African Journal of Social and Behavioural Sciences (AJSBS)
Volume 16, Number 2 (2026) ISSN: 2141-209X

# HARNESSING BIOMETRIC SIM REGISTRATION IN FIGHTING INSECURITY AND CRIMINALITY IN SOUTH-EASTERN NIGERIA

**Chinwendu Shedrack Njoku**

Department of Political Science, Faculty of Social Sciences, Kingsley Ozumba Mbadiwe University, Ideato, Imo State, Nigeria

shedrack.njoku@komu.edu.ng

**ABSTRACT:** The rising incidence of insecurity and criminality in Nigeria, particularly in South-Eastern Nigeria, continues to threaten socio-economic stability, public safety, and national development. Criminal networks increasingly exploit mobile communication technologies to coordinate kidnappings, armed robbery, cybercrime, and other organized offenses, often relying on anonymity enabled by weak Subscriber Identity Module (SIM) registration systems. This study examines biometric SIM registration as a strategic intervention for combating insecurity and criminality in the region. Adopting a qualitative research design based on secondary data and theoretical interpretation, the study draws on criminological perspectives and biometric identification frameworks to assess the policy's effectiveness. Anchored in structural functionalist theory, the analysis conceptualizes biometric SIM registration as a structural mechanism introduced to restore social order by linking mobile subscribers to verifiable biometric identifiers such as fingerprints and facial data. The findings suggest that biometric integration enhances traceability, strengthens intelligence-led policing, and aligns with primary and secondary crime prevention strategies by increasing the risk of detection and reducing opportunities for anonymous communication. However, challenges relating to data protection, institutional coordination, infrastructural deficits, and public trust limit its full potential. The study concludes that biometric SIM registration can significantly strengthen Nigeria's security architecture if supported by robust governance mechanisms. It recommends that the National Identity Management Commission (NIMC) ensure the integrity and security of the National Identity Database (NIDB) to prevent breaches and fraudulent activities. Furthermore, the Nigerian Communications Commission (NCC), NIMC, and security agencies must establish a unified and real-time data-sharing protocol to enhance coordinated enforcement and investigative efficiency.

**Keywords:** Biometric SIM Registration; Insecurity; Crime Prevention; Identity Management; South Eastern Nigeria

## INTRODUCTION

The persistence of crime and organized criminal activities in Nigeria continues to pose profound threats to national security, social cohesion, and economic development. Insecurity manifested through terrorism, kidnapping, armed robbery, cybercrime, and other violent offenses undermines public confidence, disrupts legitimate socio-economic activities, and projects an image of instability to the international community. Such conditions discourage both domestic and foreign

investment, thereby constraining sustainable development. The interconnection between insecurity and underdevelopment has been widely acknowledged in criminological literature, particularly within developing societies where weak institutional capacity compounds enforcement challenges (Dambazau, 2007).

Between 2009 and 2012, Nigeria experienced an alarming escalation in terror-related violence. Reports by Human Rights Watch indicate that approximately 2,800 lives were lost during this period, with 815 deaths recorded in the first nine months of 2012 alone in 275 suspected attacks attributed to Boko Haram (Human Rights Watch, 2012). These attacks included the killing of security personnel and the destruction of public infrastructure, including police stations and the national police headquarters in Abuja. Although much of the insurgency was concentrated in northern Nigeria, the ripple effects of insecurity have extended across the country, contributing to rising fear, displacement, and economic disruption. In recent years, South-Eastern Nigeria has also grappled with increasing incidents of kidnapping, armed violence, separatist unrest, and cyber-enabled crimes, further intensifying concerns over regional stability.

Contemporary criminal networks increasingly exploit advances in information and communication technologies to coordinate activities, evade detection, and expand operational reach. Mobile telephony and internet-based communication platforms have become central tools in planning and executing criminal acts. The anonymity historically associated with poorly regulated Subscriber Identity Module (SIM) registration systems has complicated efforts by security agencies to trace suspects and disrupt criminal networks. This technological dimension of crime presents both a challenge and an opportunity for law enforcement institutions.

