VOL. 11 NO. 6,
FEBRUARY, 2026
E-ISSN 3027-1401
P-ISSN 3026-9148

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Arts and Sociological Research (JASR)

Leveraging Technology to Combat Insecurity and Boko Haram Activities in Northeastern Nigeria

Akilu Umar Bakari; Aliyu Kolo Abana; & Habiba Inuwa Sani

School of Information and General Studies, Department of General Studies, Federal Polytechnic Bali.

Corresponding Author: akiluumarbakari33@gmail.com

DOI: https://doi.org/10.70382/ajasr.v11i6.0107

Abstract

This study investigates how technology might be strategically used to solve the ongoing insecurity caused by Boko haram and kidnapping in northeastern Nigeria. Severe acts of terrorism have occurred in the area over the years, leading to fatalities, displaced people, and economic hardships. The research explores the ways in which technological tools like satellite surveillance, drone operations, biometric systems, and communication intercepts have been used to improve intelligence collection, monitor insurgent movements, and assist military operations because conventional security measures have proven inadequate. The advent of Boko Haram and banditry in Nigeria has exacerbated the relationship between technology and terrorism. The technologies found in this study support and strengthen Boko Haram's activities and the associated counterterrorism initiatives. It looks at Boko Haram's use of sophisticated weapons like drones and improvised explosive devices (IEDs), as well as social media for recruitment and messaging that has been programmed for safe communication. Issues like inadequate infrastructure, cyber vulnerabilities, and a lack of coordination among security agencies are also highlighted in the study. Using both qualitative and secondary data sources, the study critically assesses the effectiveness of these technologies in real time threat detection and response. It concludes by recommending the need for increased investment in digital security infrastructure, inter agency collaboration, and capacity building to fully leverage technology in the fight against terrorism in the region.

Keywords: technology, insecurity, boko haram, north-eastern, Nigeria.

Introduction

The United States campaign in Vietnam in the 1960s is a prime example of a COIN operation, which is an attempt to weaken, destroy, and ultimately defeat insurgency. Insurgency is a violent uprising against a constituted government authority, and attacks on public facilities and utilities are carried out with the sole purpose of undermining public confidence in the government. The United States military's failure to win over the public's hearts and minds was a major factor in the COIN operation's failure (Roland, 2016). However, the British campaign in Northern Ireland, where the primary tactic was to "Win Hearts and Minds" (WHAM) the local populace, stands out as one of the most successful COIN operations in history. This led Gianluca (2018: 1) to assert that insurgency entails comprehending the rebels through methods and policies designed to deter them from fighting and, in the end, win the hearts and minds of the populace. The advent of Boko Haram and its effects on Central Africa highlight a significant aspect of modern conflict, where terrorism and technology are increasingly intertwined. The Lake Chad Basin is now home to the Islamist insurgent group Boko Haram, which originated in northeastern Nigeria and now operates in Cameroon, Chad, and Niger. This growth has not only increased regional instability but also demonstrated the group's skill at using contemporary technologies to expand its operational reach and impact. In order to recruit new members, coordinate assaults, and spread propaganda, the group has made extensive use of social media channels. This strategy reflects the methods used by other international terrorist groups, demonstrating how technology has enabled the convergence of local and international terrorism techniques (Freeman, 2017). A notable illustration of Boko Haram's technical integration is its skillful use of encrypted messaging apps to guarantee safe routes of communication. It's has made it possible for the organization to plan intricate operations and avoid security authorities' scrutiny. Given the situation in Central Africa, where technology infrastructure is frequently underdeveloped and government agencies might not have the resources and know-how to adequately monitor and block such advanced communication techniques, the adoption of these applications is especially important. Boko Haram's tactical capabilities have also significantly evolved with the deployment of sophisticated weapons, such as drones and improvised explosive devices (IEDs). In a noteworthy event in 2018, Boko Haram attacked a military base in Nigeria's Borno State, using drones for coordination and surveillance. Not only did this strategic use of technology improve their operational effectiveness, but it also presented a serious obstacle to the security forces, who were unprepared for this degree of technological sophistication.

