

INFORMATION TECHNOLOGY AND INTERNAL SECURITY IN NIGERIA

Abdullahi Mohammed Lawal and Etim Essien Bassey

*Department of Arts and Social Sciences, Waziri Umaru Federal Polytechnic, Birnin Kebbi, Kebbi State
Department of Economics, University of Calabar, Cross Rivers State.*

Corresponding Author's email: dbabanigeria@yahoo.com



(TETF/DESS/UNI/SOKOTO/ARJ/01)

Abstract

Information Technology is a critical infrastructure in contemporary security management across the globe. There have been a lot of important developments with respect to information Technology such as Analytic systems, Video Surveillance System, Licence Plate Readers, DNA testing, Technical Intelligence among others all have far reaching implications for internal security. The paper adopted Qualitative method (Secondary data) by reviewing available literature, journals, security reports on the interplay between information technology and internal security. The social contract theory of state was used to guide the study as government need to provide effective mechanism to ensure adequate security of lives and properties of its citizens. The study discovered that security architecture in Nigeria is still at level of information technology adoption. The study recommended that Nigeria should employ conscious policies backed up with adequate funding to encourage security agencies to elevate their operations that is embedded in the latest information technology available at any point in time to ensure internal security and minimize the occurrence of crimes.

Keywords: Information Technology, Internal Security and Nigerian State.

Introduction

The effect of information Technology (IT) in critical issues in contemporary security management cannot be overemphasized. Information technology acquisition and deployment decisions are high-priority topics for law enforcement agencies with government at all levels committing vast sums of resources to technology with the hope of improving efficiency and effectiveness in internal security. The influence of information technology to internal security framework is the involvement and use of technology blend between technology and traditional modes of internal security management without intruding into the fundamental rights of citizens in a manner that could impact on government legitimacy, citizens consent and ensuring internal security. The information technology has ensured the improvement of internal security globally (Adamu, 2017). Information technology has revolutionized crime investigation and prosecution process in secured ways, it has provide insights on enhancing law enforcement capabilities, improving case management, strengthening evidence presentation and promoting fairness and justice in the criminal justice system.

Modern states globally are utilizing information technology to combat not only crime but prevent crime. Police make use IT tools such as CCTV cameras to monitor road traffic in case of any abnormalities, Video proof can be used in court. In all most all developed countries, there is a

central database that has details of all citizens and has links to other databases such as car registration database held at the drivers vehicle licensing agency and to another powerful computer running the automated finger identification system. This integrated system helps in tracking down and controlling crimes and ensure internal security.

Information technology has played an important role in the fight against insecurity in Nigeria and at global stage (Arase, 2016)

Information technology has proven to be effective in managing threats, even though there is a huge gap between the kind of insecurity experienced in developing countries like Nigeria and the way they are handled in such countries like united states of America, Britain etc . information technology has brought positive transformation in all spheres of human endeavour, technology cannot be ignored especially when it comes to insecurity where by a lot instruments can be deployed to tackle and improve security in all the organization and societal activities. (Bassey, 2017)

Against this background, this paper explores the impact of information technology on internal security in Nigeria. To answer this, the paper is structured into four sections, the first section introduced the paper, the concept of internal security was discussed in the second section, the third section was dedicated to the analysis of information technology and internal security in Nigeria, conclusion and prognosis formed the last section.

Concept of Internal Security

Internal security is the act of maintaining peace and order within a country's borders. It involves upholding a country's law and defending against threats that originate within the country. The responsibility for internal security rest with the police, paramilitary, in some instance, the military. Internal security has been described by many scholars from different perception and context for instance: Noonan, (2019) sees internal security as a concept that has to do with anything or steps for curtailing any action or activity that disturbs or threatens the Socioeconomic and political equilibrium of the state. Internal security challenges deals with threats that emanate from domestic sources.

Arase (2016,) defined internal security as that which is primarily concerned with internal threats, including : all state actions directed at emplacing, upholding as well as deploying national laws, strategies policing, as well as law enforcement agencies towards the maintenance of peace, laws and order, at the same time safeguarding citizens from fear or threats to their values, livelihood, liberty, lives and properties within a nation's territory. Internal security therefore, revolves round the context of protection of value, critical human and infrastructural assets , territorial integrity, lives and property of citizens from threats. Internal security is measured by the extent to which a state creates and maintains law, order and development process to guarantee freedom from threats and fear of losing life, liberty and property (Lawal *et al.*, 2025).

