DISINFORMATION, INTELLIGENCE FAILURE, AND SECURITY GOVERNANCE IN NIGERIA:
AN INTEGRATED ANALYSIS OF INFORMATION RISKS, PUBLIC TRUST, AND STRATEGIC RESPONSES TO TERRORISM, INSURGENCY, BANDITRY, COMMUNAL VIOLENCE, AND VIOLENT CONFLICT

Barrister Adebayo Akinade, dfisn
Deputy President & Chief Executive,
Institute of Security Nigeria
Email: bayoakinade77@gmail.com / bayoakinade@yahoo.co.uk

Abstract

Nigeria's contemporary security environment is defined by the convergence of kinetic violence and information disorder. Terrorism, insurgency, banditry, kidnapping, communal violence, and violent conflict are increasingly amplified by disinformation, misinformation, and institutional communication failure. This position paper integrates 17 publications authored between 2007 and 2025 to construct a comprehensive framework for understanding and mitigating information risks. Drawing on theories of human security, strategic security management, intelligence systems, community policing, and performance culture, the paper examines the mechanisms through which disinformation erodes public trust, diverts operational resources, and exacerbates violence. The May 2026 killing of Mathematics teacher Michael Oyedokun in Oyo State is used as a case study to illustrate intelligence failure, delayed crisis communication, and the politicization of insecurity. The paper concludes with a policy framework centered on a National Information and Intelligence Fusion Centre, professionalized crisis communication, standardized documentation, community policing, and governance reform.

Keywords: Disinformation, Intelligence Fusion, Intelligence Failure, Strategic Security, Community Policing, Terrorism, Communal Conflict, Public Trust, Nigeria

1. Introduction

Nigeria faces a dual security challenge. The first is physical: Boko Haram and ISWAP insurgency in the North East, banditry and kidnapping in the North West and North Central, and rising communal violence and abductions in the South West and South East. The second is informational: the rapid spread of unverified security alerts, crisis misinformation, and deliberate disinformation through social media and encrypted messaging platforms.

The killing of Michael Oyedokun, a Mathematics teacher at Community High School, Ahoro-Esinele, Oriire Local Government Area, Oyo State, in May 2026, and the subsequent circulation of videos of his abduction and execution, exemplifies this convergence. The incident triggered public panic, political accusations, and a 72-hour delay in official communication. The event reveals how intelligence failure, fragmented communication, and governance deficits interact to amplify insecurity.

This paper argues that information risks are not peripheral to Nigeria's security crisis but are central to it. It synthesizes 17 publications by the author from 2007 to 2025 to propose an integrated model of security governance that treats information risk management as a core function of the state. The paper is structured into seven sections: theoretical foundations, anatomy of disinformation, operational impacts, institutional roles, intelligence fusion and failure, policy framework, and conclusion.

2. Theoretical and Conceptual Foundations

2.1 Human Security and Sustainable Development

Social and Human Security for Sustainable Development (2007) reframes security from state-centric defense to the protection of individuals and communities from physical, economic, and psychological threats. National Security, Social Coercion and Sustainable Development (2008) extends this by arguing that social exclusion and coercive governance create grievances that disinformation exploits. Disinformation targeting specific ethnic or religious groups can trigger communal violence, undermining human security and sustainable development.

2.2 Strategic Security Management and Statecraft

Managing Strategic Security and Crime Prevention Models (2017) and Managing Strategic Security in Statecraft, Public Affairs and Foreign Relations (2019) position security as a function of integrated planning, risk assessment, performance management, and public affairs. Information risks must be managed as strategic variables, not ad hoc public relations issues. Contemporary Security Issues in Governance and Statecraft (2017, 2018) demonstrates that governance failure creates permissive environments for both kinetic and informational threats.

2.3 Community Policing and Trust

Community Policing: Strategic Approaches In Crime Prevention (2018) establishes that public trust is a force multiplier. When trust erodes, communities withhold information, and the intelligence cycle breaks down. Public Policing and Private Protection For Maximum Security (2017) argues for harmonized roles

between public police and private security providers to ensure consistent messaging and coordinated response.

2.4 Performance Culture and Governance

Security Operations, Crime Prevention and Good Governance: Pattern and Trends (2007) and Standard Performance Culture For Security Personnel and Organisations (2021) link operational effectiveness to transparency, accountability, and measurable standards. Low performance culture weakens the credibility of official communication, creating space for rumours and conspiracy theories.

2.5 Communication, Diplomacy, and Documentation

Security Culture, Diplomacy and Communication Skills in International Relations (2008) positions strategic communication and public diplomacy as non-kinetic tools of security management. Communications in Security and Law Enforcement Operations (2025) outlines protocols for unified crisis communication across agencies. Communication Skills in Security Documentation in Law Enforcement (2025) emphasizes that accurate, timely documentation is essential for accountability, legal proceedings, and public assurance.

