FORENSIC SECURITY AND THE LAW IN NIGERIA AS A PANACEA FOR MODERN DEFENCE MECHANISM

By

John Bulus Mahwel*
&
Kyenlong Yeshak Francis**

Abstract:
The sophistication of modern crime in Nigeria has necessitated a transition from traditional investigative techniques to scientifically driven methods. This paper examines forensic security as a viable panacea for modern defence challenges in Nigeria. It analyses the legal framework governing forensic evidence, focusing on statutory provisions and judicial authorities. This paper argues that forensic security, when effectively integrated with Nigeria's legal system, serves as a panacea for modern defence challenges. The study further evaluates the role of forensic science in enhancing criminal justice administration and identifies challenges inhibiting its effectiveness. It concludes that while Nigeria has made significant progress through legislative and judicial recognition of forensic evidence, substantial reforms are required to optimize its utility in modern defence systems. The research is purely doctrinal as primary and secondary sources of relevant materials are consulted with a purpose making recommendations that will help the policy makers in the security and justice sector in Nigeria.
Keywords*:* Forensic, Security, Law, Defence.

---

*. John Bulus Mahwel is a Senior Lecturer in the Department of Commercial and Property Law, Faculty of Law University of Jos. email: mahwelb@unijos.edu.ng

** Kyenlong Yeshak Francis Lecturer Department of Public Law, National Open University of Nigeria, email: kyenlong@noun.edu.ng.

1. Introduction

The nature of crime in Nigeria has evolved significantly, encompassing cybercrime, terrorism, kidnapping, banditry, cultism, ritual killings, communal/ethnoreligious clashes, armed-rubbery, trafficking, money laundering and financial fraud. Traditional investigative methods primarily reliant on confessional statements and eyewitness testimony are increasingly inadequate in addressing these sophisticated crimes. Forensic security, which integrates science with legal processes, provides a reliable and objective basis for criminal investigations and adjudication.[1] The enactment of the Evidence Act 2011 and its amendment of the 2023 marked a turning point in Nigeria's legal landscape by formally recognizing scientific and electronic evidence.

2. Conceptual Framework

2.1 Meaning of Forensic Security

Forensic security is a multidisciplinary concept that integrates principles from forensic science, criminology, law and security studies to enhance the prevention, detection, and adjudication of crimes. The term "forensic" is derived from the Latin word "forensis," meaning "of the forum," signifying its relevance to legal proceedings. Security, on the other hand, refers to the protection of lives, property, and societal order.

Scholars have defined forensic science as the application of scientific methods and techniques to matters under investigation by a court of law.[2] In this regard, forensic security extends beyond mere scientific analysis to include the strategic use of forensic tools in safeguarding national and human security.

Forensic security encompasses several components, including deployment of CCTV camaras, crime scene investigation, forensic intelligence, biometric identification, cyber security and digital forensics. These components collectively contribute to a system where evidence-based approaches are employed in addressing security challenges.

---

1 Forensic Security, available at https://www.forensicscijournal.com/journals/jfsr/jfsr-aid1072.phpf accessed 2nd February, 2026.

2 O Ojo, Principles of Forensic Science (Lagos: Spectrum Books, 2018) 45.

In the Nigerian context, forensic security has become increasingly significant due to the rise in complex crimes such as terrorism, cybercrime, kidnapping, and organized criminal activities. The integration of forensic methodologies into Nigeria's criminal justice system is essential for ensuring accuracy, reliability, and fairness in the administration of justice.

Thus, forensic security can be defined as the application of scientific methods and forensic techniques in security operations to detect, prevent, investigate, and prosecute crimes in a manner consistent with legal standards.

2.2 Theoretical Underpinning

This study is anchored on the Scientific Evidence Theory, which posits that justice is best achieved when decisions are based on empirical and verifiable data rather than conjecture or unreliable testimony. The theoretical foundation of forensic security is rooted in several criminological and legal theories that explain crime causation, detection, and control.