Aja (2017), assert that internal security focuses more welfare, contentment and security for every citizen, group, community and component states/units in a country. To ensure internal security, government assumes the chief duty by means of laws, regulations and establishment of law enforcement agencies who have the institutional duties of protecting the state, the people, and their strategic assets of survival against all forms of internal threats.

Internal security management is the process of creating conducive and secure environment in any given society (Dimsey, 2008). It could be likened to the efforts which are made to protect the community people live in an environment free from intimidation and fear of violence

(Henry,2000). Oshita and Ikelegbe (2019), refers to internal security as steps taken to secure the citizenry both physically and psychologically by the use of variously assigned security function and strategies. Luara (2014) asserts that internal security management involves ways of providing security technologies and strategies which can be used mitigate the formidable security threats in the environment, these strategies or measures taken to protect and manage violence, reduce security risks and ensure that the environment is safe. Internal security equally mean the act of keeping peace within the borders of sovereign state generally by upholding the national law and defending a territory against internal security threats. Responsibility of internal security management lies with the police and other paramilitary forces and in exceptional circumstances the military. In this case, the Nigeria police is the main actor. Adamu (2017), in his paper titled internal security management and community policing in Nigeria described internal security management as multidimensional security system, where the security management structure is made up of national security structures , legislative and oversight bodies, civil society organizations and non - state security actors.

The national security structure in Nigeria includes : Council of state, National defence council. National security council, and Nigeria police council. These councils are enshrined in the exclusive powers of the 1999 constitution as amended. The councils give directions and guides national security and defence policies in Nigeria. It is superintended by the president and Commander-in-chief of the Armed forces. It is the driving force for national security objectives where national security agencies draw their inspiration to implement actions. These agencies include : Office of the national security adviser (ONSA), Nigerian army, Nigerian navy, Nigerian air force, Nigeria police, State security service, National intelligence agency, Defence intelligence agency, Nigeria custom service, Nigerian correction service, National security and civil defence corps, Nigeria immigration service, National drug law enforcement agency, Economic and financial crimes commission and Independent corrupt practices commission.

Apart from the statutory responsibilities as provided in the various laws and regulations establishing these agencies, the complex nature of crimes further raises the need for synergy among the security services in order collectively achieve the overall national security objectives and ensure internal security in Nigeria. The national security strategy document developed and launched in November 2014 by office of the national security adviser (ONSA) identifies 20 critical threats to Nigeria's internal security. These include : global challenges, transnational organized crimes, crude oil theft, illegal bunkering, Nigeria's borders, climate change, communal and ethnoreligious conflict, pastoralist/farmers conflict, politics and federalism in Nigeria, Governance challenges. Other threats include poverty, kidnapping, proliferation of small arm and light weapons, proliferation of weapons of mass destruction, illegal migration, economic challenges, financial crimes, information technology and cyber security. Banditry and Cattle rustling in my view also forms part of internal security threats in Nigeria.

Empirical literature review

Ekwutosi et al., (2021) investigated the role of information technology in enhancing national security in Nigeria between 2001 and 2020. Using both primary and secondary data sources and adopting the realist paradigm as a theoretical framework, the study found that Nigeria's security challenges have persisted due to poor management and weak institutional responses. The authors identified Nigerians themselves as major contributors to insecurity through negligence and lack of proactive engagement. The study concluded that information and communication technology can significantly improve the management of security challenges if properly utilized by security agencies.

Similarly, Kemi (2016) examined the role of information technology in strengthening national security in Nigeria. Using a case study approach, the study raised concerns regarding the adequacy of ICT infrastructure, surveillance equipment, and information-sharing mechanisms among Nigerian security agencies. The study revealed that information technology can support threat identification, improve information dissemination, and enhance national response capabilities against terrorism and cyber threats. The study recommended increased investment in ICT infrastructure and strategic digital security systems.

