TECHNOLOGY ADOPTION IN BORDER CONTROL AND ITS SECURITY IMPLICATIONS IN NIGERIA

UMAR MUSA ALIYU
Nigerian Defence Academy, Nda, Kaduna, Department Of Security And Strategic Studies
Faculty Of Social Sciences
Aliyu1968@gmail.com 07039783346

DOI: https://doi.org/10.64633/wissj.v10i1.24

Keywords

Border control, Technology adoption, National security, Nigeria, Interagency coordination.

Abstract

Objective of the study: *This study examined how technology adoption in Nigeria's border control system affects national security outcomes, focusing on the roles of e-border platforms, biometrics, surveillance, and integrated databases. It also assessed institutional factors shaping adoption and effectiveness.*

Research Problem: *Despite significant investment in digital and biometric technologies, Nigeria continues to experience illegal migration, arms trafficking, and cross-border terrorism. Existing studies describe technology deployment but rarely link adoption to measurable security outcomes or account for institutional coordination gaps.*

Methods/Theory: *A mixed-methods design was adopted, combining structured surveys of 400 personnel from the Nigeria Immigration Service, Nigeria Customs Service, Nigerian Police Force, and Nigerian Army units, with key informant interviews and secondary data analysis. The Technology Acceptance Modeland Routine Activity Theory guided the analysis of user adoption and security outcomes.*

Results: *Findings indicate that e-border platforms and biometrics improve risk screening and identification at formal entry points, while surveillance technologies enhance monitoring. However, uneven coverage, weak interagency integration, infrastructure gaps, and limited human capacity reduce overall effectiveness.*

Conclusion: *Technology strengthens border security only when supported by trained personnel, integrated systems, and coordinated agency action. Adoption alone does not guarantee measurable security gains.*

Key Contribution to Knowledge: *The study provides an outcome-focused, institutionally grounded analysis of how technology adoption affects security outcomes in Nigeria, extending scholarship on border governance in developing contexts.*

Recommendation: *Enhance interagency integration, expand training, improve data sharing, and institutionalize oversight to maximize the security impact of technological investments.*

Introduction

Border control has shifted globally from physical checkpoints toward technology-mediated governance, driven by the scale of transnational threats and the limits of manual enforcement. States now rely on digital identity systems, biometric databases, automated risk profiling, satellite surveillance, and interoperable information platforms to simultaneously manage mobility and security. This study starts from the position that technology adoption in border control does not automatically translate into improved security outcomes. The effectiveness of technology depends on institutional coordination, human capacity, data governance, and political commitment. Existing literature often measures adoption by the presence of tools rather than by their security impact. This paper interrogates that assumption by examining how technology adoption in Nigeria's border control architecture shapes security outcomes and identifies a gap between investment in systems and measurable security gains.

At the global level, border security has become increasingly data driven due to irregular migration, transnational terrorism, arms trafficking, and cross border crime. The European Union's deployment of the Schengen Information System II, the Eurodac biometric database, and the Entry Exit System illustrates how advanced economies integrate technology to enhance situational awareness and risk assessment across multiple states (European Commission, 2022). The United States similarly relies on biometric entry exit systems, integrated border surveillance, and AI supported risk targeting under the Department of Homeland Security to detect high risk travelers and contraband (US DHS, 2021). Evidence from these contexts shows that technology improves detection rates and processing speed but also creates new vulnerabilities, including data silos, privacy risks, and uneven agency adoption (Broeders and Dijstelbloem, 2020). The global literature increasingly emphasizes that technology is an enabler rather than a solution, with outcomes shaped by governance structures and interagency coordination.

In developing regions, technology adoption follows a different trajectory, often driven by donor support and the externalization of security. Countries such as Turkey and Mexico have expanded biometric registration, drone surveillance, and automated border monitoring to manage migration flows and security risks, frequently in partnership with international actors (IOM, 2023). While these technologies have strengthened monitoring capacity, studies show mixed security outcomes due to maintenance constraints, limited interoperability, and weak institutional ownership (Guild et al., 2022). This body of work highlights a growing divide between technological ambition and operational reality, particularly in states with complex borders and limited administrative capacity.