One of the key theories underpinning forensic security is the Rational Choice Theory. This theory posits that individuals commit crimes based on a rational calculation of costs and benefits.[3]The application of forensic security increases the likelihood of detection and punishment, thereby deterring criminal behavior.

Another relevant theory is the Deterrence Theory, which suggests that crime can be prevented when the consequences of criminal acts are certain, swift, and severe.[4] Forensic security enhances deterrence by improving investigative capacity and ensuring that offenders are identified and prosecuted based on credible evidence.

The Routine Activity Theory also provides a useful framework. It posits that crime occurs when a motivated offender, a suitable target, and the absence of capable guardians converge.[5] Forensic security acts as a "capable guardian" by introducing surveillance systems such

---

3 R Clarke, 'Rational Choice Theory and Crime' (1997) 12 Journal of Criminology 23.

4 J Bentham, An Introduction to the Principles of Morals and Legislation (Oxford: Clarendon Press, 1789) 170.

5 L Cohen and M Felson, 'Social Change and Crime Rate Trends: A Routine Activity Approach' (1979) 44 American Sociological Review 588.

as CCTV Camaras, biometric controls, and forensic monitoring mechanisms such as drones.

Furthermore, the Scientific Crime Detection Theory emphasizes the role of empirical and scientific methods in crime investigation. This theory supports the use of forensic tools such as DNA analysis, fingerprint identification, and digital tracking in establishing facts and linking suspects to criminal activities.

From a legal perspective, forensic security is anchored on the principle of proof beyond reasonable doubt, as required in criminal trials.[6] The use of forensic evidence strengthens the probative value of evidence presented before the court and reduces reliance on unreliable testimonial evidence. Therefore, in Nigeria, the application of these theories underscores the need for institutional reforms, capacity building, and investment in forensic infrastructure to enhance national security and justice delivery.

3. Legal Framework for Forensic Evidence in Nigeria

3.1 Evidence Act 2011

The Evidence Act 2011 governs admissibility of forensic evidence, for instance Section 68 which deals with the admissibility of expert opinion evidence, is critical in forensic and electronic evidence because expert witnesses are allowed to give opinions on digital forensics, fingerprints, handwriting analysis, or computer-generated evidence, while lay witnesses are limited to factual testimony.

Sections 68 to 72 of the Evidence Act 2011 govern the use of opinion and expert evidence in Nigerian courts. The law establishes that, as a general rule, witnesses may not give evidence of their personal opinions; they are expected to testify only to facts they have observed. An exception is made for expert witnesses, who are allowed to provide opinions in matters within their professional knowledge, skill, training, or experience. Expert evidence is admissible only when it assists the court in understanding a fact in issue, and the court retains discretion to evaluate and weigh the opinion.

Experts may base their opinions on facts they have personally observed or on information made available to them, even if such facts would not otherwise be admissible as evidence, provided that reliance on such information is standard practice within their field. Experts are

6 Woolmington v DPP [1935] AC 462; Akinfe v State (1988) 3 NWLR (Pt 85) 729 (SC),

under a duty to remain impartial and independent, prioritizing their obligation to assist the court rather than to advocate for the party that engaged them. The courts may reject expert evidence that is biased, unreliable, or beyond the expert's competence, and the weight given to such evidence depends on the expert's qualifications, methodology, and the credibility of the opinion. In essence, these provisions ensure that expert evidence in Nigerian courts is reliable, relevant, and presented in a manner that aids judicial understanding, while protecting against unqualified or biased opinions influencing the outcome of proceedings.

Similarly, Section 84 deals with the admissibility of forensic evidence in form computer-generated or electronic evidence. Together, these provisions provide a legal framework for handling specialized evidence in Nigerian courts, whether arising from expert analysis or modern technology.

