ISSN: **3107-6513**

Forensic Genomics and the Future of Continental Security

Designing an African Union DNA Security Architecture for Peace, Justice, and Counterterrorism in a Transforming Africa

Success Adeleke Dayisi[#1], Abubakar Bashir Saulawa[*2]
[1]Department of International Relations and Political Science, University of Abuja, Nigeria
[2]Department of Cybersecurity, Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Nigeria.
1dayisisuccess@gmail.com, 2Abubakarslw2@gmail.com

Abstract:
The African Union (AU) confronts a peace and security landscape that has grown more volatile and more fragmented since 2020, marked by the persistence of Boko Haram and the Islamic State West Africa Province in the Lake Chad Basin, the expansion of Jama'at Nasr al-Islam wal Muslimin across the Sahel, the entrenchment of Al-Shabaab in the Horn of Africa, the resurgence of M23 and allied armed groups in the eastern Democratic Republic of Congo, the civil war that has engulfed Sudan since April 2023, and a persistent wave of unconstitutional changes of government that has left Burkina Faso, Guinea-Bissau, Madagascar, Mali, Niger, and Sudan under African Union suspension as of early 2026. Against this backdrop, this study examines the strategic case for a harmonized African Union DNA Security Architecture (AUDSA): a continental forensic genomics framework capable of strengthening criminal investigation, counterterrorism, victim identification, and border and migration management across the Union's fifty-five member states and their constituent Regional Economic Communities. Drawing on Human Security Theory, Constructivism, and Technological Determinism, and employing a qualitative design combining comparative case analysis (South Africa, Nigeria, Ghana, Rwanda, and the European Union and INTERPOL as global benchmarks) with policy and document analysis, the study finds that forensic DNA capacity across Africa remains fragmented, under-resourced, and legally uneven, even as national initiatives South Africa's National Forensic DNA Database, Nigeria's National DNA Data Bank, and Kenya's Huduma Namba biometric programme demonstrate growing institutional appetite for genomic and biometric modernization, even as the AU's own continental e-passport, first announced in 2016, remains largely symbolic nearly a decade later. The study argues that the coup-driven suspensions of the mid-2020s, rather than foreclosing continental forensic cooperation, make a technically interoperable, legally safeguarded, and politically adaptable AUDSA more urgent, since terrorism and trafficking networks continue to operate across the boundary between AU-recognized governments and suspended transitional authorities regardless of institutional standing. It proposes a hub-and-spoke architecture, anchored in the AU Commission's Peace and Security Department and the African Peace and Security Architecture (APSA), that pairs continental standard-setting with implementation through the Regional Economic Communities ECOWAS, IGAD, SADC, ECCAS, and the EAC grounded in harmonized legislation, independent ethical oversight, and interoperability standards aligned with the AU's Malabo Convention. The study concludes that forensic genomics, responsibly governed, offers the African Union a credible pathway from reactive crisis management toward evidence-based, technology-enabled peacebuilding consistent with Agenda 2063's ambition to silence the guns.

Keywords: African Union; DNA forensics; continental security architecture; African Peace and Security Architecture; human security; counterterrorism; digital forensics; Africa

I. INTRODUCTION

Africa's security environment has deteriorated markedly since the mid-2010s. The Global Terrorism Index reports that the Sahel has for a second consecutive year accounted for a plurality of global terrorism deaths, driven by the sustained expansion of Boko Haram, the Islamic State West Africa Province (ISWAP), and Jama'at Nasr al-Islam wal Muslimin (JNIM), even as Al-Shabaab's insurgency in Somalia and the wider Horn of Africa, the M23-led rebellion in the eastern Democratic Republic of Congo, and the civil war between the Sudanese Armed Forces and the Rapid Support Forces since April 2023 have opened additional theatres of mass displacement and armed violence (Global Terrorism Index, 2025). The African Union (AU), established in 2002 as successor to the Organisation of African Unity, has for more than two decades served as the continent's principal peace and security actor through the African Peace and Security Architecture (APSA) comprising the Peace and Security Council, the Continental Early Warning System (CEWS), the African Standby Force (ASF), the Panel of the Wise, and the Peace Fund operating in coordination with the continent's Regional Economic Communities (World Peace Foundation, 2025). Yet the institutional terrain within which the AU operates has itself become markedly more volatile. Since 2019, the Union has suspended the membership of successive states in response to military takeovers, and as of early 2026, six member states Burkina Faso, Guinea-Bissau, Madagascar,

Mali, Niger, and Sudan remain under suspension and in varying stages of political transition, even after the reinstatement of Guinea and Gabon following elections judged to have restored constitutional order (Amani Africa, 2026; ISS Africa, 2023). This is, by the Peace and Security Council's own reckoning, among the highest simultaneous suspension totals in the organisation's history.