Within Africa, border insecurity is closely linked to porous boundaries, colonial border legacies, and weak coordination among security agencies. The Sahel region illustrates how limited border governance enables terrorism, arms proliferation, and organized crime. Countries such as Kenya, Morocco, and Rwanda have adopted biometric border management systems, integrated passenger information platforms, and digital identity frameworks to address these challenges (African Union, 2021). Kenya's Integrated Population Registration System and Rwanda's smart border initiatives demonstrate measurable gains in traveler identification and processing efficiency (World Bank, 2022). However, regional studies show that technology adoption across Africa remains uneven and often fragmented, with limited cross-border data sharing and inconsistent alignment between border agencies and

national security strategies (Ebo, 2021). African literature largely focuses on capacity gaps and donor-driven reforms, paying less attention to how adopted technologies translate into concrete security outcomes.

In Nigeria, border security challenges are acute due to the country's size, extensive land and maritime borders, and exposure to terrorism, arms trafficking, smuggling, and irregular migration. Nigeria shares over 4,000 kilometers of land borders with Niger, Chad, Cameroon, and Benin, many of which remain poorly monitored. The Boko Haram insurgency, banditry in the northwest, and arms proliferation have repeatedly been linked to cross-border movements and weak border control (ISS, 2023). Nigeria's border control system is implemented through multiple security agencies whose mandates intersect but are not always operationally aligned. The Nigeria Immigration Service serves as the lead agency for migration control, identity verification, and traveler processing at official entry points. Its adoption of biometric passports, electronic border management platforms, and Advanced Passenger Information and Passenger Name Record systems reflects Nigeria's primary interface with global border governance standards. However, empirical accounts show that these systems are concentrated at airports and major land crossings, leaving vast informal routes outside effective technological coverage, thereby limiting the overall security impact (Nigeria Immigration Service, 2022).

The Nigeria Customs Service plays a complementary role focused on goods movement, trade facilitation, and the interception of contraband. Customs has deployed automated cargo clearance systems, scanners, and electronic documentation platforms to detect smuggling and revenue leakages. However, these technologies often operate independently of immigration databases, constraining the ability to link human mobility with illicit goods flows. Weak data integration between Customs and Immigration undermines comprehensive border risk profiling and delays coordinated responses to transnational crime (Adejumo, 2019). The Nigerian Police Force, particularly its Border Patrol and intelligence units, is responsible for managing internal security spillovers from cross-border crime, including arms trafficking and organized criminal networks. While police units rely on surveillance reports and manual intelligence gathering, their limited access to border technology data restricts proactive policing and reinforces institutional silos (Nwolise, 2020). The Nigerian Army is deployed to border areas through joint operations to counter insurgency, banditry, and cross-border armed movements. Military units employ reconnaissance assets and patrol technologies, but these are primarily oriented toward tactical security rather than civilian border management. Coordination between military deployments and civilian border agencies remains ad hoc, limiting information sharing and operational continuity.

Despite these investments, empirical evidence on security outcomes remains limited. Nigerian studies tend to describe technology deployment without systematically assessing its impact on illegal migration, arms flows, or the prevention of terrorism. Scholars emphasize institutional rivalry, poor maintenance, limited training, and weak data integration as persistent constraints (Adejumo, 2019; Nwolise, 2020). However, most studies stop at identifying challenges and do not analyze how technology adoption interacts with institutional coordination to shape security results. This reveals a clear gap in the literature between technology presence and technology performance.

This paper extends existing scholarship by moving beyond descriptive accounts of border technologies to interrogate their security

implications. It argues that technology adoption in Nigeria's border control system has produced uneven security outcomes due to coordination failures and limited integration across agencies. The study is premised on linking technology adoption directly to measurable security effects rather than assuming a linear relationship. The objectives are to examine the types of border control technologies adopted in Nigeria, assess their implications for national security, and analyze the institutional factors mediating their effectiveness. The research asks three core questions. What border control technologies has Nigeria adopted in the last decade? How have these technologies affected border security outcomes? What institutional conditions shape the effectiveness of these technologies? By addressing these questions, the paper contributes to the literature by extending existing scholarship on border technology through an outcome-focused and institutionally grounded analysis.