The law establishes that witnesses may not give evidence of their personal opinions, except where they are qualified as experts. Expert witnesses are permitted to provide opinions in matters within their professional knowledge, skill, training, or experience, and such opinions are admissible only if they assist the court in understanding a fact in issue. Experts may rely on facts personally observed or made known to them, even if those facts would not otherwise be admissible, as long as it is standard practice in their field. Experts are under a duty to remain impartial and independent, with the court evaluating the reliability, methodology, and relevance of their opinions.

Section 84 complements these provisions by regulating the admissibility of forensic evidence which is increasingly relied upon in modern litigation. Just as expert evidence requires a foundation to establish reliability, computer-generated evidence must meet specific conditions, including certification of the system or process used to generate the data, to ensure it is authentic and trustworthy. Both Sections 68–72 and 84 emphasize accuracy, reliability, and the court's discretion in weighing specialized evidence.

In practice, the linkage is clear: expert witnesses may offer opinions on technical or forensic matters, including digital evidence, while Section 84 provides the formal mechanism for ensuring that such electronically produced evidence is admissible. This framework ensures that courts can rely on scientific, technical, or digital evidence while protecting against unverified or unreliable information, maintaining both fairness and probative value in proceedings.

3.2 Administration of Criminal Justice Act, 2015

This law enhances criminal procedure in Nigeria by introducing a modernised framework that promotes efficiency, due process, and rights protections within the justice system. Before the Administration of Criminal Justice Act (ACJA), Nigeria's criminal procedure was governed by outdated laws, which contributed to delays, irregular trials, and practices that compromised fairness. The ACJA was enacted to address these challenges by aligning criminal procedure with contemporary standards and principles of justice. The Act provides a clear statutory foundation for investigation and trial processes that minimise procedural abuses, and emphasises procedural safeguards to protect the rights of suspects and defendants, including the presumption of innocence and the right against self-incrimination.[7]

It expressly regulates the recording of confessional statements to prevent unreliable or coerced confessions and integrates technology and electronic recording into investigative and court procedures. These reforms collectively encourage the adoption of modern investigative forensic techniques, reduce undue reliance on confessions obtained without proper safeguards, and create space for the use of scientific, digital, and forensic evidence, thereby strengthening the integrity and fairness of criminal proceedings in Nigeria. [8]

3.3 Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024

The Cybercrimes (Prohibition, Prevention, etc.) (Amendment)Act 2024 is directly linked to forensic security, because it provides the legal foundation for digital and cyber forensic investigations. Forensic security involves the collection, preservation, analysis, and presentation of digital evidence to detect, prevent, and prosecute cybercrime. By recognizing electronic evidence as admissible in court, the Act ensures that data obtained from computers, networks, or other digital devices can be used to establish facts in legal proceedings.

The law empowers law enforcement agencies and forensic experts to investigate cyber offences such as hacking, identity theft, cyberstalking, and financial fraud, all of which require forensic analysis of digital systems and data. It also sets out proper procedures

---

7 Yunus A K, *Ten Years of ACJA: Evaluating the Impact of the Administration of Criminal Justice Act 2015 in Nigeria* (2025). available on SSRN at: https://ssrn.com/abstract=5599215 accessed 1st April,2026.

8 *Ibid*.

for evidence handling, authentication, and chain of custody, which are critical to maintaining the integrity and reliability of forensic evidence.

In essence, the Cybercrimes Act bridges legal frameworks and technical forensic practice, ensuring that modern investigative techniques such as computer forensics, digital data recovery, and cyber incident analysis are conducted within the law. This strengthens forensic security by guaranteeing that digital evidence collected during investigations is credible, admissible, and protected from tampering, thereby supporting both the prosecution and the broader goal of cybercrime prevention.[9]