In response, a number of technological countermeasures have been put in place by international organizations and Nigerian governments to lessen the threat posed by Boko Haram. To monitor and stop terrorist operations, surveillance technology, cyber intelligence, and data analytics have been used (Ekumaoko et al., 2021). For instance, the Multinational Joint Task Force (MNJTF), which consists of soldiers from Nigeria, Niger, Chad, Cameroon, and Benin, has become more and more dependent on

platforms for intelligence sharing and aerial surveillance in order to locate and attack Boko Haram hideouts. Despite these attempts, a number of challenges, such as a lack of resources and the rapidly changing technology threats posed by Boko Haram, frequently hinder the efficiency of such safeguards (Anzalone, 2018). The group's capacity to quickly adjust and embrace new technology usually surpasses state actors' responses, posing a chronic and ever-changing threat to regional security.

Technology has changed the criminal justice system by opening up new avenues for dealing with criminal activity (Husson, 2023). Key components of technology deployment that have had a favourable effect on reducing crime and making labour less taxing in the process of administering justice are: Among the cutting-edge technologies examined in this study are facial recognition, automated license plates, fast identification systems, and improved body cameras for surveillance and monitoring. Every community, country, and the world at large has rules that govern how people, organizations, or nations should behave in their interactions with one another. These rules are meant to be followed. Any behaviour that deviates from the norms, values, or regulations that these groups of people or nations uphold will be considered disobedience or a violation of those rules, and those who violate them will face consequences such as penalties, rapprochement, admonition, etc. Crime is the generic phrase used to describe disobedience, no observance, or a breakdown of law and order. Any guilty act or omission that is illegal and subject to state punishment is referred to as a crime. Crime varies with time and may not be the same in one area as it is in another. According to Zubair (2017), there are four types of crime: crime against a person, crime against property, criminal against a lawful authority, and crime against a local act.

STATEMENT OF THE PROBLEM

Insecurity remains one of the most pressing challenges confronting Nigeria, with the North-Eastern region experiencing prolonged instability largely due to the violent insurgency of Boko Haram. For over a decade, insurgent activities such as terrorism, kidnappings, suicide bombings, destruction of critical infrastructure, and mass displacement of civilians have significantly undermined national security, economic development, and social cohesion in Northeastern Nigeria. Despite sustained military operations and government interventions, Boko Haram has continued to adapt its tactics, exploiting difficult terrain, porous borders, intelligence gaps, and limited technological capacity of security agencies. Traditional security approaches largely dependent on manpower, conventional surveillance, and reactive responses have proven insufficient in effectively predicting, preventing, and neutralizing insurgent threats. This has resulted in delayed responses to attacks, inadequate intelligence gathering, poor coordination among security agencies, and limited protection of civilian populations.

Furthermore, the limited integration of modern technologies such as intelligence surveillance systems, data analytics, unmanned aerial vehicles (drones), biometric systems, and communication technologies has constrained the effectiveness of counter-insurgency efforts. Challenges such as inadequate funding, poor technical expertise, weak infrastructure, cybersecurity risks, and lack of clear policy frameworks have also hindered the adoption of

technology-driven security solutions. The persistent insecurity has led to severe humanitarian consequences, including loss of lives, disruption of education and healthcare, forced migration, food insecurity, and erosion of public trust in government institutions. Therefore, there is a critical need to examine how emerging and existing technologies can be strategically leveraged to enhance intelligence gathering, surveillance, early warning systems, coordination, and overall security operations in combating Boko Haram activities.

This study seeks to address the gap between technological potential and its practical application in Nigeria's counter insurgency efforts, with a focus on developing sustainable, efficient, and context-appropriate technology-driven security solutions for Northeastern Nigeria.

General Objective

The main objective of this study is to examine how technology can be effectively leveraged to combat insecurity and Boko Haram activities in Northeastern Nigeria.

Specific Objectives

The specific objectives of the study are to:

- Assess the current state of insecurity and the operational strategies employed by Boko Haram in Northeastern Nigeria.
- Examine existing security technologies currently used by Nigerian security agencies in counter-insurgency operations.
- Evaluate the effectiveness of modern technologies such as surveillance systems, drones, satellite imaging, data analytics, and communication technologies in preventing and responding to insurgent activities.
- Explore international best practices in the use of technology for counter-terrorism and insurgency management.
- Propose strategic and policy oriented recommendations for integrating advanced technologies into Nigeria's security framework to sustainably combat Boko Haram insurgency.