This fragmentation has occurred precisely as the AU's own flagship continental biometric initiative has stalled, even as national and sub-regional institutions have pressed ahead independently. The African Union e-passport, announced in 2016 at the 27th Ordinary Session of the Assembly in Kigali as a flagship project of Agenda 2063 and intended to enable visa-free travel across all fifty-five member states, remains issued almost exclusively to heads of state, diplomats, and senior officials nearly a decade later, with mass rollout to ordinary citizens indefinitely delayed (au.int, 2016; FurtherAfrica, 2022). Meanwhile individual states and Regional Economic Communities have advanced their own systems: Nigeria's National Identification Number and its ECOWAS-linked biometric identity card, Ghana's Ghana Card, and Kenya's Huduma Namba each represent significant, if imperfect, national progress. Yet DNA forensics the most rigorous scientific method available for establishing human identity remains largely undeveloped and entirely unharmonized at the continental level. Only a small number of states, notably South Africa, Nigeria, Ghana, and Kenya, possess operational national DNA laboratories, and no AU instrument currently permits the systematic cross-border exchange of forensic genetic data. This study argues that this gap is no longer marginal: as the AU's institutional map has grown more complex a core of member states in good standing operating alongside a security-critical periphery of states under suspension but geographically and operationally inseparable from continental counterterrorism and trafficking corridors the case for a technically robust, ethically governed, and politically adaptable African Union DNA Security Architecture (AUDSA) has become more urgent, not less.

This article situates the analysis within this evolving continental landscape. It examines the current state of forensic DNA capacity across AU member states; evaluates the applicability of global cross-border forensic models the European Union's Prüm Convention, INTERPOL's DNA Gateway, and South Africa's and Nigeria's national DNA data banks to a continent whose regional architecture is not static; and proposes an institutional design for AUDSA that explicitly accounts for the suspension of multiple member states, the stalled continental biometric passport, and the multiplying theatres of armed conflict across the Sahel, the Lake Chad Basin, the Horn of Africa, and the Great Lakes region. In doing so, the study contributes a current, policy-relevant analysis of how forensic genomics can strengthen counterterrorism, anti-trafficking, migration management, and post-conflict justice across a continent whose peace and security architecture continues to evolve in real time.

II. Literature Review and Conceptual Framework

A. DNA Forensics as a Security Instrument

Deoxyribonucleic Acid (DNA) is the hereditary material unique to each individual (barring identical twins), making it the most reliable scientific basis for personal identification available to modern law enforcement (Butler, 2015). Since Sir Alec Jeffreys's discovery of DNA fingerprinting in the mid-1980s, forensic DNA profiling has become central to criminal investigation, the exoneration of the wrongly convicted, disaster victim identification, and kinship verification. Centralized forensic databases the United States' Combined DNA Index System (CODIS) and the European Union's Prüm Convention framework demonstrate how institutionalized DNA data can accelerate cross-border investigation while preserving due process (Bredan & Rutten, 2021; National Human Genome Research Institute, 2023). In Africa, operational forensic DNA capacity remains concentrated in a handful of states South Africa, whose National Forensic DNA Database was formally established under the Criminal Law (Forensic Procedures) Amendment Act, Nigeria, Ghana, and Kenya leaving most of the continent's fifty-five member states without a reliable scientific means of identity verification in security operations (Ngari & Odah, 2020).

B. Peace, Security, and Technology in Africa

Contemporary security scholarship distinguishes negative peace, the mere absence of violence, from Johan Galtung's (1969) positive peace, encompassing justice, institutional legitimacy, and social equity, and situates both within the human security paradigm articulated by the UNDP (1994), which centers the safety and dignity of individuals rather than states. The African Union's own security architecture has evolved along broadly comparable lines, combining the political, military, and early-warning instruments of APSA with normative frameworks such as the African Charter on Democracy, Elections and Governance and the 2009 Ezulwini Framework on unconstitutional changes of government. Yet transnational threats terrorism, trafficking, identity fraud, and organized crime increasingly outpace institutions built primarily for interstate conflict management and coup response, a gap that recent scholarship on African regional security (Kieh, 2020; Osaghae, 2022; Arieff, 2023) attributes as much to weak forensic and identity infrastructure as to political will.

C. Digital Forensics and Convergent Technologies

Digital forensics the identification, preservation, and analysis of electronic data for investigative purposes has become indispensable as extremist and criminal networks exploit digital communications, mobile financial services, and encrypted platforms for recruitment, financing, and coordination (Casey, 2019; Eboh & Adeoye, 2023). The African Union's Malabo Convention on Cyber Security and Personal Data Protection (2014), together with the African Union Mechanism for Police Cooperation (AFRIPOL), the African Centre for the Study and Research on Terrorism (ACSRT), and the Committee of Intelligence and Security Services of Africa (CISSA), signal growing continental institutional recognition of this threat, though enforcement capacity remains weak and adoption of the Malabo Convention itself remains partial across the membership. The convergence of biological (DNA) and digital forensic evidence for example, cross-referencing a genetic profile recovered from a conflict site with mobile network or financial transaction data represents an emerging frontier capable of producing a far stronger evidentiary chain than either method alone, increasingly reinforced by artificial intelligence tools that can reduce DNA sequencing and matching times from weeks to hours (National Human Genome Research Institute, 2023).