9 See generally, Sections 39 – Interception of Electronic Communications This section empowers a judge to authorise, on sworn information, the interception, collection, and recording of content data and traffic data from electronic communications for purposes of criminal investigation. This is crucial to cyber forensic investigations because it provides lawful grounds for authorities to obtain and analyse digital communications that may be evidence of offences. Section 45 – Warrants for Electronic Evidence Under this section, a law enforcement officer may apply ex parte for a warrant to obtain electronic evidence. The judge can issue a warrant authorising search, seizure, and use of technology to collect or decode digital data from computers or networks. This is the main statutory basis for cyber forensic investigators to access, seize, and extract data in a way that ensures lawful admissibility in court. Section 53 – Foreign Evidence Assistance Section 53 deals with the admissibility of evidence gathered in foreign investigations when authenticated. It states that authenticated electronic evidence obtained abroad pursuant to the Act is prima facie admissible in Nigeria. This supports cross-border forensic cooperation and the use of digital evidence from foreign systems. Sections 55–56 – Preservation and Mutual Assistance. These sections allow Nigeria to preserve electronic data or electronic devices during investigations, including urgent preservation orders from courts. They also empower the Attorney-General to request preservation or disclosure of such data from service providers or individuals. Maintaining the integrity and chain of custody of forensic evidence is a key part of these provisions.

3.4 Judicial Authorities

Nigerian courts have developed jurisprudence on forensic and electronic evidence in some cases like *Kubor v Dickson*[10]. The case arose from the Bayelsa State Governorship Election of 2012, where the appellant challenged the election of the respondent. In an attempt to prove electoral irregularities, the appellant tendered certain documents, including printouts from online newspapers and materials downloaded from the internet (INEC website). These documents were computer-generated but were presented without complying with the requirements of Section 84 of the Evidence Act 2011, particularly the absence of a certificate identifying the manner of their production.

The Supreme Court held that the electronically generated documents were inadmissible in evidence due to non-compliance with Section 84 of the Evidence Act 2011. The Court emphasized that electronic evidence must be accompanied by a proper certificate and must satisfy the conditions relating to the reliability of the computer used. Consequently, the Court rejected the documents and dismissed the appeal, upholding the election of the respondent. Electronic (computer-generated) evidence is only admissible where the strict requirements of Section 84 of the Evidence Act are complied with. The Supreme Court held that compliance with Section 84 of the Evidence Act is mandatory for admissibility of electronic evidence.

Although certification is a condition precedent, but recently the court in the of *Attorney-General Federation v. Anebunwa*[11] The Supreme Court clarified that not every document typed using a computer qualifies as "computer-generated evidence" within the meaning of Section 84 of the Evidence Act 2011. The Court held that only documents produced through a computer process or system, where the computer itself generates or processes the information, require compliance with Section 84. Accordingly, documents that are merely typed or printed using a computer, without involving any automated or technical process of generation, do not fall within the strict requirements of Section 84. This decision refined the law on electronic evidence in Nigeria by reducing the over-reliance on Section 84 objections. It provides clarity that not all electronically produced documents require certification, thereby simplifying the admissibility of certain categories of evidence.

---

10 (2013) LPELR-20788 (SC)

11 (2022) LPELR-57750 (SC).

However, in *Kehinde Adeniyi Johnson v. Lafarge Africa Plc*[12]. The case involved employment and documentary disputes. One of the parties sought to rely on computer-generated documents (electronic evidence). The opposing counsel objected, arguing that the documents were not in compliance with Section 84 of the Evidence Act 2011. The Court reaffirmed that:
Electronic evidence must satisfy the conditions of Section 84; otherwise, it is inadmissible.

A case cannot be built on inadmissible electronic evidence.
Documents not properly certified or authenticated should be rejected.
This decision shows that Nigerian courts still apply strict compliance with forensic evidence rules when dealing with electronic or computer-generated evidence.