LITERATURE REVIEW

Technology, particularly information technology, can be used to combat crime in a variety of ways. These include using communication devices to collect, store, retrieve, process, analyse, and transfer data, among other uses. These procedures can be found in gadgets like phones, cameras, computer networks, satellites, and policing activities like maintaining records, CCTV surveillance, fingerprint scanners, speech recognition software, and more (Oyeranmi A. 2018). Traditionally, non-scientific approaches to crime prevention and detection have included foot patrols, community policing, swearing in front of the "god of iron," using sacred texts like the Bible and Qur'an, public humiliation like incarceration, and many more (Omoleke, M. 2017). However, we would first examine what constitutes crime before examining crime prevention and detection. Crime: Any guilty act or omission that is forbidden by law and subject to state

punishment is considered a crime. (A. G. Zubair, 2017). Dambazau has divided crime into four categories, which are as follows:

1. Crime against a person
2. Crime against property
3. Crime against lawful authority
4. Crime against local act Crime against a person includes: Murder, attempted murder, manslaughter, suicide, grievous harm or wounding, assault, child stealing, slave dealing, rape, kidnapping, unnatural offences and others. Crime against property is: burglary, arson, theft or stealing, armed robbery, and more. Falsifying banknotes, gambling, violating the peace, perjury, bribery and corruption, evading arrest, and other offenses are all considered crimes against lawful authority. The following are examples of crimes against locals: traffic violations, township violations, alcohol violations, drug addiction, and other offenses (Ibid: 2017). Furthermore, since 2000, when a new democratic regime was ushered in in Nigeria, the range of crimes has increased, including terrorism, insurgency, drug sales, kidnappings, abductions, human trafficking, armed banditry, and thuggery.

Insecurity and Boko Haram in North-eastern Nigeria

According to Onuoha (2014), the Boko Haram insurgency has caused extensive destruction, displacement, and fatalities. The group's activities take advantage of the northeast's weak monitoring systems, sparse governmental presence, and permeable borders. Researchers such as Aghedo and Osumah (2012) contend that the absence of early warning systems, socioeconomic marginalization, and bad governance are the main reasons why the insurgency persists.

Role of Technology in Security Operations

In today's security responses, technology is essential. Globally, satellite photography, GPS mapping, data analytics, and surveillance drones have been employed to follow insurgent activities and keep an eye on hotspots (Adeleke, 2018). Although efforts to apply such technologies have been made in Nigeria, finance, technical expertise, and coordination problems have hindered their widespread use (Ezeobi, 2020).

Technological Tools for Counter-Insurgency

UAVs and drones: are helpful for surveillance in challenging terrain. Research demonstrates how well they gather intelligence in real time (Okoro, 2021).

Data analysis and mobile phone tracking: Boko Haram has been using mobile phones to hunt down camps and snoop on plans (Chukwuma, 2019).

GIS and satellite imagery: are essential tools for tracking refugee trends, mapping insurgent movements, and estimating damage (Ajaegbu, 2015).

Social Media Monitoring: Security organizations have begun keeping an eye on social media platforms in an effort to counteract Boko Haram's propaganda efforts (Iwuoha & Aniche, 2016).

Challenges in Applying Technology

Despite the potential, several barriers exist:

Data gathering is challenging in rural northeastern Nigeria due to a lack of infrastructure. Information sharing is hampered by coordination inadequacies between local, military, and intelligence institutions (Aliyu, 2022).

Success Stories and Case Studies

Drones and real-time data have been employed by countries like Kenya and Mali to curb insurgent activity. Improved surveillance and foreign tech assistance were partly responsible for Nigeria's 2015 territorial conquests over Boko Haram (International Crisis Group, 2016).

Research Gap

The examined literature emphasizes that although technology has enormous potential to combat insurgency, structural constraints restrict its efficacy in Nigeria. For example, while biometric identification and drone monitoring have proven effective elsewhere in the globe (Aluko, 2020; Yusuf, 2022), their use in Nigeria is limited by a lack of skilled staff and financial limitations. Security services must be proactive rather than reactive in their digital information gathering since rebel groups like Boko Haram have developed the ability to use technology for their own ends (Olowookere, 2019). Additionally, as fragmentation and inadequate communication lessen the impact of technology deployment, there is an increasing need for coordinated actions across security bodies (Ajayi, 2021).