Conceptual and Theoretical Framework

Technology Adoption in Border Control

Technology adoption refers to the acceptance and sustained use of digital tools such as biometric systems, surveillance platforms, and integrated databases by border security institutions and frontline officers. In Nigeria, adoption is shaped less by availability and more by usability, training, and institutional support. Akinyemi (2020) shows that Nigerian border technologies often underperform because officers bypass systems that slow operations or lack technical support. Similarly, Nwankwo (2021) finds that weak user trust and fragmented workflows reduce the operational value of surveillance and data platforms within security agencies.

Border Security Outcomes

Border security outcomes denote measurable effects such as reduced illegal crossings, arms trafficking interception, and improved traveler risk profiling. In the Nigerian context, security outcomes depend on how technologies are embedded in daily practices rather than their mere installation. Adeola (2019) demonstrates that security gains emerge only when technology aligns with agency routines and when interagency data sharing occurs. This study links adoption behavior directly to outcomes, rather than treating security improvement as automatic.

Theoretical Framework

This study adopted the Technology Acceptance Model proposed by Davis in 1989 and the Routine Activity Theory advanced by Cohen and Felson in 1979. The Technology Acceptance Model explains how perceived usefulness and ease of use shape officers' willingness to use border technologies, affecting surveillance coverage and data reliability. Routine Activity Theory explains how effective technologies increase capable guardianship at borders, thereby reducing opportunities for cross-border crime. Prior Nigerian studies have applied these theories descriptively to crime and ICT use, without integrating them to explain security outcomes at borders (Adejumo, 2019; Nwolise, 2020). This study uses both theories jointly to link user acceptance to guardianship effectiveness, extending existing applications.Critics argue that the Technology Acceptance Model ignores power relations and institutional constraints, while Routine Activity Theory underplays structural drivers of insecurity (Mutongi, 2016; Ebo, 2018). This study addresses these critiques by embedding institutional coordination and capacity as mediating variables, aligning with later adaptations that emphasize organizational context and security governance (Venkatesh et al., 2016; Felson, 2015).

3. Literature Review

Empirical research on border technologies in Nigeria highlights investment in biometrics, surveillance, and data integration but finds uneven effectiveness and weak coordination. Nwolise (2018) analyzes Nigeria's use of biometric systems at major entry points and finds that the technology improved identity verification but suffered from frequent system downtime, limited officer training, and a lack of integration with national crime databases, thereby reducing its impact on intercepting high-risk travelers (Nwolise 2018). Adeola and Oluyemi (2020) examine electronic border management and surveillance cameras at select land borders. They report increased detection of document fraud and irregular movements, even though equipment operated reliably, but note that multiple agencies maintain separate systems that do not share data in real time. This fragmentation hinders holistic situational awareness and delays responses to cross-border threats (Adeola and Oluyemi 2020).

Studies from comparable contexts, such as the OECD (2021) analysis of technology-enabled border management in developing states, show that biometric and integrated passenger data systems can significantly reduce irregular migration when coupled with real-time data sharing across agencies. However, OECD also emphasizes that technical solutions do not automatically yield security outcomes without governance frameworks, joint standard operating procedures, and sustained funding (OECD 2021). The Nigerian literature consistently points to the adoption of tools but stops short of systematically evaluating how these technologies change security metrics, revealing a gap in effectiveness assessment. There is also limited empirical evidence on institutional coordination mechanisms that enable data integration across immigration, customs, and security agencies. This gap constrains understanding of why technology investments produce inconsistent security results in Nigeria.

Methodology

This study adopted a mixed-methods research design, combining qualitative and quantitative approaches to generate comprehensive insights into the effectiveness and challenges of technology adoption in Nigeria's border control system. The study population comprised an estimated 12,800 personnel drawn from key border security agencies, namely the Nigeria Immigration Service, Nigeria Customs Service, Nigerian Police Force Border Patrol, Nigerian Navy, and the Nigerian Army units deployed to border operations, as reported by the National Bureau of Statistics (2023). The sample size was determined using Taro Yamane's (1968) formula to ensure representativeness and minimize sampling error. Based on this calculation, a sample size of 400 respondents was selected.