In another study, Zakari (2024) explored the implications of artificial intelligence for national security in Nigeria, particularly in military logistics. Employing documentary research design and document analysis, the study found that AI technologies such as facial recognition, predictive analytics, and video surveillance significantly improve threat detection and monitoring. The study further revealed that the Nigerian Air Force utilizes AI for predictive aircraft maintenance. However, lack of awareness among policymakers and inadequate technical expertise were identified as major barriers to AI adoption. The study recommended capacity building in data science and stronger government commitment toward developing a national AI ecosystem.

Also, Afolayan (2024) examined the role of ICT in intelligence gathering within the Nigerian security system using documentary and literature review methods. The study established that ICT tools facilitate effective data and intelligence gathering, crime prevention, and information sharing among security agencies. However, challenges such as poor funding, inadequate training, and weak inter-agency collaboration hinder effective intelligence operations. The study recommended the implementation of a national intelligence gathering and sharing policy to strengthen collaboration and reduce duplication of efforts among security agencies.

On a broader scale, Al-Suqri and Gillani (2022) conducted a comparative analysis of information and artificial intelligence in relation to national security. Through a systematic literature review approach, the study found that AI plays a critical role in secure information management, cyber-attack prevention, and social media monitoring. The study highlighted that AI-driven systems improve threat analysis and support national security operations. Nevertheless, the authors warned that increased information accessibility through social media could also facilitate misinformation and cyber threats if not properly managed.

Likewise, Yeganegi K. and Ibrahim (2020) examined the role of information technology in national security using conference-based research analysis. The study emphasized that ICT reduces operational complexities and improves information sharing among governments and security institutions. Findings revealed that IT infrastructure and surveillance systems are crucial in combating modern security threats. The study concluded that nations must invest heavily in digital technologies and monitoring systems to strengthen homeland security.

Furthermore, Prianto et al., (2025) conducted a bibliometric analysis on digital transformation and national security strategies. The study revealed that technologies such as artificial intelligence, blockchain, and cybersecurity systems have become central to modern security architecture. The findings indicated that digital transformation improves efficiency in security operations but simultaneously introduces cybersecurity vulnerabilities. The study recommended adaptive policy frameworks to balance technological innovation with national security resilience.

Suleiman (2022) examined the prospects and challenges of applying ICT for national security in Nigeria. The study found that technologies such as surveillance systems, tracking mechanisms, and information-sharing platforms can effectively curb insecurity. However, Nigeria's technological limitations, inadequate infrastructure, and dependence on foreign assistance

constrain effective implementation. The study advocated for stronger technological investments and improved ICT deployment in security operations.

In another related study, Chima and Joseph (2022) investigated the adoption of digital solutions such as Automated Fingerprint Identification Systems (AFIS) and Closed-Circuit Television (CCTV) in managing insecurity in Nigeria. Using documentary evidence, the study revealed that despite the adoption of digital security tools, insecurity continues to rise due to corruption, inadequate ICT facilities, poor electricity supply, and lack of political will. The study concluded that e-governance and digital technologies are indispensable for addressing contemporary security challenges.

Similarly, Shehu et al., (2022) explored remote surveillance as a tool for intelligence gathering in Nigeria. Through secondary data analysis, the study proposed the use of wiretapping, geospatial intelligence, remote surveillance systems, and consolidated national databases for digital intelligence collection. The findings indicated that advanced surveillance technologies can significantly reduce insecurity when properly integrated into national security operations.

Additionally, Oyeboode (2022) examined the deployment of communication and digital technologies in addressing insecurity and environmental challenges in Nigeria. Using secondary data and expert opinions, the study found that digital technologies such as machine learning models, virtual simulations, and data integrity systems are essential in combating insecurity. The study emphasized the need for ICT-skilled personnel, improved networking, reliable power supply, and enhanced internet infrastructure for effective security management.

Finally, Odikpo (2025) investigated the application of artificial intelligence and media in curbing insecurity in the Niger Delta region. Adopting a survey research design with a sample size of 400 respondents, the study found that radio, television, and social media are commonly used platforms in combating insecurity. The study also revealed that AI technologies significantly contribute to peacebuilding, criminal detection, prosecution, and economic development in the region. The study recommended increased public sensitization and greater adoption of print and digital media in addressing insecurity.