Against this backdrop, biometric SIM registration has emerged as a strategic innovation in crime prevention and control. Biometrics refers to the automated recognition of individuals based on unique physiological or behavioral characteristics such as fingerprints, facial features, iris patterns, or voice recognition (Jain, Ross, & Prabhakar, 2004). Unlike traditional identity systems that rely on easily falsifiable documents, biometric systems are designed to be universal, unique, permanent, and collectable, thereby enhancing reliability in identity verification (Uludag et al., 2004). By linking SIM cards to verified biometric data, authorities can significantly reduce anonymity in telecommunications usage, strengthen investigative processes, and deter criminal misuse of mobile networks.

From a crime control perspective, biometric SIM registration aligns with broader preventive strategies aimed at increasing the risk of detection and reducing opportunities for offending (Dambazau, 2007). In South Eastern Nigeria, where digital communication plays a pivotal role in both legitimate commerce and illicit coordination, the effective harnessing of biometric registration systems offers a technology-driven pathway toward strengthening security architecture. However, its implementation also raises important questions concerning data protection, civil liberties, institutional capacity, and public trust.

This study, therefore, seeks to answer the following research question: To what extent can biometric SIM registration contribute to combating insecurity and criminality in South-Eastern Nigeria, and what institutional, technological, and ethical challenges affect its effectiveness? By addressing this

question, the study examines the extent to which biometric-based identity management can enhance crime detection, prevention, and control, while also considering the practical and ethical challenges associated with its deployment.

## LITERATURE REVIEW

The prevalence of crime across the world today is a matter of grave concern. Crime undermines the social fabric of society by eroding the sense of safety and security among citizens. Its impact varies depending on its nature and magnitude, but it becomes a serious social problem when its occurrence is so widespread that it threatens the security of lives and property, as well as social order and cohesion (Onoge, 1988).

The cost of crime may be tangible or intangible, economic or social, direct or indirect, physical or psychological, and may affect individuals or entire communities. These costs form the basis for understanding the consequences of crime. They may arise from direct victimization, such as physical injury, theft, or destruction of property. They may also manifest as psychological trauma and emotional distress suffered by victims. Additionally, resources expended in attempts to prevent or control crime constitute another dimension of its cost. In extreme cases, persistent crime can alter demographic patterns, prompting migration from crime-prone areas to relatively safer communities. Such movements may result in brain drain and broader socio-economic challenges.

Émile Durkheim viewed crime as a normal and inevitable feature of society, present in all historical periods. He maintained that certain crimes particularly mala prohibita offenses (acts criminalized because they violate social norms) serve important social functions. They help define acceptable behavior and can stimulate social change by testing and redefining societal boundaries. Crime, like many social science concepts, lacks a universally accepted definition. While it may seem simple to equate crime with moral wrongdoing, moral standards differ across societies. Not all moral wrongs are criminal offenses, nor are all criminal acts necessarily considered immoral. Legally, crime refers to the violation of laws established by a governing authority, punishable through formal sanctions such as fines, imprisonment, or capital punishment.

Quinney (1980) argues that crime reflects class struggle within society. According to this perspective, laws are created by dominant groups to protect their interests, while marginalized groups may engage in criminal acts due to structural inequalities and deprivation. The dominant class also shapes public narratives about crime in ways that legitimize its authority. Scott & Marshall (2009) argue that crime poses a significant threat to a nation's economic, political, and social stability. It discourages both local and foreign investment, reduces quality of life, destroys human and social capital, weakens the relationship between citizens and the state, and ultimately undermines democracy and the rule of law. Scott & Marshall (2009) further define crime as an offense that transcends personal harm and enters the public domain, violating prohibitory laws and requiring intervention by public authorities. For an act to be officially recognized as a crime, it must be reported, recorded, and processed by law enforcement agencies, and may subsequently form part of criminal statistics.

From a normative perspective, crime is viewed as deviant behavior that violates societal norms and cultural expectations. This approach emphasizes that definitions of crime are influenced by social, political, and economic contexts. Behaviors may be criminalized or decriminalized over time, thereby affecting crime statistics and shaping public perception.

Dambazau (1994) defines crime as an act or omission against public interest, prohibited by law and punishable upon conviction. He identifies four essential elements of crime: public wrong, moral wrong, legal prohibition, and punishment. Criminologists generally agree that crime comprises two fundamental elements: the act itself (actus reus) and the mental intent (mens rea). Without both elements, a crime cannot legally exist. Nigeria, like many developing nations, has experienced rising crime rates since the 1980s (Dambazau, 1994). Crimes range from armed robbery, murder, rape, and burglary to fraud, corruption, human trafficking, cybercrime, and money laundering. Concerns persist regarding inadequate political will to combat crime effectively, especially where corruption exists within leadership structures. The case of former Delta State Governor James Ibori, who was convicted in the United Kingdom for money laundering after acquittal in Nigeria, exemplifies challenges in prosecuting corruption cases.