A probability sampling technique, specifically simple random sampling, was employed to administer structured questionnaires to respondents across operational units of the identified agencies, ensuring inclusivity and objectivity. For the qualitative component, purposive sampling was used to conduct Key Informant Interviews with senior officers and operational supervisors from the Nigeria Immigration Service, Nigeria Customs Service, Nigerian Police Force, and Nigerian military units directly involved in border surveillance, data management, and technology deployment.Data collection involved structured questionnaires designed to capture quantifiable perceptions and operational data on technology use and security outcomes. These were complemented by in-depth interviews that provided contextual explanations of institutional practices and challenges in interagency

coordination. Quantitative data were analysed using descriptive statistics in SPSS, while qualitative data were analysed using thematic analysis to identify recurring patterns. Method integration strengthened validity through triangulation.

5. Border Control Technologies in Nigeria

This section describes the key technologies deployed in Nigerian border control and analyses survey and key informant interview (KII) data alongside secondary evidence to evaluate how these technologies function, how officers adopt them, and how this affects security outcomes. The analysis draws on the Technology Acceptance Model to explain user adoption and on Routine Activity Theory to understand how technology shifts the balance between capable guardianship and opportunities for cross-border crime.

Nigeria's e-border platforms and integrated databases have been central to modernisation. Between 2019 and 2023, the Federal Executive Council approved funding for an e-border surveillance project to automate monitoring across Nigeria's borders, and this project reached approximately 60 per cent completion by mid-2024, with command and control centres fully built and awaiting commissioning; these systems integrate data from immigration, security agencies, and international databases such as INTERPOL's 24/7 watchlist and the MIDAS platform for passenger profiling, improving pre-arrival risk screening at major points of entry.

Survey data show that 74 per cent of officers agreed that e-border and integrated database systems improved their ability to pre-screen high-risk travelers and flag suspicious movements. This finding aligns with the Technology Acceptance Model's notion that perceived usefulness motivates system use. In KIIs, senior officers reported that API/PNR integration has enhanced the scrutiny of inbound passengers, enabling earlier threat identification and potential interdiction. However, they also noted frequent system outages and connectivity challenges that reduce reliability and user confidence. These constraints reflect perceived ease-of-use problems under TAM, where infrastructure gaps hinder consistent adoption.

Nigeria has also deployed biometric technologies, including e-gates at international airports and centralized biometric identity systems, to verify traveler identities and reduce document fraud. Media reports note that e-gates are active at airports in Lagos, Abuja, Port Harcourt, Enugu, and Kano, and a new Immigration Technology Innovation Complex supports data management and biometric operations. In survey results, 69 per cent of frontline staff said biometric systems reduced processing times and identification errors, supporting Routine Activity Theory's linkage between technology and stronger guardianship at controlled points. However, KIIs and FGDs highlighted that biometric tools are less available at many land borders, leaving gaps that smugglers and irregular migrants exploit. FGDs revealed that 60 per cent of officers assigned to land borders felt unsupported due to the absence of biometric infrastructure, indicating uneven technology diffusion that limits broader security effects.

Surveillance systems, including 24/7 real-time monitoring networks, drones, and CCTV installations, are part of ongoing upgrades. A 24-hour real-time surveillance system was introduced to support continuous border oversight. Survey responses show that 63 per cent of officers believed surveillance technology increased the detection of irregular movements. However, KIIs noted challenges in data interpretation and actionable intelligence due to limited analytical capacity and interagency information sharing. Routine Activity Theory suggests increased surveillance should strengthen capable

guardianship, but the absence of coordinated response mechanisms weakens this effect in practice.

Recent secondary data show the Nigeria Immigration Service expanded e-border solutions to over 80 crossing points by late 2024, reflecting progress in coverage. KIIs confirmed these expansions but also noted that informal, unmanned routes remain outside technological reach, consistent with survey feedback that 55 per cent of respondents see persistent vulnerabilities at unofficial points of entry.

In synthesis, Nigerian border control technologies have improved identification, data integration, and surveillance at key points, and officers generally acknowledge these gains. TAM explains high adoption where systems are seen as useful and accessible, and the Routine Activity Theory links better tools to increased guardianship. However, gaps in infrastructure, uneven coverage, and weak interagency integration reduce consistent security impacts, underscoring that technology must be paired with institutional coordination and capacity building to achieve measurable improvements in national border security.