Additionally, the lack of community involvement and the moral dilemmas raised by monitoring technology underscore the necessity of a well-rounded strategy that balances security and human rights. The government must work with the private sector, invest in regional tech solutions, and provide a regulatory framework that encourages creativity, openness, and interagency collaboration in order to close these gaps.

Theoretical Framework

This study is based on Hans Kelsen's (1944) Theory of Shared Security, which holds that governments may maintain peace more effectively when they respond to challenges together rather than separately. In West Africa, where terrorists operates freely across state borders, the fundamental principle that an attack on one is a threat to all strikes a deep chord with current counterterrorism efforts. The insufficiency of unilateral measures is demonstrated by Nigeria's experience with organizations such as Boko Haram and ISWAP. Multilateral projects such as the Multinational Joint Task Force (MNJTF), comprising Benin, Nigeria, Cameroon, Niger, and Chad, represent this group approach. However, as Adela (2023) notes, political mistrust and poor coordination frequently limit their impact. Through coordinated policies, cooperative operations, and intelligence sharing, regional organizations like the African Union and ECOWAS have made an attempt. According to Medu et al. (2023), these initiatives only succeed when participating nations demonstrate political will and make a commitment to common security objectives. In a similar vein, Okpaleke et al. (2023) stress how crucial it is

to use digital tools like AI and drone technology within collaborative frameworks in order to improve regional capability. Soft-power techniques, like coordinated counter-narratives and regional de-radicalization initiatives, are crucial in addition to military methods (Ogunnubi & Aja, 2024). Today's terrorists pose both ideological and physical challenges, and no state can defeat them on its own. As Maniszewska (2024) correctly points out, combating AI-enabled terrorism necessitates cross-border cooperation and pooling of technology resources. The theory provides a theoretical and practical framework for comprehending Nigeria's security initiatives. It reinterprets national security as a regional duty requiring ongoing collaboration, shared investment, and mutual trust.

RESULTS AND FINDINGS

This section presents the findings of the literature review on leveraging technology to combat insecurity and Boko Haram activities in Northeastern Nigeria. The results are organized thematically to clearly highlight the dominant patterns, trends, and gaps identified across recent scholarly works, policy reports, and institutional studies published between 2020 and 2024.

1. Persistence of Boko Haram Induced Insecurity in Northeastern Nigeria

The reviewed literature consistently shows that insecurity in Northeastern Nigeria has persisted despite sustained military operations. Studies published after 2020 indicate that Boko Haram has shifted from holding territory to adopting asymmetric warfare tactics, including hit-and-run attacks, kidnappings, ambushes, and attacks on soft civilian targets (Onuoha, 2021; United Nations, 2023). These evolving tactics have prolonged instability across Borno, Adamawa, and Yobe states, undermining civilian safety and state authority.

Recent assessments further reveal that the insurgency has expanded beyond physical violence to include information warfare, intimidation campaigns, and exploitation of digital communication platforms (Abdulazeez & Musa, 2024). This transformation has reduced the effectiveness of conventional security strategies that rely largely on troop deployment and reactive engagement.

2. Limited Integration of Advanced Security Technologies

The review reveals a significant gap between the availability of modern security technologies and their practical deployment by security agencies in Nigeria. While technologies such as satellite imagery, geospatial intelligence, biometric systems, and unmanned aerial vehicles (UAVs) are widely recognised as effective tools for counter-insurgency, their use in Nigeria remains limited and inconsistent (Adebayo et al., 2021; Ibrahim & Mohammed, 2022).

Several studies attribute this gap to inadequate funding, lack of skilled personnel, weak infrastructure, and absence of a coordinated national framework for technology integration (Okonkwor & Bello, 2022). As a result, intelligence gathering remains largely manual, fragmented, and slow, reducing the ability of security agencies to anticipate or prevent attacks.

3. Growing Use of Digital and Communication Technologies by Boko Haram

An important finding across recent literature is Boko Haram’s increasing reliance on information and communication technologies. Research indicates that insurgents use

encrypted messaging platforms, mobile phones, and social media to disseminate propaganda, coordinate attacks, and recruit members (Onuoha, 2021; Ahmed et al., 2023).