Crime control, according to Dambazau (2007), involves strategies aimed at reducing crime threats and enhancing public safety. It includes apprehending suspects, prosecuting offenders, and preventing future criminal behavior. Crime prevention, however, focuses on disrupting the causes of crime before it occurs.

Crime prevention strategies are generally categorized into three levels (Robert, 2003):

i. **Primary Prevention** – Focuses on altering environmental conditions that create opportunities for crime, increasing the risk and effort required to commit offenses while reducing potential rewards.
ii. **Secondary Prevention** – Targets individuals at high risk of offending through early intervention programs involving media, community organizations, and NGOs.
iii. **Tertiary Prevention** – Concentrates on rehabilitating offenders and preventing recidivism through correctional and probation services.

In recent years, biometric technology has emerged as a tool in crime prevention and identity verification. Biometrics refers to the automated recognition of individuals based on physiological or behavioral characteristics (Uludag, 2004). Physiological biometrics include fingerprints, facial recognition, iris scans, retina scans, and hand geometry. Behavioral biometrics involve patterns such as voice recognition, keystroke dynamics, and signature verification.

Jain (2003) notes that an ideal biometric system should be universal (possessed by all individuals), unique (distinct for each person), permanent (unchanging over time), and collectable (easily measurable). However, practical implementation also requires attention to performance, user acceptability, and resistance to fraud (Ross, 2005). Advances in biometric technologies have led to standardized frameworks such as BioAPI to enhance system interoperability (Adler, 2004). Today, biometric authentication supports applications including web security, transaction verification, remote access, and data protection (Maltoni, 2003).

Physiological biometrics rely on measurable physical traits, while behavioral biometrics are based on patterns of action over time. Although behavioral systems measure actions, these behaviors are influenced by physiological characteristics, such as vocal cord structure in voice recognition or hand shape in signature verification.

**Theoretical Framework**

The structural functionalist theory provides a valuable lens to understand biometric SIM registration in Nigeria as a structural intervention to combat insecurity It views society as a system composed of interrelated parts that work together to maintain equilibrium and stability. According to Durkheim, institutions exist because they serve necessary functions, such as regulation, integration, and the reinforcement of collective values (Durkheim, 1938/1997). Parsons (1951) further explained that every society must perform four functional imperatives—adaptation, goal attainment, integration, and latency (AGIL). The stability of the system depends on whether social structures effectively carry out these roles. Insecurity in Nigeria disrupts social stability, while biometric SIM registration is designed to serve as a structural response to restore balance by aiding law enforcement, deterring crime, and fostering trust in public institutions

From a structural functionalist perspective, biometric SIM registration can be analyzed as a structural mechanism introduced into the Nigerian system to address the dysfunction caused by insecurity. Its functions can be classified into manifest and latent functions, alongside its role in the broader AGIL framework.

**Manifest Functions:** The manifest function of biometric SIM registration is to link every phone number to a verifiable identity, making it possible for security agencies to track communications associated with criminal activities. This directly addresses the challenge of anonymous phone usage by criminals and enhances the capacity of the state to investigate and prosecute offenders. It also strengthens public trust in the state's ability to regulate telecommunications for collective security.

**Latent Functions:** Latently, biometric SIM registration promotes order and integration by reinforcing the value of accountability in communication. It creates a sense of deterrence, as individuals are aware that their mobile communications can be traced. Furthermore, it generates a reliable national database that can serve beyond security purposes—such as planning, electoral management, and social services.

**Dysfunctions:** Despite its intended goals, structural functionalism also acknowledges dysfunctions within institutions. Biometric SIM registration has been marred by inefficiencies, corruption, and poor technological infrastructure in Nigeria. Many citizens have registered multiple times due to poor database management, while others in rural areas face challenges due to limited access to registration centers. Criminals have also adapted by using stolen or pre-registered SIM cards, thereby undermining the policy's effectiveness (Adebayo, 2020). These dysfunctions reduce public confidence in government institutions and perpetuate distrust in the system.