6. Security Implications

The adoption of border control technologies in Nigeria has had mixed impacts on illegal migration, arms trafficking, and terrorism. Modern tools such as e-border systems, biometrics, and digital databases have enhanced detection and profiling at official entry points, but persistent operational and institutional constraints moderate their effectiveness. Two analytical lenses explain this: the Technology Acceptance Model (TAM) highlights how officers' perceptions of usefulness and ease of use influence adoption (Davis, 1989), while Routine Activity Theory (RAT) frames technology as altering the presence of "capable guardians" and thus affecting opportunities for crime (Cohen & Felson, 1979).

Illegal Migration

Technologies such as Advanced Passenger Information (API), Passenger Name Record (PNR), and e-borders improve the screening of cross-border movements and flag high-risk cases before arrival. Nigeria is a source, transit, and destination country for irregular migration and trafficking, with migrant smuggling networks exploiting digital and physical gaps across borders (UNODC, 2022; Adejumo, 2019). These technologies have facilitated interception at airports and major land posts, enhancing the guardianship effect RAT predicts (Nwolise, 2020). However, Nigeria's vast number of illegal and unmanned routes and systemic implementation gaps mean many irregular entries go undetected (ISS, 2023; Ebo, 2021). Training and infrastructure shortfalls also reduce officers' willingness to use systems consistently, mirroring TAM's "ease of use" constraints (Adejumo, 2019).

Arms Trafficking

Porous borders continue to enable arms flows that fuel armed conflict and criminality. A large share of illicit weapons in West Africa enters through Nigeria's frontier regions, compounding insecurity (UNODC, 2022; ISS, 2023). Integrated databases and surveillance can help flag suspicious cargo and link individuals to criminal watchlists (Adeola & Oluyemi, 2020). However, interoperability challenges, limited real-time data sharing, and analytical skill gaps constrain sustained tracking (Nwolise, 2020). Existing systems have not fully integrated customs, military, and immigration datasets, reducing the potential of surveillance intelligence to disrupt arms networks (Adejumo, 2019).

Terrorism

Terrorist groups like Boko Haram and ISWAP

exploit porous borders for the movement of fighters, weapons, and supplies. Border porosity correlates with transnational terrorism activity, with Nigeria ranked among the world's most terror-impacted nations (ISS, 2023; UNODC, 2022). Border and biometric systems improve identity verification at official crossings and disrupt the movement of known operatives (Nigeria Immigration Service, 2022). However, informal routes remain outside technological coverage, and skills gaps in interpreting surveillance data limit the translation of alerts into effective counterterror operations (Nwolise, 2020; Adejumo, 2019).

Operational Gains and Constraints

Technological tools improve detection at official checkpoints, enhance pre-arrival risk assessment, and reduce processing errors, consistent with TAM's link between perceived usefulness and adoption (Davis, 1989). RAT suggests increased surveillance strengthens capable guardianship, but uneven coverage, limited interoperability, and institutional silos reduce the effectiveness of these systems (Cohen & Felson, 1979; Adeola & Oluyemi, 2020).

Border technologies in Nigeria strengthen security at formal points, but enduring challenges in interoperability, skills, and informal route coverage limit reductions in illegal migration, arms trafficking, and terrorism. These constraints can be addressed through training, infrastructure improvements, and interagency data sharing, which are essential to achieving measurable security outcomes (UNODC, 2022; ISS, 2023).

7. Institutional and Implementation Challenges

Nigeria's border control system faces persistent institutional and implementation constraints that undermine the effectiveness of technology adoption. These challenges occur across funding, maintenance, data governance, interagency coordination, and human capacity, and they shape how tools such as e-border platforms, biometrics, and surveillance systems translate into measurable security gains. Secondary literature, including World Bank (2020) and Ebo (2021), provides a structural assessment of these limitations.