III. Theoretical Framework

This study is anchored in three complementary theories. Human Security Theory (UNDP, 1994) reframes security

around individual safety and dignity rather than state sovereignty alone, and situates DNA forensics as a protective, empowering, and restorative instrument preventing repeat offending, granting evidentiary credibility to victims of violence and trafficking, and enabling the identification of the missing and the dead in post-conflict settings from the Sahel to the Great Lakes. Constructivism, following Wendt (1999), holds that regional cooperation is socially constructed through shared norms and mutual trust rather than dictated by material capability alone; applied here, it explains how a harmonized forensic data-sharing norm, as the EU's Prüm Convention demonstrates, can transform relations among security agencies from mutual suspicion toward institutionalized collaboration, even among states with divergent political systems and, within the AU context, even among states whose formal political standing is temporarily suspended. Technological Determinism (Marx, 1859; McLuhan, 1964) holds that technological innovation is itself a driver of institutional and social transformation; applied to the African Union, it predicts that the institutionalization of DNA and digital forensic systems will compel member states to modernize investigative, judicial, and border-management institutions, catalyzing continental standardization in ways that political negotiation alone including the AU's repeated cycle of suspension and reinstatement has not achieved. Read together, these theories position forensic genomics not as a neutral technical add-on but as simultaneously a moral obligation, a norm-building exercise, and a structural transformation, one whose relevance is heightened, not diminished, by the AU's coup-suspension cycle, since Constructivism in particular suggests that technical cooperation frameworks can sometimes sustain relationships that formal political membership no longer does.

IV. Methodology

The study adopts a qualitative, exploratory design combining comparative case analysis, document analysis, and synthesis of the current policy and news record. Five cases were purposively selected to reflect varying stages of forensic development and institutional maturity across Africa's principal sub-regions: South Africa, examined for its National Forensic DNA Database and its application in criminal investigation at continental scale; Nigeria, examined for its National DNA Data Bank (2017) and its application in counterterrorism and insurgency-zone investigations in the Lake Chad Basin; Ghana, examined for its Forensic Science Laboratory and the integration of DNA into criminal justice and identity verification; Rwanda, examined for its post-1994 genocide identification programmes and their long-term contribution to transitional justice and reconciliation in the Great Lakes region; and the European Union and INTERPOL, examined comparatively for their Prüm Convention and DNA Gateway frameworks respectively, as global benchmarks for cross-border forensic cooperation. Document analysis draws on African Union treaties and protocols, the Malabo Convention on Cyber Security and Personal Data Protection (2014), the ECOWAS Supplementary Act on Personal Data Protection (2010) as an illustrative Regional Economic Community instrument, national forensic and data-protection legislation, and contemporaneous reporting on AU suspensions, political transitions, and biometric identity initiatives through early 2026. Data were analyzed thematically, with findings organized around the study's four analytical domains criminal justice and counterterrorism, human trafficking, border and migration management, and digital forensic integration before being synthesized into the proposed AUDSA framework.

V. Findings and Discussion

A. DNA in Criminal Justice and Counterterrorism

The persistence of Boko Haram, ISWAP, and JNIM across the Lake Chad Basin and the Sahel, the entrenchment of Al-Shabaab in Somalia and the wider Horn of Africa, and the resurgence of M23 and allied armed groups in the eastern Democratic Republic of Congo have repeatedly exposed the limits of confession- and testimony-based investigation, which is vulnerable to coercion, manipulation, and witness intimidation. DNA profiling offers an objective alternative: biological trace evidence recovered from attack sites, improvised explosive devices, mass graves, or detained combatants can identify perpetrators, corroborate intelligence, and support prosecutions that withstand judicial scrutiny. Nigeria's National DNA Data Bank, established under the National Biotechnology Development Agency in 2017, has already been applied to disaster victim identification and selected criminal cases, though inconsistent funding, weak inter-agency coordination, and the absence of comprehensive DNA legislation constrain its counterterrorism application (Olabode & Ezenwa, 2021). South Africa's National Forensic DNA Database demonstrates a more mature trajectory, having been used to link serial offences and secure convictions at national scale, while Ghana's Forensic Science Laboratory shows a comparable pattern in a more institutionally stable environment, with DNA increasingly integrated into homicide and sexual assault prosecutions. These cases confirm the study's central proposition: where deployed, forensic DNA measurably strengthens conviction rates and judicial credibility (Eze, 2022), but its counterterrorism value across the continent remains capped by the absence of any mechanism to share or compare data across the multi-country theatres Nigeria–Niger–Chad–Cameroon in the Lake Chad Basin; Somalia–Kenya–Ethiopia in the Horn of Africa; and the DRC–Rwanda–Uganda–Burundi nexus in the Great Lakes in which these networks and conflicts actually operate.