**Application of the theory to the topic.**

Applying Structural Functionalist Theory to the relationship between harnessing biometric SIM registration in the fight against insecurity and criminality in Nigeria provides a systematic framework for explaining how technology-driven regulation can contribute to restoring social order and institutional stability. Structural functionalism conceives society as a complex system made up of interrelated institutions government, law enforcement, the telecommunications sector, and regulatory agencies, each performing functions necessary for maintaining equilibrium and social cohesion (Talcott Parsons, 1951; Robert K. Merton, 1968). When these structures fail to perform effectively, dysfunction arises, resulting in deviance, crime, and social disorder.

Within this framework, the telecommunications sector constitutes an essential social structure that facilitates communication, economic transactions, and national integration. However, the proliferation of anonymous and poorly regulated SIM cards in Nigeria has created systemic dysfunction by enabling criminal actors to coordinate kidnapping, armed robbery, insurgency, and other illicit activities while evading identification. Studies show that mobile phones are frequently used to plan ransom negotiations and violent attacks, thereby weakening the capacity of security agencies to perform their protective and regulatory roles (Nigerian Communications Commission, 2021; National Bureau of Statistics, 2022). This breakdown in institutional control undermines societal stability and public trust.

Biometric SIM registration can thus be interpreted as an adaptive mechanism designed to restore functional balance. By linking SIM cards to unique biometric identifiers, the policy enhances traceability, strengthens intelligence gathering, and improves law enforcement's ability to detect and apprehend offenders. In functionalist terms, it reinforces social control, promotes normative compliance, and supports the integrative and regulatory functions of the state (Parsons, 1951).

Nevertheless, structural functionalism also emphasizes that the effectiveness of any reform depends on the proper functioning of all interdependent institutions. Persistent challenges—such as weak enforcement, corruption, inadequate infrastructure, and data protection vulnerabilities—represent continuing dysfunctions that limit the policy's impact. Consequently, biometric SIM registration can only contribute meaningfully to reducing insecurity when embedded within broader institutional and governance reforms that strengthen coordination, accountability, and socio-economic development.

## METHODOLOGY

This study adopts a qualitative desk-based research design based on secondary data and theoretical analysis. Relevant sources including peer-reviewed articles, books, government policy documents, regulatory reports, and credible media publications were purposively selected for their relevance to biometric SIM registration, crime prevention, and insecurity in Nigeria, particularly between 2009 and 2025. Data were analyzed using qualitative content analysis through thematic review and interpretive synthesis. Structural Functionalist Theory guided the analysis in explaining biometric SIM registration as a structural response to insecurity.

**Biometric SIM Registration, Insecurity, Criminality and Social Order**

Insecurity undermines social order by generating fear, eroding trust among citizens, and weakening the legitimacy of state institutions. From the perspective of structural functionalism, society operates as an interconnected system in which each institution performs essential roles necessary for stability and continuity. When a critical component such as the security apparatus—fails to function effectively, the resulting imbalance threatens the entire social structure. Other institutions must then adapt and strengthen their roles to restore equilibrium. In South Eastern Nigeria, rising incidents of kidnapping, armed robbery, separatist violence, and cybercrime have disrupted social harmony and diminished public confidence in governance. In response, the Nigerian state has sought to harness biometric SIM registration as a technological mechanism to reinforce security and restore order.

Biometric SIM registration links mobile phone subscribers' identities to verifiable physiological data within a centralized national database. By reducing anonymity in telecommunications usage, the system is designed to enhance the capacity of law enforcement agencies to trace communications associated with criminal and terrorist activities. In principle, this strengthens investigative processes, deters the misuse of communication networks, and reinforces governance structures. Within South Eastern Nigeria, where mobile communication plays a significant role in coordinating both legitimate commerce and illicit operations, biometric registration provides a strategic tool for disrupting criminal networks.

However, insecurity in the region persists despite the introduction of biometric controls. Criminal actors have demonstrated adaptability, often using cloned SIM cards, virtual private networks (VPNs), identity theft, and other digital evasive tactics to bypass regulatory measures. Kidnappers frequently rely on mobile phones to negotiate ransom payments, while cybercriminal syndicates exploit online platforms to perpetuate fraud. These realities indicate that while biometric SIM registration addresses a critical structural gap, it cannot function effectively as a standalone solution.

