

The Future of Civil-Military Intelligence in the 21st Century. A Smarter Security Future: Intelligence at a Crossroads - From Information to Insight, From Reports to Results. Intelligence without collaboration is guesswork.

EDITORIAL FOREWORD

The Future of Civil-Military Intelligence in the 21st Century. A Smarter Security Future: Intelligence at a Crossroads - From Information to Insight, From Reports to Results. Intelligence without collaboration is guesswork. The Nigerian security environment is evolving rapidly. From insurgency and cybercrime to geopolitical rivalries and technological disruptions, the role of intelligence in safeguarding our nation has never been more critical. Intelligence is the heartbeat of statecraft. From the renaissance courts to the cyber age, it has shaped how nations defend themselves, manage crises, and project influence. For Nigeria, the stakes are even higher. Surrounded by regional instability, threatened by terrorism, cybercrime, and organized crime, the country cannot afford an outdated or fragmented intelligence ecosystem.

Insecurity in Nigeria is no longer just about bandits, insurgents, or cyber criminals. It is about how intelligence is produced, shared, and applied. The missing link in our security architecture is not the absence of agencies or reports, but the absence of trust, collaboration, and synergy between intelligence managers and policymakers. As Prof. K. L. Fwa of NIPSS reminds us, intelligence does not win wars; it prevents them. Yet, Nigeria continues to experience "surprise" events that intelligence was meant to forestall.

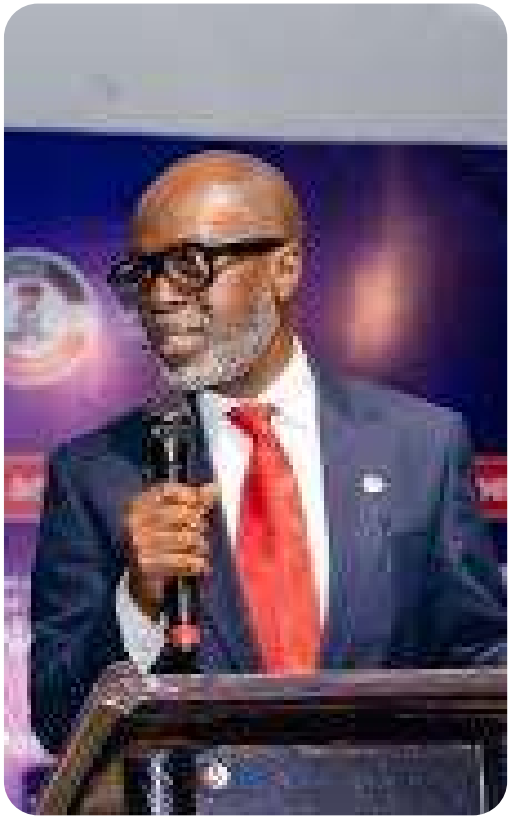
Nigeria's insecurity is not just a failure of weapons or manpower; it is a failure of intelligence management and its connection to policy. Our agencies collect vast amounts of information, yet policymakers are often "surprised" by crises that could have been prevented.

This edition brings together nine powerful voices, from security professionals, academics, and practitioners, who dissect Nigeria's challenges and propose pathways for reform. Their insights converge on one urgent message: Nigeria must evolve from reactive responses to proactive intelligence-led governance.

NIGERIA'S INTELLIGENCE REVIEW

Kayode Bolaji, the Executive Director of Peace Building Development Consult and course Director of the Leadership Course in Criminal and Security Intelligence Management and the Commandant, Defence Intelligence College, Admiral EE Effa both highlighted that the aim of the course is to discuss the place of intelligence in operations. We all know that the country is bedevilled with security issues in almost every zone of the country, and operations are ongoing to combat the myriads of insecurities. However, the principal thing is that intelligence drives operation and for us to enhance our operational successes, we need to focus on intelligence.

Feature 1: Robotics, Machine Learning, and AI in Intelligence
(Timothy O. Avele, CEO Agent-X Group)
Avele champions AI, ML, and robotics as game changers for Nigeria's intelligence community. From predictive analytics to robotic drones, the possibilities are vast. But weak infrastructure, foreign dependence, and ethical dilemmas must be addressed. He remarked that Artificial Intelligence (AI), Machine Learning (ML), and Robotics are redefining intelligence operations globally. For Nigeria, adopting these technologies could transform counter-insurgency, border security, and economic intelligence.
Applications already in view:
a.AI-based predictive analytics to detect insurgency patterns.
b.Robotic drones for Niger Delta patrols and border surveillance.



c.ML-driven fraud detection in the oil sector.
d.A proposed Nigerian Joint All-Domain Command and Control (NJADC2) system linking DSS, DIA, NIA, Police, EFCC, Customs, and Immigration into one real-time intelligence-sharing platform.
Yet, Nigeria faces challenges: weak infrastructure, shortage of skilled AI professionals, and risks of over-dependence on foreign technologies. Ethical dilemmas also loom, from AI bias to privacy concerns.