B. DNA and Counter-Trafficking

Human trafficking and smuggling routes spanning West Africa, the trans-Saharan corridor into North Africa, and the Horn of Africa's migration routes toward the Gulf and the Mediterranean continue to exploit porous borders and weak identity verification, disproportionately affecting women and children. DNA-based kinship verification, deployed in partnership with the International Organization for Migration and INTERPOL's DNA Gateway which INTERPOL has promoted globally as a tool for identifying missing persons through family DNA (INTERPOL, 2021) offers a credible mechanism for confirming the origins of trafficked persons, reuniting separated families, and establishing evidentiary links between traffickers and victims that do not depend on victim testimony alone, a critical advantage given the intimidation and re-traumatization that often undermine prosecutions. A proposed Continental DNA Trafficking Registry, nested within AUDSA and subject to strict human-rights safeguards, would formalize this capability across member states, operationalizing the AU's own commitments on trafficking under the Ouagadougou Action Plan framework. Here again, the AU's coup-suspension cycle complicates rather than eliminates the imperative: trafficking corridors through the Sahel, the Horn of Africa, and Central Africa remain active irrespective of a given state's AU standing, meaning any registry confined strictly to member states in good standing would leave a critical gap in

exactly the territory most implicated in continental trafficking flows.

C. DNA, Biometrics, and Border and Migration Management

The AU's 2018 Protocol to the Treaty Establishing the African Economic Community Relating to Free Movement of Persons, Rights of Residence and Right of Establishment remains foundational to the Union's integration ambitions but has struggled to enter into force at continental scale and has long been vulnerable to exploitation by criminal and extremist networks through document fraud and multiple identities. The AU's own flagship response the continental e-passport announced in 2016 and intended to abolish visa requirements across all fifty-five member states illustrates the gap between ambition and delivery: nearly a decade later it remains, in practice, a largely symbolic instrument issued to a small circle of officials and diplomats rather than a functioning continental identity layer (Grokipedia, 2026). Into this vacuum, national and Regional Economic Community-level systems have advanced unevenly: Nigeria's ECOWAS-linked biometric identity card, Ghana's Ghana Card, and Kenya's Huduma Namba each embed facial and fingerprint biometrics into national or sub-regional credentials, but none currently interoperates with the others at continental scale. DNA-based identity verification represents the logical next layer of assurance beyond biometrics, particularly for cases asylum verification, disputed parentage, unaccompanied minors, and disaster victim identification where fingerprint or facial data cannot resolve identity with certainty. The practical lesson for AUDSA is unambiguous: a continental forensic architecture cannot afford to wait on the AU's own stalled biometric passport project, and must instead be designed from the outset to interoperate technically with the more advanced national and REC-level systems that already exist.

D. Digital Forensic Integration and Emerging Technologies

The convergence of DNA forensics with digital intelligence, artificial intelligence, and geospatial analytics represents the most consequential frontier for the AU's peace and security modernization. Linking a future AUDSA database with the Continental Early Warning System (CEWS) would allow predictive identification of high-risk movement patterns, terrorist financing networks, and identity duplication in near real time, complementing the analytical work already carried out by ACSRT and the intelligence-sharing function of CISSA. AI-assisted DNA sequencing, underpinned by secure data-collection protocols and interoperable data-merging technologies (Eboh & Adeoye, 2023), has already reduced analysis turnaround from weeks to hours in advanced forensic systems, a capability with direct relevance to time-sensitive counterterrorism and disaster-response operations, while blockchain-based recordkeeping offers a credible mechanism for preserving chain-of-custody integrity and deterring data tampering. A Continental Forensic and Digital Evidence Centre, situated within the AU Commission's Peace and Security Department and operated in partnership with INTERPOL and AFRIPOL, would provide the institutional home for this convergence, standardizing data-collection protocols and training forensic professionals across a continent where such expertise remains acutely scarce and unevenly distributed.

E. The Coup-Suspension Cycle and Its Implications for a Continental Forensic Architecture

The wave of unconstitutional changes of government that began in 2019 and accelerated after 2021 constitutes one of the most significant institutional stress tests in the African Union's history and carries direct implications for any continental forensic architecture. Between June 2019 and August 2023 alone, the AU suspended seven member states Sudan, Mali, Guinea, Burkina Faso, Niger, and Gabon, in addition to an earlier Sudan suspension with Guinea-Bissau and Madagascar added to the list following coups in late 2025 (ISS Africa, 2023; PSC Report, 2023). As of early 2026, six states Burkina Faso, Guinea-Bissau, Madagascar, Mali, Niger, and Sudan remain suspended and in political transition, even as Guinea's suspension was lifted in January 2026 following a presidential election judged by the Peace and Security Council to have restored constitutional order, and Gabon's suspension was lifted earlier still (Amani Africa, 2026). This pattern demonstrates both the persistence of institutional volatility as a structural feature of continental governance and the existence of a credible pathway back to good standing. Yet counterterrorism, trafficking, and displacement do not respect the boundary between suspended and recognized states: fighters, traffickers, and displaced populations continue to move across Sahelian, Central African, and Horn of Africa frontiers regardless of a government's formal AU status, and Sudan's civil war in particular has produced one of the world's largest displacement crises without regard to the country's suspended standing. This study therefore argues that AUDSA should be designed from the outset as a two-tier architecture: a fully integrated core encompassing member states in good standing, and a parallel technical protocol modeled on the EU's practice of forensic cooperation with non-member states through which suspended states and their transitional authorities could participate in narrowly defined, humanitarian and counterterrorism-specific data exchange (for example, disaster victim identification or trafficking-victim family reunification) without requiring full reinstatement of political membership. The demonstrated pattern of suspension followed by eventual reinstatement, evident in the Guinea and Gabon cases, further reinforces the case for a forensic architecture resilient enough to function amid continued political flux, rather than one designed around a static assumption of fifty-five states permanently in good standing.