Other judicial decisions on the issue of admissibility of forensic evidence in Nigeria include: *Kubor & Anor v. Dickson & Ors*[13] where the Supreme Court held that computer-generated documents are admissible only upon strict compliance with Section 84 of the Evidence Act 2011, including certification and proof of the reliability of the computer system used. In *Kalu & Anor v. Ohuabunwa & Ors*[14] the Court of Appeal followed *Kubor v Dickson* and upheld that computer-produced data, such as INEC ICT outputs, properly accompanied by a Section 84(4) certificate, was admissible. Similarly, in *Abubakar & Anor v. INEC & Ors*[15] the Court of Appeal held that INEC computer printouts, which are public documents, must be certified and satisfy Section 84 conditions to be admissible. Again, in *FRN v. Ojo & Anor*[16] electronically extracted information by an EFCC forensic officer was held inadmissible for failure to comply with Section 84 and Section 104 requirements. In *Attorney-General of the Federation v. Princewill Ugonna Anuebunwa*[17] The Supreme Court stated in obiter that computerised bank statements must be certified to demonstrate that the source computer was reliable and tamper-

12 NICN, National Industrial Court, 17 February 2026. See also< https://www.nicnadr.gov.ng> accessed 1st April, 2026.

13 (2013) 4 NWLR (Pt. 1345) 534; (2013) LPELR-20788 (SC).

14 2015 LPELR-26016 (CA).

15 2019 LPELR-48488 (CA).

16 2018 LPELR-4554 (CA).

17 2022 LPELR-57750 (SC).

ing-free. Akin to the above, *UBN v. Agbontaen & Anor (2018)*[18] The Court of Appeal held that bank statements generated from computer systems are computer-generated evidence and must comply with Section 84 to be *admissible.* However, in *BUA International Ltd v. SAIMA (Nig.) Ltd*[19] The Court of Appeal held that bank statements are not necessarily computer-generated evidence requiring Section 84 compliance, indicating a judicial evolution in the treatment of electronic evidence. *Dickson v. Sylva & Ors*[20] The Court of Appeal emphasized that failure to meet Section 84 conditions renders electronic evidence inadmissible.

Generally, from these cases, the core principles of Nigerian forensic/electronic evidence jurisprudence are that strict compliance with Section 84 of the Evidence Act is generally required, certification and proof of the reliability of the computer system are essential, bank statements and public electronic documents may be treated as computer-generated evidence, and oral testimony by experts can sometimes satisfy Section 84 conditions.

4. Forensic Security as a Modern Defence Mechanism

4.1 Crime Detection and Prevention

Forensic security technologies such as CCTV[21] surveillance, biometric systems, and advanced monitoring tools play a critical role in proactive crime prevention. These technologies allow law enforcement agencies to identify suspicious behaviour, monitor high-risk areas, and intervene before crimes escalate. Integration of forensic security tools into urban planning and corporate security frameworks enhances situational awareness and enables real-time crime detection, significantly reducing the window of opportunity for offenders.

18 2018 LPELR-44160 (CA).

19 2023 LPELR-59533 (CA).

20 2017 LPELR-41257 (CA).

21 Research shows that CCTV surveillance systems are widely used by security authorities to monitor public spaces, detect unlawful actions, and contribute to crime prevention through proactive live monitoring and recording of events. These systems help operators identify suspicious behaviour in real time and respond to emerging threats, thereby contributing to community safety and reducing opportunities for criminal activity.

Moreover, the ability to record, store, and retrieve digital or visual evidence ensures that investigations are supported by accurate and objective information, which strengthens preventative measures.[22]

4.2 Accuracy in Investigation

The use of scientific and forensic evidence, including DNA profiling, fingerprint analysis, and ballistic examinations, reduces wrongful convictions and strengthens the credibility of criminal investigations. Forensic methods provide a factual and objective basis for identifying suspects, reconstructing events, and corroborating witness testimony. By grounding investigations in empirical evidence rather than solely on confessions or circumstantial evidence, forensic security enhances judicial reliability and public confidence in the legal system. Properly collected and analysed forensic evidence is also less vulnerable to challenge, increasing the likelihood of successful prosecution.[23]