2.6 Intelligence Systems

Intelligence System: Principles and Practice (2015) defines intelligence as the product of processed, analyzed information that meets criteria of accuracy, relevance, timeliness, and usability. It identifies compartmentalization, poor dissemination, and weak analytical capacity as primary sources of intelligence failure. Security and Criminal Intelligence For Law Enforcement (2021) applies these principles to criminal intelligence, outlining the intelligence cycle and the legal-ethical framework for its use in countering terrorism, banditry, and organized crime.

2.7 Asymmetric Threats and Communal Violence

Policing Terrorism, Insurgency and Weapons of Mass Destruction (2023) analyzes terrorism and insurgency as asymmetric threats that exploit state vulnerabilities, including information gaps. Communal Conflict and Violence: Response, Resolution and Prevention (2009) examines the drivers of communal violence and proposes early warning and mediation mechanisms. Disinformation is identified as a catalyst that can rapidly escalate localized disputes into widespread violence.

2.8 Agrosecurity and Non-Traditional Threats

Agrosecurity, Bioterrorism and Environmental Protection (2019) expands the threat landscape to include food security, bioterrorism, and environmental sabotage. False information about contamination or disease outbreaks can trigger public health crises and economic disruption comparable to physical attacks.

3. Anatomy and Impact of Security-Related Disinformation

Disinformation in Nigeria’s security context typically exhibits three features: threat inflation, false authority, and actionable panic. The May 2025 message alleging mass infiltration of Boko Haram fighters into Lagos, Ilorin, and Rivers State, and the May 2026 videos of Oyedokun’s abduction and execution, illustrate these features.

Impacts and Effects

1. Operational Diversion: Security personnel are diverted from genuine threats to verify false alarms, reducing readiness against terrorism, banditry, and kidnapping.
2. Public Panic and Economic Disruption: Avoidance of markets, schools, and public gatherings causes economic losses and social dislocation.
3. Erosion of Trust: Repeated false alarms create "alert fatigue," making the public less responsive to genuine warnings.
4. Escalation of Communal Violence: Messages specifying regions or ethnic groups can trigger reprisals, as analyzed in Communal Conflict and Violence (2009).
5. Legal and Evidentiary Weakness: Poor documentation weakens prosecution of those who originate malicious falsehoods, per Communication Skills in Security Documentation (2025).
6. Exploitation of Grievances: Disinformation thrives where governance failure, exclusion, and coercion exist, as argued in National Security, Social Coercion and Sustainable Development (2008).

4. Role of Security Personnel and Organizations

4.1 Operational Response

Communications in Security and Law Enforcement Operations (2025) emphasizes that rapid verification, containment, and neutralization require unified command-and-control communication and inter-agency coordination. Fragmented communication channels compound operational delays during crises.

4.2 Communication and Public Assurance

Security organizations must provide timely, accurate, and accessible information. Managing Strategic Security in Statecraft, Public Affairs and Foreign Relations (2019) positions public communication as a core function of statecraft. Failure creates an information vacuum filled by rumour and disinformation.

4.3 Documentation and Accountability

Accurate incident reporting, intelligence briefs, and public debunk statements are essential for accountability and legal proceedings. Communication Skills in Security Documentation in Law Enforcement (2025) provides protocols for chain-of-custody, evidence handling, and public communication standards.

4.4 Community Engagement and Public-Private Cooperation

Community Policing: Strategic Approaches In Crime Prevention (2018) shows that trusted community actors are critical in countering rumours at the grassroots level. Public Policing and Private Protection For Maximum Security (2017) advocates for harmonized roles to ensure consistent messaging and coordinated response across public and private actors.

5. Intelligence Fusion, Intelligence Failure, and Information Risk Management

5.1 Intelligence Fusion

Intelligence System: Principles and Practice (2015) defines intelligence fusion as the process of integrating data from human intelligence, signals intelligence, open-source intelligence, community reports, and digital

forensics into a coherent analytical product. Fusion reduces duplication, resolves contradictions, and produces actionable intelligence for decision-makers.

In the context of information risks, fusion is critical for rapid verification of viral security alerts. When NPF, DSS, NEMA, and cyber units operate in silos, unverified messages circulate longer and reach wider audiences before official debunks are issued.

5.2 Intelligence Failure

Security and Criminal Intelligence For Law Enforcement (2021) identifies intelligence failure as the breakdown in collection, analysis, dissemination, or use of intelligence that leads to inaccurate assessments or delayed responses. Common causes include compartmentalization, confirmation bias, poor communication, and weak documentation.