F. Institutional Fragmentation, Database Interoperability, and Foreign Technology Dependency: The Nigerian Case

Beyond the DNA-specific gaps identified above, Nigeria's experience illustrates a deeper structural weakness that plausibly generalizes across much of the continent: the absence of a single, statutorily empowered forensic investigation agency comparable to the forensic institutes operated in the United States and across the European Union. Existing capacity is instead distributed piecemeal across the Economic and Financial Crimes Commission, the Nigeria Police Force, the Office of the National Security Adviser, and a small number of private and university-affiliated laboratories, none of which holds the combined statutory mandate, standardized accreditation, and nationwide reach that a dedicated forensic authority would provide (Sibe & Muller, 2022; Odo, 2026). Nigeria's own federal training authorities have acknowledged that digital forensic science, despite being indispensable to modern security operations, remains comparatively underdeveloped relative to the scale of cyber-enabled crime, cyberterrorism, and extremist exploitation of digital and financial infrastructure the country now confronts (Voice of Nigeria, 2026). This deficit is compounded by law-enforcement agencies improvising forensic workflows without the technological, human-resource, and funding baseline that

genuine forensic readiness requires (Sibe & Muller, 2022), and by the urban concentration of what limited capacity exists, which leaves large parts of the country effectively outside the reach of scientific investigation (Odo, 2026). Absent a body empowered to set and enforce binding national forensic standards, chains of custody, and cross-agency evidentiary protocols, any future AUDSA node hosted in Nigeria and in member states with comparable institutional gaps across the continent risks resting a continental architecture on an unstable national foundation.

A related and arguably more consequential constraint is the fragmentation of Nigeria's administrative and security databases, a pattern with clear analogues elsewhere on the continent. Although the National Identity Management Commission has presented the National Identification Number (NIN) as a unifying identity layer intended to harmonize sectoral identifiers such as the Bank Verification Number (BVN), independent assessments by technology analysts, bankers, and policy researchers find that seamless interoperability has not been achieved in practice, and that citizens continue to resubmit the same biometric and biographic data to agencies that maintain independent, non-communicating databases (Vanguard, 2026; HumAngle, 2026). Nigeria currently operates at least seven parallel identity systems the NIN, BVN, voter's card, driver's licence, Tax Identification Number, Corporate Affairs Commission registration, and international passport each purpose-built and none designed to reconcile records with the others, a fragmentation that a federal payroll audit linked to the discovery of more than 23,000 unverifiable 'ghost workers' drawing salaries from the public purse (Businessday NG, 2026). The security and financial-intelligence implications are direct: because the Central Bank of Nigeria's transaction-monitoring systems, the Nigeria Police Force's criminal records, the Nigeria Immigration Service's travel and border data, and the military's operational intelligence do not share a common, queryable identity layer, prosecutors attempting to establish the full financial trail behind a terrorism-financing charge frequently cannot assemble, within the statutory window available for pre-trial detention, a complete picture of a suspect's transaction history across institutions and years (Blueprint Newspapers, 2025). This evidentiary gap is not hypothetical: despite official assurances that the state possesses intelligence on terrorism-financing networks, this intelligence has only inconsistently translated into arrests, prosecutions, and convictions capable of withstanding judicial scrutiny, with several high-profile financing cases stalling or being downgraded to lesser charges after failing to produce a prosecutable financial record (Ibrahim, 2026). The Financial Action Task Force's own regional assessment of terrorist financing in West Africa similarly found that concealment of the financial trail of financiers, through cash couriers, informal value-transfer networks, and cross-border smuggling, remains among the most persistent obstacles to prosecution (Financial Action Task Force, 2013), a pattern replicated in the financing networks that sustain Al-Shabaab in the Horn of Africa and armed groups in the eastern DRC. Fragmentation therefore does not merely inconvenience citizens applying for services; it materially degrades the state's capacity to convert counterterrorism intelligence into admissible evidence, a gap that any future AUDSA financial-forensic module must treat as a foundational design constraint rather than an implementation afterthought.