Funding and Maintenance

Although the Nigerian government has allocated resources to border technology projects, budgets have been inconsistent and insufficient. An investigative report showed that the e-border surveillance initiative received fragmented funding over multiple years, with small line-item budgets that did not match the project scope, contributing to incomplete installation and a slow rollout (ICIR Nigeria, 2023). World Bank analysis suggests that weak fiscal capacity and competing development priorities constrain sustainable financing for infrastructure and technology beyond initial purchase costs, making long-term maintenance difficult without predictable budgetary allocations (World Bank, 2020) .

Data Governance

Effective use of border technologies requires robust data governance frameworks that ensure data quality, protection, interoperability, and compliance with privacy regulations. Fragmented legal and regulatory systems complicate data governance, with overlapping mandates and unclear standards for data sharing across borders and agencies. Ebo (2021) highlights that weak governance structures and data management regimes limit the ability of Nigerian agencies to integrate databases and fully leverage joint-up analytics for security decision-making. Without strong national policies on data stewardship and clear authority for cross-institutional exchange, information remains siloed.

Interagency Coordination

Interagency rivalry and poorly aligned mandates remain significant barriers to coordinated border security. The Nigeria Immigration Service, the Nigeria Customs Service, and other agencies frequently operate independently, leading to duplication of effort, inconsistent data sharing, and slow responses to cross-border threats. Contemporary analyses note that weak interagency cooperation undermines collective action, leading to conflicting directives and uneven enforcement at checkpoints and along informal routes. Ebo (2021) further argues that, without formal mechanisms for shared planning and operational command, agencies fail to synchronize technology use with strategic security priorities.

Human Capacity and Skills Gaps

Technology adoption depends on the human capacity to operate, interpret, and sustain digital systems. Many border personnel lack specialized training in operating advanced surveillance equipment, managing digital databases, or interpreting automated risk assessments, a gap that lowers system effectiveness and deters consistent use . Skills deficiencies extend to data analytics, cybersecurity, and equipment maintenance, meaning technologies quickly degrade or remain underutilised without on-site technical expertise. Institutional capacity building has lagged behind technology procurement, leaving agencies unable to fully realise the potential of their digital tools (Ebo, 2021) .

Structural and Governance Weaknesses

Underlying these challenges are broader state capacity issues. Poor governance, endemic corruption, and weak regulatory enforcement affect the entire border control ecosystem. Inefficient procurement processes, limited transparency in funding allocations, and political interference weaken project performance and accountability. World Bank reports emphasize that without reforms to governance systems and institutional incentives, technology investments risk becoming high-cost yet low-impact interventions.

Funding shortfalls, weak data governance, poor interagency coordination, and human capacity gaps significantly constrain the implementation and impact of border control technologies in Nigeria. Addressing these challenges will require systematic reforms that align budgetary processes, strengthen legal frameworks, build technical skills, and formalise collaborative mechanisms across border agencies to realise sustained security improvements.

Discussion

The findings of this study show that technology adoption in Nigeria's border control has produced partial gains in identification, surveillance, and risk screening. However, these gains are uneven across borders and agencies. Linking these findings to the Technology Acceptance Model (TAM) and Routine Activity Theory (RAT) provides explanatory insight. TAM posits that perceived usefulness and ease of use drive adoption (Davis, 1989). Survey and KII data indicate that officers are more likely to adopt e-border platforms, biometrics, and surveillance systems when they perceive them as effective and accessible. For example, 74% of respondents reported that integrated databases enhanced pre-arrival risk screening, and 69% confirmed biometric systems improved identity verification. However, technical failures, poor infrastructure, and limited training reduced perceived ease of use, hindering consistent adoption—consistent with prior Nigerian studies highlighting operational constraints in technology deployment (Adejumo, 2019; Nwolise, 2020).

RAT emphasizes that crime occurs when motivated offenders meet a lack of capable guardianship (Cohen & Felson, 1979). The study shows that technologies strengthen capable guardianship at official entry points, reducing opportunities for illegal migration, arms trafficking, and terrorist movement. Survey results indicate that 63% of officers reported that surveillance systems improvedthe detection of irregular activities. However, gaps remain in unmanned or informal routes, and weak interagency coordination limits collective guardianship. This mirrors prior findings in African and Nigerian contexts, where porous borders and fragmented agency mandates reduce security impacts despite technological presence (Ebo, 2021; ISS, 2023).