The May 2026 Oyo incidents demonstrate this failure. Multiple abductions occurred along the CRIN corridor between March and May 2026, yet no fused assessment triggered a preventive operation. The killing of Oyedokun was followed by a 72-hour delay in official communication, allowing competing narratives to dominate public discourse.

5.3 Link to Operational and Trust Outcomes

Intelligence failure diverts resources from genuine threats such as terrorism, banditry, and kidnapping. Policing Terrorism, Insurgency and Weapons of Mass Destruction (2023) shows that terrorist groups exploit this distraction to execute attacks. When fused intelligence is not communicated effectively, public trust declines. Community Policing (2018) argues that trust is a precondition for community intelligence, which in turn feeds the fusion process.

5.4 Documentation as Mitigation

Communication Skills in Security Documentation in Law Enforcement (2025) provides protocols for recording debunks, incident timelines, and analytical judgments. Proper documentation reduces the risk of repeating intelligence failure and provides legal evidence for prosecuting those who originate malicious falsehoods.

6. Case Study: The Killing of Michael Oyedokun and the Oyo Security Crisis, May 2026

6.1 Incident Overview

On May 15, 2026, bandits abducted teachers and pupils from Community High School, Ahoro-Esinele, Oriire LGA, Oyo State. Michael Oyedokun, a Mathematics teacher, was executed days later. Viral videos of his plea and execution circulated widely. The Oyo State Government and federal authorities issued statements approximately 72 hours after the attack.

Between March and May 2026, at least four other abductions occurred along the CRIN corridor in Idi-Ayunre, Ibadan. On May 16, Adeleke Ridwan Olayemi was abducted, with ransom demands escalating from ₦15 million to ₦20 million. A Mazda driver was found murdered with bullet wounds in a nearby bush.

6.2 Analysis Through the Integrated Framework

Intelligence Failure: The pattern of abductions along a defined corridor indicates a failure of tactical intelligence fusion. Intelligence System: Principles and Practice (2015) argues that such patterns should trigger preventive operations and early warning to communities.

Communication Lag: The delayed response reflects the communication gaps identified in Communications in Security and Law Enforcement Operations (2025). The absence of timely, unified messaging created space for political accusations that the state was targeted for being non-federal-compliant.

Politicization of Insecurity: Communal Conflict and Violence (2009) warns that when political competition overlaps with insecurity, rumors become weapons. The suggestion that the attacks were politically orchestrated illustrates this risk.

Anti-Education Targeting: The killing of a Mathematics teacher aligns with Boko Haram's ideological opposition to Western education, as analyzed in Policing Terrorism, Insurgency and Weapons of Mass Destruction (2023). Such attacks aim to break the link between state and community development.

Trust Erosion: Community Policing (2018) notes that when citizens perceive government as prioritizing politics over protection, community cooperation collapses, reducing the intelligence flow needed to counter banditry.

7. Integrated Policy Framework for Managing Information Risks

7.1 National Information and Intelligence Fusion Centre

Establish a centre with the mandate to aggregate open-source, social media, and agency intelligence on viral security alerts within two hours of detection. Produce and disseminate fused assessments to all security agencies and the public via verified channels. This operationalizes the principles in Intelligence System: Principles and Practice (2015) and addresses failure points identified in Security and Criminal Intelligence For Law Enforcement (2021).

7.2 Professionalized Crisis Communication

Establish 24/7 public information units with standardized crisis messaging protocols, as recommended in Communications in Security and Law Enforcement Operations (2025) and Security Culture, Diplomacy and Communication Skills (2008). Protocols should include pre-approved templates for abduction, killing, and mass casualty incidents.

7.3 Standardized Documentation and Evidence Management

Implement standardized formats for incident reports, intelligence briefs, and public statements. Maintain a public archive of debunks and incident reports, following the protocols in Communication Skills in Security Documentation in Law Enforcement (2025).

7.4 Deepened Community Policing

Build trust through problem-oriented policing and local partnerships, as detailed in Community Policing (2018). Trusted community actors are critical in countering rumours and providing early warning.

7.5 Public-Private Security Cooperation

Harmonize roles between public police and private security providers to ensure consistent messaging and coordinated response, per Public Policing and Private Protection (2017).

7.6 Strategic Security Planning

Incorporate information risk assessment into strategic security planning using the models in Managing Strategic Security and Crime Prevention Models (2017) and Managing Strategic Security in Statecraft (2019).

7.7 Governance and Human Security Reform

Apply the governance and human security frameworks in Contemporary Security Issues on Governance and Statecraft (2018), National Security, Social Coercion and Sustainable Development (2008), and Security Operations, Crime Prevention and Good Governance (2007) to reduce the grievances that disinformation exploits.