The same fragmentation undermines even routine cross-institutional verification. Completion of the National Youth Service Corps (NYSC), which many federal, paramilitary, and military recruitment processes formally require, cannot currently be authenticated in real time against a central NYSC database by an independent agency such as the Nigeria Immigration Service or the Armed Forces; verification instead relies on the physical presentation of a discharge certificate, a paper-based instrument that is vulnerable to forgery and unavailable for cross-checking at the point of recruitment. Nigerian technologists interviewed on the state of the country's digital identity infrastructure attribute this pattern to a broader institutional reality in which agencies maintain differing biometric standards and lack full real-time access to one another's databases (HumAngle, 2026). Programmes such as the Nigeria Data Exchange framework and the e-Government Interoperability Framework have been introduced to address this gap, but their own architects concede that most agencies continue to operate independent databases under distinct legal mandates, so that the country can identify its citizens in principle yet struggles to verify them reliably in practice (Businessday NG, 2026). For a continental forensic and biometric architecture such as AUDSA, whose value depends entirely on the reliability of cross-referencing identity, criminal history, and biometric data across institutions and borders, this national-level interoperability failure is a precondition that must be resolved domestically, in Nigeria and comparable member states alike, before continental-level data exchange can be meaningfully implemented.

A fourth constraint, largely absent from existing literature on African forensic capacity, is the continent's structural dependence on foreign-supplied digital forensic and surveillance technology, and the vulnerability this dependence creates. Investigative research by the University of Toronto's Citizen Lab documented that a Nigerian security agency had acquired signalling-system interception technology from the Israeli firm Circles, a company commercially and technically affiliated with the NSO Group, as part of a pattern replicated across at least twenty-five governments worldwide (Citizen Lab, 2020). Such arrangements illustrate a broader risk directly relevant to AUDSA's design: because the underlying software, licensing, and technical support for these systems originate with a small number of external vendors operating under their home governments' export-control regimes, client states have no independent guarantee of continued access. NSO Group itself has confirmed suspending several government clients' access to its technology following misuse investigations, without those governments' consent or advance notice (Estrin, 2021). For a member state whose early-warning, financial-tracing, or counterterrorism capability has come to depend on a single foreign vendor's platform, such a suspension whether prompted by misuse findings, licensing disputes, or shifts in the exporting country's foreign policy can remove operational capability overnight and without recourse. This vulnerability is reinforced at the policy level: digital forensic and cyber-surveillance systems have been formally incorporated into the European Union's dual-use export control list, and the export-control regimes of major supplier states more broadly including the United States, Russia, France, and Israel routinely subject licensing and technology-transfer decisions for such systems to national-security and foreign-policy considerations rather than to the recipient state's operational need (Bromley, 2017, 2020). The consequence for the African Union is that forensic sovereignty cannot be achieved through

procurement alone: a continental architecture built primarily on licensed, externally supported platforms will remain hostage to the political and commercial decisions of exporting states. This underscores the case, developed further in Section 7, for AUDSA to prioritize regionally owned intellectual property, open and auditable technical standards, and negotiated technology-transfer agreements with academic and industry partners, rather than exclusive reliance on turnkey systems procured from external suppliers.

VI. Challenges and Ethical Considerations

Seven categories of challenge condition the feasibility of AUDSA. First, privacy and human rights: DNA data is uniquely sensitive, revealing genetic heritage and familial relationships far beyond simple identity, and its collection without robust legal safeguards risks violating the African Charter on Human and Peoples' Rights; only a minority of AU member states currently maintain comprehensive data-protection legislation, and the Malabo Convention on Cyber Security and Personal Data Protection (2014) has yet to achieve the ratification threshold needed for widespread enforcement. Second, institutional and financial capacity: DNA analysis requires specialized laboratories, reliable power, cold-chain storage, and trained personnel that remain scarce and unevenly distributed, concentrated overwhelmingly in a handful of urban centers across the continent. Third, legal fragmentation: the absence of harmonized forensic legislation across fifty-five jurisdictions means DNA evidence collected in one state may be inadmissible in another, creating exploitable gaps for transnational criminal and terrorist networks; a Continental Model Law on Forensic and DNA Data Governance, aligned with the Malabo Convention, would address this directly. Fourth, the risk of political misuse: in states with fragile democratic institutions or recent histories of unconstitutional government, genetic data gathered for counterterrorism purposes could be repurposed for surveillance, ethnic profiling, or political persecution absent independent oversight a risk this study regards as the single most consequential barrier to public trust and therefore to AUDSA's long-term legitimacy. A fifth and increasingly salient challenge is technical interoperability amid political fragmentation: differing laboratory standards, genetic marker systems, and at least five official AU working languages Arabic, English, French, Portuguese, and Spanish, in addition to Swahili's growing continental use across a Union whose membership standing is itself not fixed, requiring AUDSA's technical standards to be resilient to future suspensions, reinstatements, and realignments rather than designed around a static assumption of universal good standing. Sixth, institutional and database fragmentation: as the Nigerian case illustrates, the absence of a single, statutorily empowered forensic investigation agency, combined with non-interoperable financial, immigration, police, and civil-registry databases, prevents even comparatively well-resourced member states from assembling the complete evidentiary and financial trail that counterterrorism and anti-trafficking prosecutions require, meaning AUDSA cannot succeed as a purely continental overlay if the national data foundations beneath it remain disconnected (Sibe & Muller, 2022; Blueprint Newspapers, 2025; Vanguard, 2026). Seventh, foreign technology dependency: much of the digital forensic and surveillance infrastructure currently in use across the continent is licensed from a small number of external suppliers based in Israel, the United States, Russia, and France, whose home-government export-control regimes govern continued access and can suspend or withdraw it unilaterally, leaving client states without independent recourse and undermining the operational continuity on which any continental forensic system depends (Citizen Lab, 2020; Estrin, 2021; Bromley, 2017).