This reviewed studies demonstrate that ICT, AI, digital surveillance systems, and digital transformation initiatives are increasingly essential for effective national security management in Nigeria. However, common challenges identified across the literature include inadequate ICT infrastructure, poor funding, corruption, weak policy implementation, insufficient technical expertise, and limited inter-agency collaboration. The literature therefore suggests the need for stronger institutional commitment, improved digital infrastructure, policy reforms, and enhanced capacity building to fully harness the benefits of ICT and AI in addressing

Conclusion

There is tightly intertwined nexus between law enforcement, information technology, community policing and internal security. A law enforcement community to engage technology in the most ethical, knowledgeable and legally compliant manner, will eventually attract community confidence, consent and partnership in a manner that will strengthen internal security. A law enforcement community that is not in synergy with the dynamics of technology or which deploys its technological assets with impunity will elicit distrust and disdain from the citizens in a manner that will threaten the virtues of internal security.

In consequence, for security agencies in Nigeria to take full advantage and opportunities that information technology provides, and to stay ahead of technology driven crimes and criminal

elements, it is imperative that the nation placed policies and invests towards having cutting edge technology that stand the test of time, and have trained and composed officers that possess the skills needed for the maintenance of the technology edge over and above the criminal actors. Strategic security players should equally appreciate the reality that technology on its own cannot engender internal security unless and until it is bonded with the people and with systems that will regulate its deployment.

These can only be achieved if police and other security managers at strategic levels move beyond the current level of technological illiteracy and develop skills and capacity that will not only enable them to clearly articulate their technological requirements but also to ensure that implementation strategies and deployment frameworks of acquired technologies are driven by highly ethical, legal, and professional standards and are guided by overriding community and national interest aimed at achieving internal security.

Until the country places conscious policies backed up with adequate budgetary funding to encourage policing agencies in Nigeria to upgrade their operations to this critical technological height, the law enforcement bodies in the country shall continue to play catch up with technology driven operations, our internal security management framework will continue to be under threats.

Policy recommendations

The Nigerian government can significantly improve internal security by adopting a coordinated national strategy for information technology-driven policing, intelligence gathering, and public safety management. A first and most critical step is the creation of a National Integrated Security Data Platform that connects all relevant agencies, including the police, immigration services, vehicle registration authorities, national identity management systems, and correctional services. This system should be built on a secure, government-controlled cloud infrastructure with standardized data formats and strict role-based access controls to ensure that only authorized personnel can retrieve sensitive information. Alongside this, the government should deploy a nationwide smart surveillance network in major cities and high-risk areas, using AI-enabled cameras capable of facial recognition, object detection, and real-time anomaly detection, all feeding into a centralized command and control centre to support rapid response to incidents.

In addition, Nigeria should fully enforce digital identity integration by making the National Identification Number the mandatory authentication system for all critical services such as telecommunications, banking, voting, and transportation-related registrations. This should be supported by biometric verification systems and real-time API integration between agencies to reduce identity fraud and enhance tracking of criminal activity. Internal security can also be strengthened through predictive policing, where a dedicated crime analytics unit within the police uses data and machine learning tools to identify crime hotspots, forecast potential security threats, and allocate personnel dynamically based on evidence-driven insights rather than reactive deployment.

Cybersecurity capacity must also be expanded through the establishment of a National Cybersecurity Operations Centre responsible for monitoring, preventing, and responding to cyber threats across government and critical infrastructure. All security agencies should maintain specialized cybercrime units trained in digital forensics and open-source intelligence, while private sector operators in telecoms, banking, and energy must be legally required to report cyber incidents promptly. Communication between security agencies should be modernized through a

secure, encrypted national communication system that ensures interoperability and real-time coordination among the police, military, and intelligence services.

Furthermore, border security should be fully digitized using biometric e-gates, handheld verification devices, and drone or satellite surveillance to monitor remote entry points, all integrated with national criminal databases. Emergency response systems should be unified under a single national emergency number supported by GPS-enabled dispatch systems that automatically route incidents to the nearest responders. To ensure accountability and reduce corruption, all arrest records, investigations, and evidence handling processes should be digitized with secure audit trails, and body cameras should be deployed for frontline officers to improve transparency.