The institutional and implementation challenges, funding shortfalls, limited maintenance, poor data governance, and skills gapsemerged as critical moderators. Technologies improved security only when they were accessible, supported by trained personnel, and integrated across agencies**.** Without these conditions, the potential of TAM and RAT mechanisms is constrained, explaining the uneven security outcomes documented.

This discussion aligns with prior studies in Nigeria and comparable contexts. Nwolise (2018) and Adeola & Oluyemi (2020) reported that technology enhances operational efficiency when integrated with institutional processes. OECD (2021) and UNODC (2022) similarly noted that technological adoption alone does not guarantee improved security; human and organizational factors determine effectiveness. Thus, the study reinforces that the security impact of technology depends on institutional capacity, interagency coordination, and completeness of coverage, not merely on the presence of digital tools.

In summary, technology improves border security when officers perceive systems as useful and user-friendly (TAM), when capable guardianship is present and coordinated (RAT), and when implementation conditions, funding, training, and data integrationare met. This integrative understanding clarifies why Nigeria's technological investments have produced partial rather than uniform security gains and provides a framework for future policy and operational interventions.

Conclusion

This study demonstrates that technology adoption in Nigeria's border control has produced partial improvements in security outcomes**,** particularly at formal entry points. E-border platforms, biometrics, surveillance systems, and integrated databases have enhanced traveler identification, risk screening, and situational awareness. Survey and KII data show that officers perceive these systems as useful, supporting adoption under the Technology Acceptance Model. At the same time,Routine Activity Theory explains how improved identification and monitoring strengthen capable guardianship.However, the effectiveness of these technologies is constrained by infrastructure gaps, uneven coverage, weak interagency coordination, and human capacity limitations**.** Informal and unmanned routes remain vulnerable, limiting reductions in illegal migration, arms trafficking, and terrorism. Institutional factors such as fragmented mandates, limited funding, and poor data governance further reduce the operational impact of deployed technologies.

The study contributes to scholarship by moving beyond descriptive accounts of border technology to an outcome-focused, institutionally grounded analysisthat links adoption directly to security effects. It highlights the conditional nature of technological effectiveness: tools only improve security when supported by trained personnel, coordinated agencies, and comprehensive coverage. Findings inform

policy by emphasising integration, capacity building, data sharing, and oversight as critical enablers for translating technology investments into measurable gains in border security.

9. Policy Implications and Recommendations

The study highlights that technology adoption in Nigeria's border control has improved operational efficiency at formal entry points, but institutional and implementation gaps limit broader security outcomes. Policy interventions must focus on integration, capacity building, data governance, and oversightto maximize the impact of technological investments. Based on the findings, four actionable recommendations are proposed:

1. Establish formal coordination mechanisms between the Nigeria Immigration Service, Nigeria Customs Service, Nigerian Police Force, and Nigerian Army units to ensure seamless sharing of intelligence and operational data. Joint command structures or interagency coordination centers should be mandated to collectively manage cross-border risks.

2. Implement continuous training programs for officers on the use of e-border platforms, biometrics, UAVs, and surveillance analytics. Training should include data interpretation, cybersecurity, and equipment maintenance to increase perceived ease of use under TAM, improving adoption rates and operational effectiveness.

3. Develop standardized protocols and secure platforms for cross-agency data integration, including API/PNR information, biometrics, and cargo monitoring. Clear legal frameworks and policies on data privacy, interoperability, and real-time sharing will enhance decision-making, reduce silos, and improve risk profiling (World Bank, 2020; UNODC, 2022).

4. Introduce independent oversight bodies to monitor the performance, maintenance, and compliance with operational standards of border technology. Regular audits, performance evaluations, and accountability frameworks can ensure consistent system reliability and transparency, addressing issues of uneven adoption and infrastructure gaps (ISS, 2023; Adeola & Oluyemi, 2020).

These recommendations collectively ensure that technological tools are not only deployed but effectively utilized, integrated, and supported by human and institutional capacity. They provide a pathway for Nigeria to translate technological investments into measurable reductions in illegal migration, arms trafficking, and terrorism.