VII. Policy Recommendations

First, the African Union should formally establish an African Union DNA Security Architecture (AUDSA) under the Commission's Peace and Security Department, structured as a two-tier system: full integration for member states in good standing, and a parallel technical protocol enabling narrowly scoped humanitarian and counterterrorism data exchange with states currently under suspension, preserving forensic cooperation independent of political membership status. Second, each member state should establish or strengthen a National DNA Forensic Center accredited to ISO/IEC 17025 standards, linked to the continental architecture through its Regional Economic Community and mandated to serve criminal justice, disaster victim identification, migration verification, and counterterrorism functions. Third, the AU should adopt a Continental Legal and Ethical Framework for Forensic Data Protection, modeled on the EU's General Data Protection Regulation and grounded in the Malabo Convention, explicitly governing consent, retention limits, and redress mechanisms, and should prioritize driving Malabo Convention ratification toward universality as a precondition for AUDSA's legal foundation. Fourth, an independent AU Continental Bioethics and Forensic Oversight Committee, including civil society and human rights representation, should be established to prevent the political misuse documented as a central risk in this study. Fifth, AUDSA should be technically integrated with the Continental Early Warning System and, where feasible, with national and REC-level biometric infrastructure such as Nigeria's identity systems, Ghana Card, and Kenya's Huduma Namba, rather than waiting on the AU's own stalled continental e-passport project, converting early warning from a preventive tool into a proactive, evidence-based system. Sixth, given the high cost of forensic infrastructure, the AU should pursue Public-Private Partnerships with biotechnology and digital infrastructure providers under strict data-sovereignty safeguards, alongside sustained capacity-building support from AFRIPOL, ACSRT, INTERPOL, and the United Nations Office on Drugs and Crime. Seventh, each member state should establish or formally empower a dedicated national forensic and digital-evidence investigation agency, analogous to the forensic institutes operated in the United States and the European Union, with statutory authority to set binding forensic and chain-of-custody standards, accredit laboratories, and coordinate across security, financial, and immigration institutions; this agency should be mandated to interoperate with the national identity system so that financial, criminal, immigration, and civil-registry records can be queried against a single verified identity, closing the fragmentation that currently obstructs terrorism-financing prosecutions and routine cross-institutional verification such as national service and prior-employment checks. Eighth, to reduce structural dependence on externally licensed and export-controlled forensic and surveillance platforms, the AU should invest in indigenous digital forensic research and development capacity, negotiate multi-year technology-transfer and local-manufacturing agreements with international partners rather than relying on turnkey procurement, and require that any externally supplied AUDSA-linked system include contractual continuity guarantees against unilateral vendor suspension. Finally, given the demonstrated volatility of the continent's institutional

landscape a suspension cycle that has, within a single decade, touched close to a dozen member states the AU should build political and technical redundancy into AUDSA's governance from inception, ensuring the architecture can absorb further membership changes without collapsing the forensic cooperation it is designed to sustain.

VIII. Conclusion

This study has examined the case for a harmonized African Union DNA Security Architecture at a moment of unusual institutional flux across the continent. The suspension of Burkina Faso, Guinea-Bissau, Madagascar, Mali, Niger, and Sudan from AU activities has not diminished the continent's need for scientific, interoperable identification capacity if anything, it has sharpened it, since the terrorist and trafficking networks that forensic genomics is best positioned to counter operate across precisely the frontiers, from the Sahel to the Horn of Africa to the Great Lakes, that now separate states in good standing from states in transition. The evidence from South Africa's National Forensic DNA Database, Nigeria's National DNA Data Bank, Ghana's forensic modernization, Rwanda's post-genocide identification efforts, and the AU's own stalled continental e-passport collectively demonstrate that the technical and institutional building blocks for a continental forensic architecture already exist in nascent, unevenly distributed form; what remains absent is harmonization, legal safeguarding, and a governance design robust enough to function amid continued political realignment. Properly built with independent ethical oversight, interoperability standards resilient to membership change, and a two-tier architecture that treats technical cooperation as separable from political standing, an African Union DNA Security Architecture would represent a genuine advance from reactive crisis management toward evidence-based, rights-respecting continental peacebuilding a practical, forensic complement to the AU's own Agenda 2063 ambition of silencing the guns across a continent that remains as interconnected as it is, for now, institutionally divided.