---

22 U.S. Government Accountability Office. Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training and Policies for Civil Liberties; GAO-23-105607. U.S. Government Accountability Office; Washington, DC, USA: 2023. [(accessed on 15 March 2024)]. Available online:
< https://www.gao.gov/products/gao-23-105607 >accessed 2nd April, 2026; see also Kassler W.J., Bowman C.L. Overcoming public health "surveillance": When words matter. Am. J. Public Health. 2023;113:1102–1105. available at https://doi.org/10.2105/ajph.2023.307348

23 The significance of scientific evidence in modern criminal justice
Available at:<
https://thelaw.institute/criminal-justice-administration/scientific-evidence-transform-
ing-criminal-justice/#the-significance-of-scientific-evidence-in-modern-criminal-justice> accessed 2nd April 2026, see also, Tracing the Crime Scene Location, available at
https://thelaw.institute/criminal-justice-administration/scientific-evidence-transforming-criminal-justice/#tracing-the-crime-scene-location accessed 2nd April 2026.

4.3 ***Cybersecurity***

In the digital age, cybercrime poses a significant threat to both individuals and institutions. Digital forensics a key component of forensic security enables the identification, preservation, and analysis of electronic evidence in cases of hacking, identity theft, cyber fraud, and online financial crimes. Cyber forensic investigations help protect financial systems, corporate networks, and personal data from malicious actors. By providing a legal and technical framework for gathering digital evidence, forensic security supports both enforcement and deterrence in the cyber domain.[24]

4.4 National Security

Forensic intelligence contributes significantly to national security by enabling the tracking and disruption of criminal networks, insurgent groups, and terrorist organizations. Through analysis of physical evidence, electronic communications, and financial transactions, forensic security assists in identifying patterns, predicting threats, and coordinating timely interventions. Agencies tasked with counter-terrorism and internal security increasingly rely on forensic techniques to connect seemingly disparate pieces of evidence, strengthen intelligence-led operations, and safeguard the populace from organized criminal activity.[25]

Forensic intelligence contributes significantly to national security by enabling the tracking and disruption of criminal and terrorist networks. Research shows that forensic intelligence supports intelligence-led policing by linking evidence and identifying patterns across multiple incidents. The United Nations Office on Drugs and Crime highlights the importance of forensic science in counter-terrorism, particularly in analysing both physical and digital evidence to dismantle criminal networks. Additionally, studies on organized cybercrime demonstrate that analysis of financial transactions and elec-

---

24 Casey E, *Digital Evidence and Computer Crime*. (Academic Press 2011).. Also see:

Behl A & Behl K, *Cybersecurity and Cyberwar* (Oxford University Press 2017).

25 Rossy Q et al., *Forensic Intelligence: Data, Information and Knowledge in the Investigation of Crime*. (CRC Press 2015).

tronic communications is essential in uncovering hidden links between offenders, thereby enhancing national security operations.[26]

4.5 Judicial Efficiency

Courts increasingly depend on forensic evidence to expedite adjudication and improve the accuracy of judicial decisions. Reliable scientific data and digital records reduce the time required to verify facts and cross-examine witnesses, thereby accelerating trials while ensuring fairness. Expert testimony and authenticated electronic evidence help judges and juries understand complex technical issues, minimize speculation, and base rulings on objective findings. This integration of forensic security into judicial processes enhances the efficiency, transparency, and credibility of the legal system.[27]

5. Challenges of Forensic Security in Nigeria

5.1 Inadequate Infrastructure

A major impediment to the effective implementation of forensic security in Nigeria is the inadequacy of forensic infrastructure. Modern forensic investigation is fundamentally dependent on the availability of well-equipped laboratories, advanced analytical instruments, and sophisticated technological systems capable of processing and interpreting complex scientific data with precision. These facilities are indispensable for conducting critical examinations such as DNA profiling, toxicological analysis, ballistic testing, and digital forensic investigations.[28]

However, the Nigerian criminal justice system continues to grapple with a significant deficit in this regard. There is a conspicuous shortage of functional and fully operational forensic laboratories across the country. Although institutions such as the Nigeria Police Force Forensic Science Laboratory in Lagos and the Lagos State DNA and Forensic Centre exist, their capacity is grossly insufficient

---

26 *ibid*

27 Mason S, *Electronic Evidence* (4th ed.). (Institute of Advanced Legal Studies 2017). Also see: Jackson G & Jones S *The Role of Forensic Science in the Criminal Justice System* (2018).