Avele argues Nigeria must:
a.Build local AI capacity via universities and startups.
b.Align deployments with Nigeria's National AI Strategy.
c.Ensure policies emphasize ethics, transparency, and sovereignty.
The message is clear: AI is not a replacement for human intelligence, but an augmentation tool. Used wisely, Nigeria can leapfrog into becoming Africa's AI-security hub
Avele's vision makes one fact unavoidable: Nigeria cannot remain a passive consumer of foreign AI systems. If intelligence remains human-driven while adversaries deploy autonomous drones and predictive algorithms, Nigeria risks strategic irrelevance. The way forward is deliberate adoption: invest in robotics for border patrol, AI for cyber-intelligence, ML for financial forensics - but always underpinned by ethical guidelines and sovereign control. This is not about replacing human intelligence but augmenting it with super-intelligence tools. If implemented wisely, Nigeria could leapfrog into becoming Africa's hub for AI-driven security. If ignored, it risks being outpaced not only by terrorists but by rival states.
Mr Timothy Avele emphasis how as intelligence agency can incorporate local solution to the rising challenges in insecurities in Nigeria, whereby they can build programs locally to solve teaching problems. He remarked that the participants, were really enthusiastic about the course and were willing to make a lot of improvement and even make sacrifices so that they can apply the things they learn in robotics, artificial intelligence, machine learning and other security courses. Thus, the course will breed new officers with new skills.

Feature 2: Cyber Warfare and National Security
(Gen. Nnorom)
Advances in ICT have transformed not only economies but also the battlefield. Cyber warfare — the use of computer network attacks and defences to achieve political or military objectives — has emerged as one of the defining security challenges of our time. He identified the Key Attributes of Cyber Warfare
a.Covert or Overt: Attacks may be hidden or declared depending on political intent.
b.State or Non-State Actors: Nation-states, terrorist groups, or even criminal syndicates can wage cyber campaigns.

NIGERIA'S INTELLIGENCE REVIEW

Standalone or Blended: Cyber-attacks may occur independently or alongside traditional kinetic warfare.
d.Diverse Targets: From critical infrastructure to financial systems and military networks.
e.Sustained Campaigns: Not one-off hacks, but long-term operations designed to cripple adversaries.
Gen. Nnorom's paper is a stark reminder that Nigeria's digital battlefield is as real as its physical one. While insurgents terrorize villages and criminals exploit porous borders, unseen adversaries probe banks, ministries, and infrastructure.
The lesson is clear: without a credible cyber defence strategy — and offensive capabilities to deter adversaries — Nigeria risks economic paralysis and strategic irrelevance. Cyber warfare is not tomorrow's war; it is today's war, unfolding silently in our servers, cables, and networks.

Gen. Nnorom's paper is a stark reminder that Nigeria's digital battlefield is as real as its physical one. While insurgents terrorize villages and criminals exploit porous borders, unseen adversaries probe banks, ministries, and infrastructure.
The lesson is clear: without a credible cyber defence strategy — and offensive capabilities to deter adversaries — Nigeria risks economic paralysis and strategic irrelevance. Cyber warfare is not tomorrow's war; it is today's war, unfolding silently in our servers, cables, and networks.

Feature 3: Privacy and Intelligence Sharing in Nigeria's War on Terror
(Godwin Bassey Eteng, ADG Rtd, fsi, PhD)
Eteng highlights Nigeria's greatest weakness: intelligence hoarding and poor sharing. He calls for a National Intelligence Fusion Centre, legal frameworks for sharing, cybersecurity investments, and culture change. Eteng's argument is a sobering reminder that Nigeria's greatest weakness in counterterrorism is not a lack of information, but the failure to share and act on it collectively. He makes a strong case that until intelligence is treated as a national asset, agencies will continue to guard it as turf, undermining the fight against terrorism.

NIGERIA'S INTELLIGENCE REVIEW

The tension between privacy and intelligence sharing is also critical. Nigeria cannot afford a surveillance state that erodes civil liberties, yet it cannot fight 21st-century terror threats without big data analysis. Eteng urges policymakers to legislate clear privacy safeguards, while also mandating inter-agency cooperation.

