# LEVERAGING TECHNOLOGY TO COMBAT INSECURITY IN NIGERIA: A LEGAL PERSPECTIVE

**By Esther Adeyemi**

**Abstract**

*In recent years, insecurity in Nigeria has evolved from isolated violent attacks to large-scale, tech-enabled crimes that threaten national stability. From banditry in the Northwest to cyber-enabled kidnapping rings in urban centers. The failure of traditional methods in combating insecurity in Nigeria is evident. This article examines the intersection of technology and security in Nigeria, evaluates the existing legal frameworks, identifies challenges, highlights international practices, and proposes recommendations for harmonizing technological innovations with the rule of law.*

**Keywords:** Insecurity, Crime, Technology, Artificial Intelligence, Law.

## 1.0 INTRODUCTION

In recent decades, Nigeria has witnessed an alarming rise in multifaceted insecurity challenges. Such as terrorism, spearheaded by groups like Boko Haram and ISWAP, which continues to ravage the North-East, and kidnapping for ransom has spread like wildfire across the North-West and Southern regions. Banditry, communal clashes, and armed robbery, plague vast rural areas. Also, cybercrime, locally dubbed "Yahoo Yahoo", has gained notoriety both domestically and internationally.

According to the Global Terrorism Index (2024), Nigeria remains among the top 10 countries most impacted by terrorism. Reports from SBM Intelligence indicate over 3,600 people were kidnapped across Nigeria in 2023 alone.[181] These grim statistics underscore the dire reality that insecurity threatens Nigeria's territorial integrity, economic viability, and social cohesion.

Traditional security measures, like the deployment of soldiers, sensitization of the public to be security-conscious, and other measures, although critical, have yielded limited success. For instance, the deployment of soldiers in the Northeast to combat the Boko Haram insurgency has

[181] David Ijaseun, 'Has the military tech failed to tame Nigeria's insecurity?' *Business Day* (19 February 2024)<https://businessday.ng/politics/article/has-the-military-tech-failed-to-tame-nigerias-insecurity/#:~:text=Businessday%20businessday,fight%20against%20kidnapping%20and%20insecurity > accessed 10 June 2025

not led to the desired outcomes, as the group continues to launch deadly attacks on civilians and security personnel. The infamous abduction of the Chibok girls in 2014 and the more recent attack on a school in Kankara, Kastina state, are stark reminders of the failure of traditional security methods.

In contrast, many countries around the world, have turned to technology to tackle insecurity. For example, in South Africa, the city of Cape Town has implemented a network of CCTV cameras and license plate recognition systems to monitor and prevent crime. In Rwanda, the government has launched a digital platform to report and track crime, allowing citizens to contribute to security efforts. Western countries have also leveraged technology to enhance security. In the United States, cities like New York and Chicago have implemented advanced surveillance systems including facial recognition technology, to identify and track potential threats. In the United Kingdom, the government has invested heavily in digital surveillance and data analytics to combat terrorism and other serious crimes.

These examples illustrate the growing recognition of technology's potential to match the evolving sophistication of these threats.

## 2.0 TECHNOLOGICAL INNOVATIONS ADDRESSING INSECURITY

Against this backdrop of unmet security needs, technology has emerged as a vital frontier where innovative tools can augment human effort, improve intelligence gathering, and create strategic deterrents. These interventions take many forms and can be grouped as part of a holistic modernization of Nigeria's security architecture. Importantly, such technologies are most effective when integrated with each other rather than deployed alone.

One key area is surveillance and situational awareness. High-resolution CCTV networks, satellite monitoring, unmanned aerial vehicles (UAVs, or drones) and other remote sensors can vastly expand the "eyes on the ground" available to security forces. In practice, a citywide CCTV grid similar to Britain's well-known public camera system allows law enforcement to monitor public spaces and rapidly identify criminal activity. Although exact figures vary, reports suggest the UK deploys millions of cameras nationwide, aiding investigations and deterring crime.[182]Nigeria has begun experimenting with such systems in metropolitan areas; for example,

[182] Pelco <https://www.pelco.com/blog/uk-cctv-crime-prevention>accessed 10 June 2025

the Lagos State government has installed hundreds of cameras at key junctions.[183] Likewise, drones offer promise in rural and border zones.[184] Satellite imagery and geospatial tools also allow authorities to detect patterns like mass movements of armed groups or identify illicit cultivation (such as marijuana or illicit cocaine plantations) in forested areas. By linking these platforms to central command-and-control centers, Nigeria can build a real-time security picture that would be impossible through boots on the ground alone.