7.8 Legal and Policy Response

Apply the Cybercrimes Act 2015 proportionately against deliberate creation and dissemination of security hoaxes, while safeguarding freedom of expression and avoiding the criminalization of legitimate reporting.

8. Discussion

The Oyo case study demonstrates that Nigeria's security crisis cannot be addressed through kinetic response alone. Intelligence failure, communication lag, and governance deficit create conditions where disinformation thrives and violence escalates. The integrated framework proposed here treats information risk management as inseparable from operational security.

Security and Criminal Intelligence For Law Enforcement (2021) argues that intelligence-led policing requires not only data but also the capacity to communicate findings to both operational commanders and the public. Communications in Security and Law Enforcement Operations (2025) provides the mechanism for this communication. Without both, the state cedes the information domain to non-state actors.

Furthermore, National Security, Social Coercion and Sustainable Development (2008) reminds us that sustainable solutions require addressing the root causes of distrust. Governance reform, inclusive development, and accountability are not separate from security but are prerequisites for it.

9. Conclusion

Disinformation, miscommunication, and intelligence failure are integral to Nigeria's security challenges. They amplify the impact of terrorism, insurgency, banditry, kidnapping, communal violence, and violent conflict by eroding trust, diverting resources, and paralyzing public response.

Addressing these challenges requires a shift from reactive policing to strategic security governance. This governance model must integrate intelligence fusion, professional communication, accurate documentation,

community trust-building, inter-agency coordination, and governance reform. The body of work from 2007 to 2025 provides a comprehensive roadmap for this transition.

Securing Nigeria's information environment is now as critical as securing its territory. The state must act to close the gap between intelligence, communication, and public trust, or risk losing all three.

References

1. Akinade, A. (2007). Security Operations, Crime Prevention and Good Governance: Pattern and Trends. Lagos: ISN Publications Series.
2. Akinade, A. (2008). National Security, Social Coercion and Sustainable Development: Panacea to Conflict, Violence and Xenophobia. Lagos: ISN Publications Series.
3. Akinade, A. (2008). Security Culture, Diplomacy and Communication Skills in International Relations. Lagos: ISN Publications Series.
4. Akinade, A. (2009). Communal Conflict and Violence: Response, Resolution and Prevention. Lagos: ISN Publications Series.
5. Akinade, A. (2015). Intelligence System: Principles and Practice. Lagos: ISN Publications Series.
6. Akinade, A. (2017). Public Policing and Private Protection For Maximum Security. Lagos: ISN Publications Series.
7. Akinade, A. (2017). Managing Strategic Security and Crime Prevention Models. Lagos: ISN Publications Series.
8. Akinade, A. (2017). Contemporary Security Issues in Governance and Statecraft. Lagos: ISN Publications Series.
9. Akinade, A. (2018). Community Policing: Strategic Approaches In Crime Prevention. Lagos: ISN Publications Series.
10. Akinade, A. (2018). Legal and Forensic Issues in Elections and Peace Education. Lagos: ISN Publications Series.
11. Akinade, A. (2019). Agrosecurity, Bioterrorism and Environmental Protection. Lagos: ISN Publications Series.
12. Akinade, A. (2019). Managing Strategic Security in Statecraft, Public Affairs and Foreign Relations. Lagos: ISN Publications Series.
13. Akinade, A. (2021). Security and Criminal Intelligence For Law Enforcement. Lagos: ISN Publications Series.
14. Akinade, A. (2021). Standard Performance Culture For Security Personnel and Organisations. Lagos: ISN Publications Series.
15. Akinade, A. (2023). Policing Terrorism, Insurgency and Weapons of Mass Destruction. Lagos: ISN Publications Series.
16. Akinade, A. (2025). Communications in Security and Law Enforcement Operations. Lagos: ISN Publications Series.
17. Akinade, A. (2025). Communication Skills in Security Documentation in Law Enforcement. Lagos: ISN Publications Series.
18. Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, Etc.) Act.

19. Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Council of Europe.
20. Huntington, S. (1957). The Soldier and the State: The Theory and Politics of Civil-Military Relations. Cambridge, MA: Harvard University Press.
21. Adedayo, F. (2026, May 24). Boko Haram's slaughter of Mathematics in Oyo. The Cable.

Appendices

Appendix A: Protocol for Rapid Verification and Debunking of Security Hoaxes
Appendix B: Template for Public Security Communication and Crisis Messaging
Appendix C: Checklist for Lawful and Admissible Security Documentation
Appendix D: Framework for National Information and Intelligence Fusion Centre
Appendix E: Community Early Warning and Mediation Model for Communal Conflict Prevention
Appendix F: Performance Indicators for Information Risk Management in Security Agencies.

Barrister Adebayo Akinade, dfisn
Deputy President & Chief Executive
Institute of Security Nigeria