Structural functionalism suggests that restoring systemic equilibrium requires coordinated interaction among multiple institutions. In South Eastern Nigeria, effective harnessing of biometric SIM registration must be complemented by robust intelligence sharing among agencies such as the Department of State Services (DSS), the Nigerian Police Force (NPF), and the Nigerian Communications Commission (NCC). Judicial efficiency, prosecutorial diligence, and legal reforms are equally essential to ensure that biometric evidence leads to successful convictions. Furthermore, community-based security initiatives and local intelligence networks can bridge trust deficits between citizens and the state, facilitating early detection and prevention of criminal activities.

Therefore, harnessing biometric SIM registration in South-Eastern Nigeria represents a functional and technologically driven response to insecurity and criminality. Yet, sustainable social order can only be achieved when technological regulation, law enforcement, judicial systems, and community participation operate synergistically. Through such integrated efforts, the region can move toward restoring stability, strengthening public trust, and achieving a more secure and balanced social system.

**Biometric SIM Registration in Nigeria**

Biometric SIM registration in Nigeria forms part of the national digital identity policy implemented by the National Identity Management Commission (NIMC), which requires telecommunications subscribers to link their Subscriber Identity Modules (SIMs) with their National Identification Number (NIN). The policy is designed to establish a comprehensive identity management system by connecting individuals' biometric information to their mobile phone numbers. The primary objective of this initiative is to strengthen national security and reduce criminal activities such as kidnapping, terrorism, and financial fraud that often rely on anonymous communication channels. By ensuring that every SIM card is linked to a verified identity, the government seeks to eliminate anonymity in telecommunications systems and improve the ability of law enforcement agencies to trace criminal communications (Gelb & Clark, 2013; World Bank, 2018).

The initiative aligns with global trends in digital identity governance, where biometric identification systems are increasingly adopted to enhance public administration and security management. Biometric identification systems use unique physical characteristics, such as fingerprints and facial recognition, to authenticate individuals, making them more reliable than traditional identification methods (Jain, Ross, & Nandakumar, 2011). In many developing countries, biometric identity systems have been introduced to improve governance, enhance service delivery, and strengthen law enforcement capabilities. Scholars argue that digital identity infrastructures can improve accountability and enable governments to better regulate communication networks and financial transactions (Gelb & Clark, 2013).

Despite these anticipated benefits, the effectiveness of SIM registration policies in reducing crime remains widely debated. Studies examining SIM registration policies across several countries indicate that such measures often fail to significantly reduce criminal activities because offenders can circumvent registration requirements through fraudulent identities or informal markets for pre-registered SIM cards (Martin & Taylor, 2021). In Nigeria, the persistence of kidnapping, fraud, and other crimes despite the widespread implementation of the NIN–SIM linkage policy has led many analysts to question whether biometric SIM registration alone can effectively address the country's complex security challenges.

Beyond questions about effectiveness, the implementation of the policy has encountered substantial logistical and operational challenges. The NIN enrollment process, which is required before SIM linkage can occur, has been characterized by infrastructural limitations, inadequate registration facilities, and technical difficulties. These challenges are particularly pronounced in rural areas, where access to registration centers and digital infrastructure remains limited. As a result, many citizens have experienced long queues, system failures, and delays in obtaining their NIN, making compliance with the policy burdensome for large segments of the population (World Bank, 2019).

In addition to operational difficulties, biometric SIM registration raises significant concerns regarding data privacy and security. The creation of centralized databases containing sensitive biometric data presents potential risks if adequate data protection mechanisms are not implemented. Unlike passwords or identification cards, biometric identifiers cannot easily be replaced once compromised. Consequently, a breach of biometric databases could expose individuals to long-term

risks such as identity theft, financial fraud, and unauthorized surveillance (Jain et al., 2011). Scholars of surveillance studies have also warned that large-scale biometric identification systems may expand state surveillance capabilities and potentially undermine civil liberties if appropriate legal safeguards and oversight mechanisms are not in place (Lyon, 2018).

Another important concern relates to the potential exclusionary effects of the policy. Mandatory SIM registration requirements can disproportionately affect vulnerable populations who lack formal identification documents or who face barriers in accessing registration centers. Individuals living in rural communities, internally displaced persons, and economically disadvantaged groups often encounter significant challenges in obtaining official identification documents. When access to telecommunications services becomes contingent on possessing a national identity number, these populations risk being excluded from essential communication services and digital financial platforms that increasingly rely on mobile connectivity (Martin & Taylor, 2021). Such exclusion can deepen existing socioeconomic inequalities and limit access to economic opportunities and public services.