This digital adaptation allows insurgents to evade detection, mobilise support, and exploit the slow pace of state-level technological responses. The absence of robust cyber-intelligence systems and real-time digital monitoring further compounds the challenge faced by Nigerian security agencies.

4. Potential of Data Analytics and Artificial Intelligence in Counter-Insurgency

Recent studies highlight the transformative potential of data analytics, artificial intelligence (AI), and machine learning in predicting insurgent activities and improving decision-making (Johnson & Anene, 2020; Smith & Peters, 2022). These technologies enable the analysis of large datasets drawn from surveillance feeds, mobile communication patterns, and social behaviour to forecast security threats.

However, empirical evidence suggests that Nigeria faces major structural barriers to adopting these technologies, including limited technical expertise, poor inter-agency data sharing, and cybersecurity vulnerabilities (Amadi & Yakubu, 2023).

5. Weak Inter-Agency Coordination and Policy Frameworks

The review further reveals that poor coordination among security agencies significantly undermines the benefits of technology deployment. Studies indicate that the Nigerian military, police, intelligence services, and civil defence operate largely in silos, with minimal real-time information sharing (Nwankwo, 2021).

The absence of unified digital platforms, legal guidelines for data exchange, and national cybersecurity policies limits the effectiveness of technological tools even where they are available (Okoye & Eze, 2023).

Conclusion

This study has investigated the effective use of technology to monitor Boko Haram activity in northeaster Nigeria and fight instability. Communities have been uprooted, lives have been disturbed, and national security systems have been put under stress due to the terrorist group's ongoing threat. However, a revolutionary potential to improve security responses is presented by developments in satellite imagery, drone deployment, artificial intelligence, mobile tracking systems, and surveillance technology.

According to the findings, Nigeria has implemented a few of these instruments, but their application is still restricted because of a lack of political will, financial resources, technical know-how, and interagency cooperation. Additionally, the integration of human rights-conscious tactics, local participation, and community-based intelligence is crucial to the effectiveness of such technologies.

Recommendations

The study adopts the following recommendations after taking into account the introduction, theory, literature review, findings, and conclusions about the use of technology to fight insecurity:

1. **Investment in Security Technology:** To monitor rebel activity in real time, the government should allocate more funds for the purchase of cutting-edge technologies like drones, biometric systems, CCTV networks, and satellite surveillance tools.
2. **Capacity Building:** To effectively use available technology in the battle against terrorism, security professionals need to be taught in cyber security tactics and new digital tools.
3. **Improved Intelligence Sharing:** To exchange intelligence and better coordinate counterterrorism tactics, agencies (military, police, DSS, and NIA) ought to work together on a single technology platform.
4**. Community-Based Tech Integration:** By using SMS platforms and smartphone apps, residents can anonymously report suspicious activity. Participating in communities builds trust and guarantees that local expertise is applied when using digital tools.
5. Public Private Partnerships: The government should work with academic institutions, telecom companies, and private tech companies to develop domestic technology specifically suited for counter-insurgency.
6. **Policy and Legal Frameworks:** To control drone use, digital monitoring, and data privacy in a way that upholds human rights and maintains national security, updated laws are required. Nigeria can improve its ability to identify, track, and eliminate threats from Boko Haram and other insurgent groups by putting these tactics into practice. One of the most important problems facing the country can be effectively solved by technology provided it is used appropriately and is backed by robust institutional frameworks.

References

Abdulazeez, A., & Musa, H. (2024). Information and communication technologies in insurgent operations in West Africa. *Global Security Review, 18(1), 44–61.*

Adebayo, K., Okoro, U., & Salihu, T. (2021). Drone technology and counter-insurgency operations in Nigeria. *African Security Review, 30(3), 256– 272.*

Ahmed, M., Yusuf, S., & Bello, P. (2023). Digital communication and insurgent adaptability in Nigeria. *Journal of Terrorism and Security Studies, 11(2), 89–104.*

Amadi, D., & Yakubu, F. (2023). Policy frameworks for technology-driven counter-terrorism in Africa. *Journal of African Policy Studies, 15(1), 71–88.*

Alex Roland, (2016). War and Technology: A Very Short Introduction. *Oxford, Oxford University Press.*

Anzalone, Christopher. "Salafism in Nigeria: Islam, Preaching, and Politics." *American Journal of Islam and Society 35, no. 3 (July 1, 2018): 98–103.* http://dx.doi.org/10.35632/ajis.v35i3.4 89

Adeleke, A. (2018). Digital surveillance and national security. *Nigerian Journal of Security Studies, 3(1), 24-38.*

Aghedo, I., & Osumah, O. (2012). The Boko Haram uprising: How should Nigeria respond? Third World Quarterly, 33(5), 853-869.