References

[1] African Union Commission. (2016, June 13). African Union set to launch e-Passport at July Summit in Rwanda. au.int.

[2] African Union Peace and Security Department. (n.d.). The African Peace and Security Architecture (APSA). African Union.

[3] Amani Africa. (2026, February 27). Informal consultation with member states in political transition. Amani Africa Media and Research Services.

[4] Arieff, A. (2023). Peace and security in West Africa: Prospects and challenges for ECOWAS. Congressional Research Service.

[5] Blueprint Newspapers. (2025, July 30). BVN, NIN sale, a threat to national security. Blueprint Newspapers.

[6] Bredan, C., & Rutten, M. (2021). Forensic DNA databases: Global trends, legal frameworks, and ethical considerations. International Journal of Forensic Science & Policy, 7(4), 211–230.

[7] Bromley, M. (2017). Export controls, human security and cyber-surveillance technology: Examining the proposed changes to the EU dual-use regulation. Stockholm International Peace Research Institute.

[8] Bromley, M. (2020, February 12). A search for common ground: Export controls on surveillance technology and the role of the EU. About:Intel.

[9] Businessday NG. (2026, May 8). You can't build a digital economy on a broken foundation. BusinessDay Nigeria.

[10] Butler, J. M. (2015). Advanced topics in forensic DNA typing: Methodology. Academic Press.

[11] Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers, and the internet (4th ed.). Academic Press.

[12] Citizen Lab. (2020). Running in circles: Uncovering the clients of cyberespionage firm Circles. University of Toronto.

[13] Eboh, C., & Adeoye, J. (2023). Digital forensics and transnational crime prevention in Africa. African Security Review, 32(1), 47–68.

[14] Estrin, D. (2021, July 29). NSO Group blocks some governments from using its spyware over misuse claims. NPR.

[15] Eze, M. (2022). DNA profiling in Nigeria: Challenges and opportunities. Nigerian Journal of Forensic Science, 8(2), 45–67.

[16] Financial Action Task Force. (2013). Terrorist financing in West Africa. FATF.

[17] FurtherAfrica. (2022, July 7). African Passport: A mixed bag of opportunities?

[18] Galtung, J. (1969). Violence, peace, and peace research. Journal of Peace Research, 6(3), 167–191.

[19] Global Terrorism Index. (2025). Global Terrorism Index 2025: Measuring the impact of terrorism. Institute for Economics and Peace.

[20] Grokipedia. (2026, January 14). African Union Passport.

[21] HumAngle. (2026, June 16). Inside Nigeria's tedious paths to harmonised digital identity systems. HumAngle Media.

[22] Ibrahim, H. (2026, May 5). Nigeria's hidden war: Why terror financing prosecutions remain elusive. African Health Report.

[23] INTERPOL. (2021, June 1). INTERPOL unveils new global database to identify missing persons through family DNA. INTERPOL.

[24] Institute for Security Studies. (2023, November 20). Why aren't sanctions preventing coups in Africa? ISS Africa.

[25] Kieh, G. K. (2020). West Africa's regional security complex and ECOWAS conflict management mechanisms. African Studies Quarterly, 19(4), 56–81.

[26] National Human Genome Research Institute. (2023). A brief guide to forensic DNA analysis. National Institutes of Health.

[27] Ngari, A., & Odah, N. (2020). Strengthening forensic capacity for justice and accountability in Africa (Policy Brief No. 135). Institute for Security Studies.

[28] Odo, C. J. (2026). Limitations of digital forensic investigation in Nigeria's rural communities. Emerging Minds Journal for Student Research.

[29] Olabode, T., & Ezenwa, C. (2021). The National DNA Data Bank and criminal justice modernization in Nigeria. Nigerian Journal of Forensic Science, 7(1), 12–29.

[30] Osaghae, E. E. (2022). Nation-building and regional integration in West Africa: ECOWAS in perspective. African Affairs, 121(484), 75–97.

[31] PSC Report. (2023). Sanctions and suspensions not necessarily the solutions. Institute for Security Studies.

[32] Sibe, R. T., & Muller, S. R. (2022). Digital forensic readiness of cybercrime investigating institutions in Nigeria: A case study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force. Annals of Computer Science and Information Systems, 34, 53–57.

[33] UNDP. (1994). Human development report: New dimensions of human security. Oxford University Press.

[34] Vanguard. (2026, July 14). Why Nigeria's national database is still fragmented despite NIMC's claims. Vanguard News.

[35] Voice of Nigeria. (2026, July 16). Nigeria expands digital forensics to boost cybersecurity. Voice of Nigeria.

[36] Wendt, A. (1999). Social theory of international politics. Cambridge University Press.

[37] World Peace Foundation. (2025, March 21). The African Peace & Security Architecture.