Finally, long-term sustainability requires investment in human capital through scholarships, training programs, and innovation hubs focused on cybersecurity, artificial intelligence, and data science, with structured partnerships between government, universities, and the private sector. These reforms should be implemented through a phased national digital security transformation plan backed by strong legal frameworks, independent oversight mechanisms, and strict data protection laws to balance security effectiveness with civil liberties.

References

- Adamu, M. A. (2017), Internal security management and community policing in Nigeria: in Bassey C O and Ogbonnaya M. (eds) internal security crisis and community policing in Nigeria; policy option and strategies: Lagos : Concept publications.
- Afolayan, O. T. (2024). *Role of information and communications technologies in intelligence gathering in the Nigerian security system*. Adeleke University Journal of Business and Social Sciences, 4(1), 194–205.
- Aja A, (2017), internal security framework and community policing in Nigeria: A Theoretical perspective ; in Bassey C O and Ogbonnaya M, (eds) Internal security crisis and community policing in Nigeria: policy option and strategies: Lagos: concepts publications
- Al-Suqri, M. N., & Gillani, M. (2022). A comparative analysis of information and artificial intelligence toward national security. *IEEE Access*, 10, 64420–64434.
- Arase, S E (2016), Science, Technology and innovation framework for internal security and community policing in Nigeria; in Bassey, C O, and Ogbonnaya M, (eds) internal security crisis and community policing in Nigeria: policing option and strategies ; Lagos : concept publication.
- Bassey, C O. (2017) Internal security, challenges, system failure and community policing in Nigeria. In Bassey C O and Ogbonnaya M, (eds) internal security crisis and community policing in Nigeria: policy option and strategies: Lagos; Concept publications.
- Chima, P., & Joseph, I. S. (2022). Adoption of digital solutions in managing security challenges of the 21st century in Nigeria: Options for effective responses. *NDA Journal of Management Sciences Research*, 2(1), 334–341.
- Dimsey J S, (2008) Introduction to private security. Belmont: Thomas wardsworth publishers
- Ekwutosi, E. O., Effiong, E. N., & Inyang, E. B. (2021). The role of information technology in enhancing national security in Nigeria (2001–2020). *Pinisi Journal of Art, Humanity and Social Studies*, 1(1), 44–53.
- Henry S, (2000) what is security violence? An integrated definition, *Annals of the American Academy of political and social science*, 5(6) 16- 19
- Kemi, A. O. (2016). The role of information technology in national security: A case study of Nigeria. *Global Journals Inc., USA*, 16(3).
- Lawal, A. M., Bassey, E. E., & Tijjani, A. (2025). Community Policing and Economic Development in Nigeria. *Journal of Public Administration, Policy and Governance Research (JPAPGR)*, 3(4), 147-153
- Luara, S (2014), way of school security management, www.securitymanagement.com/article/school-lesson-005964
- Noonan, A. P. (2019). *Anarchist Terrorism and American National Security, 1881–1903* (Doctoral dissertation, Boston College).
- Odikpo, N. (2025). Application of artificial intelligence and media in curbing insecurity in the Niger Delta region. *Communication and Media Codes*, 2, 40–49.

- Oyebode, O. J. (2022). Deployment of communication and digital technology for the handling insecurity and environmental challenges in Nigeria. *Journal of Energy, Environmental and Carbon Credit*, 12(3), 17–27.
- Prianto, A. L., Amri, A. R., & Ilik, G. (2025). Digital transformation on national security strategy: A bibliometric analysis. *Advanced Research in Intelligence and National Security*, 1(1), 1–28.
- Shehu, A., Hadiza, A. K., & Sani, A. (2022). Remote surveillance: A means of intelligence gathering for minimizing security challenges in Nigeria. *Journal of Engineering Science*, (4), 59–71.
- Suleiman, M. M. (2022). Application of information and communication technology for national security: Prospects and challenges. *International Conference on Smart, Secure and Sustainable Nation*, 153–156.
- Yeganegi, K., Arbabi, Z., & Ibrahim Hussein, A. (2020). The role of information technology in national security. *Journal of Physics: Conference Series*, 1530(1), 012112.
- Zakari, M. (2024). Implication of artificial intelligence on national security for the Nigeria security agencies. *Journal of Terrorism Studies*, 6(1), 6.