Furthermore, critics argue that biometric SIM registration policies may create opportunities for state-sponsored surveillance if strong legal protections are absent. Centralized identity databases enable governments to track communication activities more easily, raising concerns about potential misuse of personal information for political monitoring or suppression of dissent. Surveillance scholars emphasize that while digital identity systems can enhance security, they must be accompanied by transparent governance structures, independent oversight mechanisms, and comprehensive data protection regulations to prevent abuses of power (Lyon, 2018).

The financial and operational costs associated with implementing biometric identity systems also represent a significant challenge. Establishing and maintaining biometric databases requires substantial investments in technology infrastructure, equipment, and personnel training. Governments must allocate considerable financial resources to maintain these systems and ensure their security and reliability. When the anticipated security benefits of such systems are not clearly demonstrated, policymakers may face questions about the long-term sustainability and cost-effectiveness of biometric registration initiatives (Gelb & Clark, 2013).

Overall, Nigeria's biometric SIM registration policy illustrates the complex relationship between digital identity technologies, national security objectives, and civil liberties. While the initiative reflects a broader global movement toward digital identification systems intended to strengthen governance and improve security, its implementation reveals significant challenges related to infrastructure, data protection, and social inclusion. The persistence of informal markets for pre-registered SIM cards and the limited evidence of substantial crime reduction highlight the limitations of relying solely on technological solutions to address complex security problems.

For biometric SIM registration to achieve its intended objectives, it must be integrated into a broader strategy that includes robust legal frameworks for data protection, transparent governance structures, and improved digital infrastructure. Strengthening institutional capacity, ensuring independent oversight, and addressing the socioeconomic factors that contribute to insecurity are essential steps toward building public trust and maximizing the benefits of digital identity systems.

Without these complementary measures, biometric SIM registration may struggle to balance the goals of national security, privacy protection, and social inclusion.

**Prospects of Biometric SIM Registration**

The prospects of biometric SIM registration in combating insecurity and criminality in South-Eastern Nigeria generate both optimism and caution among policymakers and scholars. The policy, implemented through the National Identity Management Commission (NIMC) and regulated by the Nigerian Communications Commission (NCC), requires mobile subscribers to link their Subscriber Identity Modules (SIMs) with their National Identification Number (NIN). The central objective of this initiative is to strengthen national security by eliminating anonymity in telecommunications systems and enabling the traceability of mobile communications used in criminal activities. By linking biometric data such as fingerprints and facial recognition to mobile phone numbers, law enforcement agencies can more effectively identify and track individuals involved in crimes such as kidnapping, cyber fraud, armed robbery, and organized criminal activity (Gelb & Clark, 2013; World Bank, 2018).

Biometric identification systems have increasingly been adopted worldwide as part of broader digital identity initiatives aimed at improving governance, strengthening law enforcement capabilities, and enhancing service delivery. Biometric technologies provide a reliable means of identifying individuals because they rely on unique physiological characteristics that are difficult to falsify or duplicate (Jain, Ross, & Nandakumar, 2011). In the context of telecommunications regulation, linking biometric identity to SIM cards is expected to reduce the ability of criminals to use anonymous communication channels to coordinate illegal activities. Scholars argue that digital identity infrastructures can enhance transparency and accountability in communication networks while supporting crime detection and prevention efforts (Gelb & Clark, 2013).

In South-Eastern Nigeria, where crimes such as kidnapping for ransom and cyber fraud have become significant security concerns, biometric SIM registration holds the potential to strengthen investigative capabilities. By enabling authorities to trace communication records to verified individuals, the policy could facilitate more efficient intelligence gathering and disrupt criminal networks that rely heavily on mobile communication technologies. In theory, the availability of a centralized identity database can support coordinated law enforcement responses and improve the speed at which security agencies identify suspects involved in criminal operations (World Bank, 2019).

However, the realization of these benefits depends largely on addressing persistent implementation challenges. One of the major obstacles undermining the effectiveness of SIM registration policies in many countries is the existence of informal markets for pre-registered SIM cards, which allow individuals to bypass identity verification procedures. Research on SIM registration policies globally indicates that such loopholes significantly weaken the intended security benefits of identity-linked telecommunications systems (Martin & Taylor, 2021). In Nigeria, the continued availability of improperly registered SIM cards limits the ability of security agencies to fully rely on telecommunications data for criminal investigations.