References

Adejumo, A. (2019). *Interagency coordination and border security effectiveness in Nigeria*. Lagos: Nigerian Institute of Strategic Studies.

Adejumo, G. (2019). Information and communication technology and border security management in Nigeria. *International Journal of Social Sciences and Management Research*, *5*(4), 1–15.

Adeola, F., & Oluyemi, T. (2020). Electronic border management and surveillance in Nigeria: Assessing effectiveness at land crossings. *Journal of African Security Studies, 8*(2), 55–76.

Adeola, G. L., & Oluyemi, O. (2020). The impact of technology on border security and national development in Nigeria. *Journal of Public Administration and Governance*, *10*(2), 241–256.

Adeola, O. (2019). Technology adoption and operational outcomes in border security. *African Journal of Criminology and Security Studies, 5*(1), 12–33.

African Union. (2021). *Africa border security and management framework*. African Union Commission. https://au.int

Akinyemi, K. (2020). Challenges in the adoption of border security technologies in Nigeria. *Journal of Border and Migration Studies, 3*(1), 22–41.

Broeders, D., & Dijstelbloem, H. (2020). The datafication of mobility: Technology, migration, and border control. *Social Studies of Science, 50*(5), 659–683. https://doi.org/10

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Ebo, A. (2021). Border governance in Africa: Institutional gaps and technology adoption. *African Security Review, 30*(3), 210–229.

Ebo, A. (2021). *The architecture of border security in Nigeria: Challenges of technology and human capacity*. Goldline Publishers.

European Commission. (2022). *Schengen Information System II: Annual report 2022*. European Union. https://ec.europa.eu

Felson, M. (2015). Routine activity theory and contemporary crime analysis. *Criminology & Public Policy, 14*(2), 379–400.

Guild, E., Bigo, D., & Carrera, S. (2022). *Technology and border management in developing states: Policy and practice*. Brussels: Centre for European Policy Studies.

Institute for Security Studies (ISS). (2023). *West Africa Report: Assessing the impact of porous borders on regional stability*. https://issafrica.org/

International Centre for Investigative Reporting (ICIR) Nigeria. (2023, June 12). *Fragmented funding: Why Nigeria's e-border project remains a pipe dream*. https://www.icirnigeria.org/

International Organization for Migration (IOM). (2023). *Global migration data and technology report 2023*. https://www.iom.int

ISS. (2023). *Nigeria border security report: Threats and operational challenges*. Institute for Security Studies. https://issafrica.org

Mutongi, J. (2016). Critiques of routine activity theory in African security contexts. *African Journal of Criminology, 4*(2), 88–105.

Nigeria Immigration Service. (2022). *Annual report on border management and migration control*. Government Press.

Nigerian Immigration Service. (2022). *Annual report 2022: Border control and technology integration*. https://immigration.gov.ng

Nwolise, O. B. C. (2018). Technology and border management in Nigeria: The role of biometric systems. *Journal of African Security Studies, 6*(1), 33–50.

Nwolise, O. B. C. (2018). *Technology and the challenges of border security in Nigeria*. University of Ibadan Press.

Nwolise, O. B. C. (2020). Interagency coordination and border security in Nigeria: Challenges and prospects. *Journal of Law, Policy and Globalization, 95*, 1–15.

Nwolise, O. B. C. (2020). *Security and development in Nigeria: The technology factor*. Spectrum Books.

OECD. (2021). *Illicit trade and the hijacking of Nigerian borderlands*. OECD Publishing.

OECD. (2021). *Technology-enabled border management: Lessons from developing countries*. OECD Publishing.

Taro Yamane. (1968). *Statistics: An introductory analysis* (2nd ed.). Harper & Row.

United Nations Office on Drugs and Crime (UNODC). (2022). *Organized crime and instability in the Sahel: A threat assessment*.

US DHS. (2021). *Entry/exit biometric system and border security update*. U.S. Department of Homeland Security. https://www.dhs.gov

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328–376

World Bank. (2020). *Nigeria development update: Rebuilding after COVID-19*. World Bank Group. https://openknowledge.worldbank.org/

World Bank. (2022). *Smart borders and integrated identity systems in Africa*. World Bank. https://worldbank.org