His most powerful point is cultural: the intelligence war will not be won by technology alone, but by trust. Without institutional trust between producers and consumers of intelligence, even the most advanced systems will fail.

Feature 4: Espionage and Statecraft in Nigeria's Foreign Policy
(Prof. Efem N. Ubi, PhD, NIIA Lagos)

Ubi situates intelligence as both defence and diplomacy. Nigeria relies heavily on foreign partners, but this dependence undermines sovereignty. Rivalry, politicization, and weak oversight worsen the problem. Ubi's study forces us to confront a critical paradox: Nigeria wants to project strength as a regional leader, yet its intelligence system often betrays weakness at home. The DSS, NIA, and DIA are powerful on paper, but in reality, they mirror Nigeria's political struggles, fragmentation, corruption, and partisan misuse.

The reliance on foreign powers is another sore point. While satellite feeds from Washington or maritime intel from Europe strengthen Nigeria's fight against Boko Haram and piracy, they also highlight Nigeria's technological dependence. In intelligence, dependence is vulnerability.

NIGERIA'S INTELLIGENCE REVIEW

Perhaps the sharpest insight here is the blending of espionage with diplomacy. Embassies as intelligence hubs, covert cooperation in ECOWAS, and secret deals with Western partners underscore how much of Nigeria's foreign policy is driven not in press conferences, but in classified cables and encrypted channels. Ubi's recommendations are sound: coordination, capacity-building, oversight. But the real reform must be cultural, Nigeria's intelligence must be professionalized and depoliticized if it is to earn credibility abroad. Until then, Nigeria risks being seen as both a partner and a liability in global intelligence cooperation.

Feature 5: Bridging the Gap: Intelligence Managers and Policymakers
(Prof. K. L. Ewa, PhD, NIPSS Kuru)
Ewa underscores Sherman Kent's principle: the fragile relationship between intelligence managers and policymakers. In Nigeria, mistrust, poor communication, and politicization distort this relationship, creating cycles of failure. Prof. Ewa's intervention strikes at the heart of Nigeria's intelligence dilemma: the disconnect between producers and consumers. Analysts labour to provide foresight, but policymakers often sideline or politicize the outputs. The result is a cycle of blame and surprise: intelligence is accused of failure when, in reality, the failure is political inaction. This piece is a sharp reminder that intelligence is not magic, it is advisory, not executive. Nigeria's security breakdowns—whether in counterterrorism, communal violence, or organized crime, reflect not just intelligence weaknesses, but a breakdown in trust and collaboration between managers and decision-makers.
The solutions Ewa offers are pragmatic: clearer terms of engagement, interoperable systems, trust-building, and doctrinal frameworks to replace ad hoc arrangements. But the deeper challenge is cultural. As long as policymakers treat intelligence as a political weapon rather than a strategic compass, Nigeria will continue to stumble from one surprise to the next.

NIGERIA'S INTELLIGENCE REVIEW

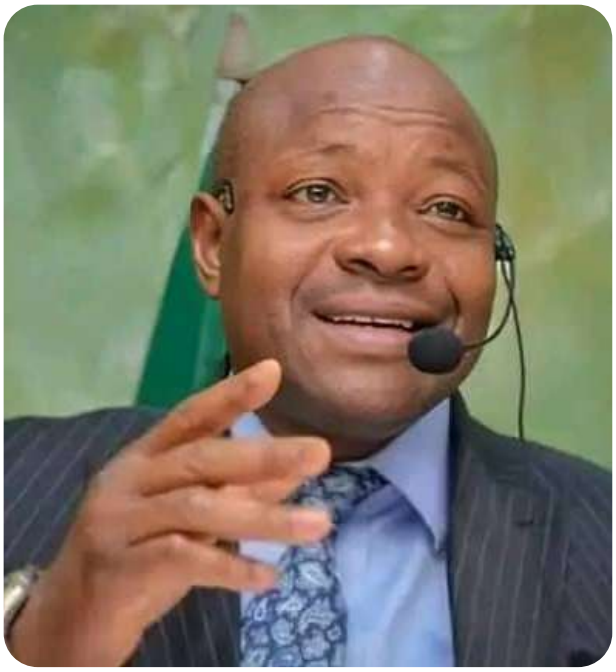
His key point: intelligence does not fail Nigeria—Nigeria fails its intelligence.