To improve the prospects of biometric SIM registration in South Eastern Nigeria, stronger institutional collaboration between regulatory authorities and security agencies is essential. Effective coordination between the NCC, NIMC, and law enforcement institutions could enhance monitoring and enforcement mechanisms designed to prevent the circulation of unregistered or fraudulently registered SIM cards. Additionally, improvements in technological infrastructure, including efficient data verification systems and secure law enforcement access to identity databases, are necessary to translate the theoretical benefits of the policy into practical security outcomes.

Another critical factor influencing the success of biometric SIM registration is public trust in the management of personal data. The creation of large centralized databases containing sensitive biometric information raises important privacy and data protection concerns. Because biometric identifiers cannot easily be changed once compromised, inadequate security safeguards could expose individuals to identity theft, financial fraud, or unauthorized surveillance (Jain et al., 2011). Scholars of surveillance and digital governance emphasize that strong legal frameworks and independent oversight mechanisms are necessary to prevent misuse of personal data and ensure that identity systems are used strictly for legitimate purposes (Lyon, 2018).

Strengthening data protection regulations and ensuring transparent governance practices would therefore play an important role in building citizen confidence in biometric SIM registration initiatives. Public trust is particularly important in encouraging compliance with identity registration policies, as citizens are more likely to participate in such programs when they believe their personal information is adequately protected. Furthermore, integrating the national identity system with other identity verification platforms could enhance the reliability of the digital identity ecosystem and reduce opportunities for identity fraud.

Despite these challenges, biometric SIM registration has the potential to contribute meaningfully to broader security reforms in South-Eastern Nigeria if implemented effectively. However, scholars caution that technological solutions alone cannot fully address complex security challenges. Crime and insecurity are often influenced by socioeconomic factors such as unemployment, poverty, and weak institutional capacity. Consequently, digital identity policies should be integrated into broader strategies that include intelligence gathering, community policing initiatives, judicial reforms, and socioeconomic development programs (Gelb & Clark, 2013; Lyon, 2018).

## Conclusion

The Nigerian government's policy of mandatory biometric SIM registration represents a significant, though complex, step toward addressing insecurity and criminality in South-Eastern Nigeria by creating a traceable digital identity for mobile phone users. While the concept is theoretically sound, linking SIM cards to identifiable individuals in order to deter anonymous criminal activities, its practical implementation has revealed persistent challenges. The continued circulation of unregistered and fraudulently registered SIM cards, combined with increasingly sophisticated criminal networks capable of circumventing regulatory controls, demonstrates that digital identity systems alone cannot fully resolve the region's security challenges. Logistical limitations,

insufficient enforcement mechanisms, and limited integration with other national security databases have constrained the policy's effectiveness in curbing criminal activities.

The success of biometric SIM registration in South-Eastern Nigeria ultimately depends on its integration into a broader and more comprehensive security framework. For the policy to move beyond a procedural compliance exercise and become an effective crime-control tool, it must be supported by robust data protection legislation, improved collaboration among regulatory agencies and security institutions, and sustained efforts to build public trust in digital identity systems. The effectiveness of the initiative should not be measured merely by the number of SIM cards successfully linked to national identities, but by the capacity of government institutions to utilize this information responsibly, securely, and strategically in criminal investigations and intelligence operations. Without these complementary reforms, biometric SIM registration risks remaining a well-intentioned but limited solution in its ability to fully achieve the goal of a safer, more secure, and digitally inclusive South-Eastern Nigeria.

**Recommendations**

To effectively leverage biometric SIM registration in addressing insecurity and criminality in Nigeria, a multi-dimensional strategy is required. Rather than relying solely on the technical process of SIM–NIN linkage, the government and relevant institutions must adopt broader structural and institutional reforms. The following recommendations are proposed:

**i. Strengthening Data Security and Public Trust**: The National Identity Management Commission (NIMC) must ensure the integrity and security of the National Identity Database (NIDB) through robust cyber security infrastructure, regular system audits, and strict enforcement of penalties for unauthorized access or data breaches. Strengthening data protection measures will enhance public confidence in the biometric identity system and encourage greater compliance with registration requirements.