Another pillar is biometric and data-driven identity systems. Accurately identifying criminals or suspicious persons is notoriously difficult in Nigeria's fluid population. To counter this, a robust national ID framework can ensure that individuals are known to the state. Nigeria has long had a National Identity Management Commission (NIMC) issuing identification numbers, and more recently the government has been integrating various government databases.[185] Lessons from countries with better experience are instructive here. For instance, India's Aadhaar system has created a 12-digit biometric identity for over 1.3 billion residents, this ID's uniquely linked to services ranging from banking to mobile phone registration.[186] In security terms, Aadhaar's authentication infrastructure allows agencies to verify an individual's identity against the national database nearly instantly. In practice, law enforcement in India can use biometric fingerprint or iris scanners on smartphones to check a person's identity against Aadhaar, deterring identity fraud and aiding criminal investigations. Nigeria can adapt this model by further leveraging its own NIN (National Identification Number) system. For example, connecting crime records and watch lists to biometric ID databases means that even nomadic or undocumented suspects could be identified on the spot. Of course, such linkage raises privacy considerations, but the core idea is powerful if police can instantly confirm that a detained suspect's fingerprint matches a known felon in the system, then weak evidentiary cases and mistaken releases can be reduced.

---

[183] Titilola Oludimu, 'Lagos state's new surveillance system amplifies the need for a unified database', *Techpoint.africa*(3 May, 2017)<https://techpoint.africa/general/lagos-surveillance-system/>accessed 10 June 2025

[184] Pat Medina, 'Lagos, Nigeria Might Deploy Drones to Fight Crime' *Futurism*( 28, October, 2015)<https://futurism.com/lagos-nigeria-might-deploy-drones-to-fight-crime>accessed 10 June 2025

[185] Biometric post, 'The New Nigeria ID Card: A More Inclusive Digital Identity' *Aratek (14 August, 2024)*<https://www.aratek.co/news/the-new-nigeria-id-card-a-more-inclusive-digital-identity accessed 10 June 2025

[186] Ted O'Callahan, 'What Happens When a Billion Identities Are Digitized?' Yale Insights(27 March,2020)<https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized> accessed 10 June 2025

Furthermore, terrorist groups and criminal gangs increasingly use encrypted messaging apps and social media for planning. Nigeria's security agencies have begun deploying signals intelligence (SIGINT) tools to intercept communications, but the field is evolving. Advanced software can be applied to data analytics and artificial intelligence to sift through large volumes of communications or social media posts. For example, a machine-learning system might flag keywords or patterns indicating a planned raid or rally. In addition, digital forensics can crack phones or memory cards recovered from suspects, turning snippets of data into actionable leads. Financial networks, critical energy grids, and even election machinery have all been targets of cyber threats; therefore, developing strong cybersecurity capabilities, both defensive measures (like firewalls and intrusion detection) and offensive capacities (the ability to disrupt criminal botnets), is now part of national security. Estonia, a global leader in e-governance, has taught the world how to build resilience after a series of cyber-attacks in 2007: it enshrined secure digital IDs and mandatory incident reporting into law.[187] Nigeria has enacted cybercrime legislation and is building a CERT (Computer Emergency Response Team) to coordinate responses to cyber incidents.[188] By integrating cyber defenses with other security work (like, using financial transaction monitoring to track criminal financing), technology creates an interconnected net that catches bad actors who might slip past traditional patrols.

Furthermore, the use of Artificial Intelligence and Predictive Policing Artificial Intelligence (AI) applications in predictive policing can identify crime hotspots, forecast criminal activities, and optimize resource deployment. AI tools analyzing vast datasets can detect patterns invisible to human analysis, thereby pre-empting security breaches. For instance, predictive policing is transforming law enforcement worldwide by leveraging data analytics to forecast criminal activities.[189] Below are some examples of the benefits and challenges of utilizing predictive policing as experienced by different countries. In the United States, in cities like Los Angeles, predictive policing has led to a 12% reduction in property crimes. The Angeles Police Department's (LAPD) use of PredPol software has helped allocate resources more efficiently,

[187] Isabel Skierka, 'When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis' Government Information Quarterly 40 (2023) 101781,<www.elsevier.com/locate/govinf>accessed 10 June 2025

[188] Cybercrimes( Prohibition Prevention, etc.) Amendment Act 2015, s14

[189] Anyck Sturgeon, ' Is AI-powered Predictive Policing Good, Great or Ugly? LinkedIn (4, September 2024)<https://www.linkedin.com/pulse/ready-more-ai-based-predictive-policing-anyck-turgeon-dl3bc?utm_source=share&utm_medium=member_android&utm_campaign=share_via>accessed 10 June 2025

resulting in a notable decrease in burglaries and vehicle thefts.[190]The Tokyo Metropolitan Police in Japan implemented predictive policing to address rising cybercrimes, leading to a 15% reduction in reported cyber incidents. The system's ability to predict and prevent cybercrimes proved highly effective[191] However, criticisms over algorithmic bias and racial profiling have necessitated reevaluation of such programs.