Ajaegbu, O. O. (2015). Rising youth unemployment and violent crime in Nigeria. *American Journal of Social Issues & Humanities, 5(1), 315-321.*

Aliyu, S. (2022). Challenges of counter-terrorism in Nigeria: A technology perspective. African Security Review, 31(2), 144-158.

Castells, M. (2010). The Rise of the Network Society. Wiley-Blackwell.

Chukwuma, E. (2019). Phone surveillance and security. *Journal of African Policing, 6(2), 112-125.*

Ekumaoko, Chijioke Egwu, Kenneth Igbo Nwokike, Ozioma Victoria Uchime, Ikenna Ukpabi Unya, and Emmanuel Obiahu Agha. "Why is The Hague Sitting on the Fence in Prosecuting Boko Haram Terrorism in Nigeria?" *African Journal of Legal Studies 14, no. 2 (December 14, 2021): 167–89.* http://dx.doi.org/10.1163/1708738412340086

Ezeobi, C. (2020). Gaps in Nigeria's security architecture. West African Security Review, 4(1), 47–59.

Freeman, Laura. "Environmental Change, Migration, and Conflict in Africa: A Critical Examination of the Interconnections. "*Journal of Environment & Development 26, no. 4 (September 6, 2017):*351–74. http://dx.doi.org/10.1177/1070496517727325

Ghani A. Z. (2017). A comparative study of Urban Crime between Malaysia and Nigeria. *Journal of Urban Management, Elsevier. Dx.doi.org/10.1016/J.jum2017.03.03.001*

Gianluca C, (2018). "Small Drones and Geographic Observation", (eds) in Gianluca Casagrande, András Sik, Gergely Szabó (2018) in Small Flying Drones: Applications for Geographic Observation, Springer International Publishing.

Husson University. (2023). The role of technology in criminal justice. www. husson.edu

Ibrahim, S., & Mohammed, L. (2022). Geospatial intelligence and counter-insurgency effectiveness in Northeastern Nigeria. *Journal of Defence and Strategic Studies, 9(2), 133–150.*

International Crisis Group. (2016). Boko Haram: Strategic and Tactical Evolution. Africa Report No. 247.

Iwuoha, V. C., & Aniche, E. T. (2016). Social media and Boko Haram: A new frontier for counter-terrorism. *African Journal of Political Science, 9(2), 56-74.*

Johnson, P., & Anene, O. (2020). Artificial intelligence and predictive analytics in counter-terrorism. *International Journal of Data Science and Security, 6(4), 201–218.*

Nwankwo, E. (2021). Inter-agency collaboration and national security in Nigeria. *Defence Studies Quarterly, 13(1), 55–70.*

Okonkwor, J., & Bello, A. (2022). Cybersecurity challenges in Nigeria's national security architecture. *African Journal of Cybersecurity, 4(2), 97–113.*

Okoye, A., & Eze, C. (2023). Biometric systems, data integration and internal security in Nigeria. Security *Journal, 36(3), 389–405.*

Okoro, J. (2021). Drone technology and the fight against insurgency in Nigeria. Defence and Security *Journal, 8(3), 102-118.*

Olayinka, T. (2021). *Privacy vs. security: Surveillance concerns in Nigeria. *Journal of African Law and Ethics, 5(1), 33-48.*

Onuoha, F. C. (2014). Boko Haram and the evolving Salafi jihadist threat in Nigeria. In Boko Haram: Islamism, politics, security and the state in Nigeria.

Smith, R., & Peters, J. (2022). Technology-enabled counter-insurgency: Lessons from global conflict zones. Global Defence Technology *Journal, 10(2), 118–134.*

United Nations. (2023). Security situation in Northeastern Nigeria. UN Department of Peace Operations.