**ii. Enhancing Institutional Collaboration and Data Integration**: Effective coordination among the Nigerian Communications Commission (NCC), NIMC, telecommunications service providers, and national security agencies is essential. These institutions should establish an integrated and secure real-time data-sharing framework that facilitates intelligence gathering and enhances investigative efficiency. Improved interoperability among national databases will enable law enforcement agencies to trace communications more effectively and respond more rapidly to criminal activities.

**iii. Eliminating the Circulation of Pre-Registered SIM Cards**: Regulatory authorities must enforce stricter monitoring of SIM card registration and distribution processes. Telecommunications operators and licensed vendors should be required to implement stringent identity verification procedures, while the sale and distribution of pre-registered SIM cards should attract severe regulatory sanctions and penalties. Eliminating the informal market for improperly registered SIM cards is critical for maintaining the credibility and effectiveness of the biometric registration system.

**iiv. Strengthening Law Enforcement Capacity**: Security agencies should be equipped with modern investigative tools, digital forensic capabilities, and advanced communication technologies to enable them to effectively utilize biometric registration data. Adequate training in cybercrime investigation and digital intelligence analysis will further enhance the ability of law enforcement personnel to identify and prosecute offenders.

**v. Addressing the Socioeconomic Drivers of Crime**: Technological interventions alone cannot fully resolve insecurity. Government policies should also address underlying socioeconomic factors such as unemployment, poverty, and youth marginalization, which often contribute to criminal behavior. Expanding employment opportunities, supporting youth empowerment initiatives, and investing in social development programs can reduce incentives for criminal involvement.

**vi. Promoting Community Engagement and Public Awareness**: Sustained public awareness campaigns should be implemented to educate citizens about the importance of biometric SIM registration in strengthening national security. Encouraging cooperation between communities and law enforcement agencies will help improve intelligence gathering, enhance early detection of criminal activities, and strengthen trust between citizens and the state.

**REFERENCES**

Adebayo, T. (2020). Challenges of biometric SIM registration and criminal adaptation in Nigeria. *Journal of Security Studies, 5*(2), 45–60.

Adler, A. (2004). Sample images can be independently restored from face recognition templates. In *Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1163–1166). IEEE. https://doi.org/10.1109/CCECE.2004.1347336

Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. Cambridge University Press.

Dambazau, A. B. (1994). *Criminology and criminal justice*. Nigerian Defence Academy Press.

Dambazau, A. B. (2007). *Criminology and criminal justice* (2nd ed.). Spectrum Books.

Durkheim, É. (1997). *The division of labor in society* (W. D. Halls, Trans.). Free Press. (Original work published 1893)

Gelb, A., & Clark, J. (2013). *Identification for development: The biometrics revolution*. Center for Global Development.

Gomez-Barrero, M., & Galbally, J. (2024). Reversing the irreversible: A survey on inverse biometrics. *arXiv*. https://doi.org/10.48550/arXiv.2401.02861

Human Rights Watch. (2012). *Spiraling violence: Boko Haram attacks and security force abuses in Nigeria*. Human Rights Watch.

Jain, A. K. (2003). Biometric recognition: How do I know who you are? *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20.

Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of fingerprint recognition*. Springer.

Martin, A. K., & Taylor, L. (2021). Exclusion and identity in the digital state: SIM registration and digital ID systems. *Information Technology for Development, 27*(3), 1–17.

Merton, R. K. (1968). *Social theory and social structure*. Free Press.

National Identity Management Commission. (n.d.). *National identification number (NIN) enrolment and SIM linkage guidelines*. National Identity Management Commission.

Onoge, O. F. (1988). *Crime and deviance in Nigerian society*. Malthouse Press.

Parsons, T. (1951). *The social system*. Free Press.

Quinney, R. (1980). *Class, state, and crime: On the theory and practice of criminal justice*. Longman.

Robert, B. (2003). Crime prevention strategies and community safety. *International Journal of Social Policy, 12*(3), 215–229.

Ross, A. (2005). Multibiometric systems. In A. K. Jain, P. Flynn, & A. A. Ross (Eds.), *Handbook of biometrics* (pp. 289–320).

Scott, J., & Marshall, G. (2009). *A dictionary of sociology* (3rd ed.). Oxford University Press.

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE, 92*(6), 948–960.

World Bank. (2018). *ID4D global dataset: Identification for development*. World Bank.

World Bank. (2019). *Digital identity: Towards shared principles for public and private sector cooperation*. World Bank.