Feature 6: The Global Evolution of Intelligence
(DIG Ben Nebolisa Okolo, PhD)
From the Renaissance through the Cold War to the digital age, intelligence has been the heartbeat of statecraft. Okolo traces intelligence from the Renaissance through the Cold War to today's digital age. He highlights rising threats: data breaches and insider threats, terrorist networks that thrive on disinformation, climate-induced conflicts and pandemics that cross borders. cyber warfare and climate change. These risks challenge traditional models of intelligence. His call is clear: intelligence reform must focus on governance, synergy, cyber defence, and regional cooperation. Without these, Nigeria will remain reactive instead of proactive in global security dynamics.
His key point: Nigeria has structures but not systems; reforms without enforcement will only recycle the failures of the past

Feature 7: Nigeria's Intelligence Gap – Structures Without Strategy
(Maj Gen G. Oyefesobi, DSS)
Oyefesobi makes a sharp distinction: information is raw, intelligence is refined, contextual, and actionable. He warns that Nigeria confuses information for intelligence. Over-reliance on HUMINT, neglecting TECHINT and OSINT. Poor analysis culture and politicization of findings. Stove-piping between agencies, creating duplication. He stresses that modern threats require multi-dimensional security, political, cyber, economic, societal, and environmental.

NIGERIA'S INTELLIGENCE REVIEW

Maj Gen G. Oyefesobi expertise remark: Fighting 21st-century threats with 20th-century methods is a recipe for failure. Intelligence without analysis is noise; analysis without policy is wasted effort.



Feature 8: Intelligence as the Operational Backbone
(Ikenweiwe, DSS)
Intelligence is not just an input to operations; it is the spinal cord of security strategy. From counterterrorism to crime prevention, Ikenweiwe stresses that intelligence provides: Early warning, Situational awareness, Operational targeting.
His professional note: If operations are carried out without intelligence, they amount to blind reactions. Nigeria must fund, train, and professionalize its intelligence cadres - not just expand its military footprint.

Feature 9: The Future of Crime Mapping and GEOINT
(Ojo, Defence Space Administration)
Ojo emphasizes the power of geospatial intelligence (GEOINT) to map crime hotspots, track insurgents, and forecast threats. Nigeria has begun experimenting with satellite imagery and data-driven policing, but challenges remain: Limited infrastructure; Low local expertise; Fragmented adoption across agencies.
His insight thought: In the age of drones, encrypted apps, and cryptocurrencies, data-driven intelligence is non-negotiable. Without GEOINT, security forces will always arrive late, after the damage is done.

NIGERIA'S INTELLIGENCE REVIEW

Closing Reflection

Nigeria does not lack intelligence agencies, reports, or structures. It lacks collaboration, trust, and accountability. Intelligence must be timely, accurate, and actionable — but more importantly, it must be used. The combined insights from these thought leaders paint a single truth: Nigeria's intelligence ecosystem must transform or risk irrelevance. From geopolitics to cyber warfare, from espionage diplomacy to AI, the terrain is shifting rapidly. Espionage diplomacy strengthens policymaker collaboration. GEOINT expands our vision of the battlefield. Cyber warfare demands digital resilience. AI and robotics point to the future of security. Failure to adapt risks strategic irrelevance. But with bold reforms, capacity building, and technology adoption, Nigeria can move from a reactive to a proactive intelligence posture.

The way forward demands:

a.Stronger inter-agency collaboration and between intelligence managers and policymakers.

1. Technology adoption rooted in local capacity.
2. Trust-building and depoliticization of intelligence.
3. Clear legal frameworks and oversight.
4. Reform intelligence laws.
5. Invest in technology.
6. Train analysts, not just collectors.
7. Use intelligence for foresight, not hindsight.

If Nigeria invests in these pillars, it can shift from a reactive posture to proactive leadership in African and global security. Nigeria's problem is not the absence of intelligence — it is the absence of collaboration, trust, and application. The future of Nigeria's security depends not on out-gunning adversaries, but on out-thinking them. In the end, the strength of Nigeria's intelligence will not be measured by how much information it gathers, but by how effectively that information shapes wise decisions

"NIGERIA'S SECURITY FUTURE LIES NOT IN OUTGUNNING ADVERSARIES, BUT IN OUT-THINKING THEM THROUGH INTELLIGENCE, TECHNOLOGY, AND TRUST. THUS, INTELLIGENCE DOES NOT FAIL NIGERIA—NIGERIA FAILS ITS INTELLIGENCE."