Importantly, these technologies should not be viewed in isolation but as synergistic. For example, a CCTV system may identify a fleeing suspect, who's biometric ID then automatically flags a criminal record, triggering an alert that mobilizes a drone or drone-like response. Or, intelligence from signal intercepts may direct satellites to monitor a hideout. By weaving these tools together with analytics, biometrics, drones, and cameras, Nigeria can create a 21st-century security apparatus where information flows quickly between field officers and decision-makers. This shift requires significant investment in infrastructure and training, but the upside is that a relatively small team equipped with the right tools can achieve surveillance coverage and investigative depth far beyond what large but disconnected forces could accomplish.

## 3.0 LEGAL AND REGULATORY CONSIDERATION

The advent of technology has brought about a paradigm shift in our approach to security. From surveillance systems to artificial intelligence-powered analytics, technology has proven to be a potent tool in the fight against insecurity. However, as we harness the power of technology to tackle security threats, it is imperative that we do so within the bounds of the law.

One of the key legal considerations in leveraging technology for security purposes is the regulatory framework governing its use. In Nigeria, surrounding surveillance, data protection, and cybersecurity are still evolving to keep pace with rapid technological advancements. For instance, the use of facial recognition technology in public spaces raises concerns about privacy and data protection.[192] The American case of **Katz v. United States**[193] underscores that surveillance activities without appropriate judicial authorization violate constitutional rights.

[190] Ibid
[191] Ibid
[192] R (Bridges) v Chief Constable of South Wales Police [2020]EWCA Civ 1058, shows the necessity of balancing surveillance with privacy rights.
[193] 389, U.S. 347 (1967)

Similarly, the deployment of drones for surveillance purposes raises questions about airspace regulations and liability in the event of accidents.

Another critical legal issue is the handling and admissibility of digital evidence in investigations and prosecutions. As technology advances, digital evidence is becoming increasingly important in criminal investigations. However, the integrity and authenticity of digital evidence can be easily compromised which can have serious implications on the integrity of the investigation and the prosecution. The use of technology in security operations also raises questions about liability and accountability, for instance, if an autonomous security system like artificial intelligence, drones malfunctions and causes harm to innocent individuals, who bears the liability? The manufacturer, the operator, or the system itself? These are complex questions that require careful consideration of legal principles and regulatory frameworks. While these technologies have the potential to revolutionize security, they also raise complex legal questions about their use and regulation.

The existing laws in Nigeria aimed at tackling insecurity, starting from the **Constitution of the Federal Republic of Nigeria, 1999 (as amended),** which serves as the foundation for all security-related interventions. **Section 14(2) (b)**[194] provides that "the security and welfare of the people shall be the primary purpose of government." Similarly, **Section 45** [195] permits restrictions on certain rights in the interest of national security, public safety, or public order, enabling lawful surveillance and restrictions in times of insecurity. **Section 37**[196]of guarantees and protects the privacy of citizens in their homes, correspondence, telephone conversations, and telegraphic communications. However ***section 45*** provides for the interception of communication.

Other laws in Nigeria enable the use of technology to address insecurity these include the Cybercrimes (Prohibition and Prevention, Etc.) Act, 2024, Nigeria Data Protection Act, 2023 Terrorism (Prevention and Prohibition) Act, 2022, The Economic and Financial Crimes Commission (Establishment, etc.) Act, 2004, The Money Laundering (Prevention and Prohibition) Act, 2022, and The Nigerian Communications Communication Act, 2003.

[194] The 1999 Constitution of the Federal Republic of Nigeria ( as amended)
[195] Ibid
[196] Ibid

However, a critical examination reveals that these laws do not expressly provide for the high use of technology tools like CCTV, block chain, AI, robots, and drones in security operations. Moreover, these laws lack specific provisions protecting citizens' rights and freedoms when these tech tools are used. This legislative gap raises concerns about potential abuses of power, infringement on individual privacy rights, and lack of accountability for technology-related errors.

The increasing deployment of emerging technologies in security operations necessitates a review of the existing legal framework. Nigeria's laws must be updated to address the integration of these technologies, ensuring that individual rights are safeguarded while leveraging technology to enhance security. A nuanced approach is required to balance security needs with individual freedoms. This can be achieved by enacting laws that specifically regulate the use of emerging technologies in security operations, provide guidelines for data protection and privacy, and establish clear liability and accountability frameworks.

Ultimately, the effective use of technology in security operations requires a robust legal framework that protects citizens' rights while promoting national security. By updating its laws, Nigeria can harness the benefits of emerging technologies while ensuring that individual freedoms are respected. As supported by the Latin maxim *'salus populi suprema lex esto',* the welfare of the people shall be the supreme law these legal frameworks affirm the state's authority to adopt technological measures in securing lives and property, provided such measures are reasonable, necessary, and proportionate to the threat posed.

## 4.0 CONCLUSION

Technological innovation holds immense potential for addressing Nigeria's multifaceted security challenges, technology must not become a substitute for the rule of law or a justification for rights violations. An equilibrium must be struck where technological adoption enhances security while safeguarding constitutional liberties. International experiences demonstrate that technology, when embedded in a robust legal and ethical framework, can significantly strengthen security governance.