28 O Nwankwo, 'Challenges of Forensic Investigation in Nigeria' (2021) 7 *African Journal of Criminology* 89.

relative to the country's population and rising crime profile.[29]Where such facilities exist, they are often underfunded, poorly maintained, or lack the requisite modern equipment and technical expertise necessary for effective service delivery. This infrastructural deficiency severely constrains the capacity of law enforcement agencies to conduct timely and accurate investigations.[30]

5.2 Lack of Expertise

Closely related to infrastructural challenges is the shortage of skilled forensic professionals in the country. Forensic science is a highly specialized field requiring expertise in areas such as pathology, toxicology, digital forensics, ballistics, and crime scene investigation. Nigeria currently suffers from a limited pool of trained experts capable of handling the technical demands of modern forensic analysis.[31] Many law enforcement officers lack the necessary training in evidence collection, preservation, and analysis, which may result in errors that compromise the integrity of evidence. Furthermore, opportunities for continuous professional development, specialized training, and international exposure are limited, thereby restricting the growth of forensic expertise. The absence of structured institutional frameworks for training forensic scientists within Nigerian universities and professional bodies also contributes to this gap. As a result, the effectiveness of forensic security is weakened, and the ability of the justice system to rely on scientific evidence is significantly reduced.[32]

5.3 Chain of Custody Issues

Another critical challenge is the poor management of the chain of custody, which is essential to maintaining the integrity of evidence from the point of collection to its presentation in court. In many instances, evidence is improperly handled, inadequately documented, or exposed to contamination due to lack of standard operating procedures and insufficient training of personnel. Breakdowns in the chain

---

29 A Adebayo, 'Forensic Science Development in Nigeria: Challenges and Prospects' (2020) 5 *Nigerian Journal of Criminal Justice* 112.

30 E Eze, 'Administration of Criminal Justice and Forensic Evidence in Nigeria' (2019) 3 *University of Lagos Law Review* 67.

31 n 29

32 *Ibid*.

of custody create opportunities for tampering, loss, or substitution of evidence, thereby raising doubts about its authenticity and reliability[33]. This often leads to the exclusion of such evidence in court or a reduction in its evidential weight. In a legal system where admissibility is closely tied to the credibility of evidence, any flaw in the chain of custody can have serious implications for the outcome of a case. Strengthening protocols for evidence handling and ensuring strict compliance with legal requirements remain essential for improving forensic security in Nigeria.

5.4 Judicial Conservatism

Judicial conservatism also poses a significant obstacle to the advancement of forensic security. While the legal framework in Nigeria increasingly recognizes the importance of scientific and electronic evidence, some courts and legal practitioners remain hesitant to fully embrace these modern methods. There is still a tendency in certain cases to rely heavily on traditional forms of evidence, such as confessional statements and eyewitness testimony, which may be less reliable than scientific evidence.[34] This cautious approach may stem from limited familiarity with forensic science, lack of technical knowledge, or concerns about the authenticity and interpretation of scientific findings. Additionally, inconsistencies in judicial attitudes toward the admissibility of forensic evidence may create uncertainty for investigators and prosecutors.[35] To address this challenge, there is a need for continuous judicial education and capacity building to enhance understanding and confidence in forensic methodologies.

5.5 Funding Constraints

Funding constraints remain a pervasive challenge affecting all aspects of forensic security in Nigeria. The development and maintenance of forensic infrastructure, acquisition of modern equipment, and training of personnel require substantial financial investment. However, budgetary allocations to forensic science and related sectors are often

---

33 *Ibid*.

34 J O Olatunbosun, 'Admissibility of Electronic Evidence in Nigerian Courts' (2016) 10 *Nigerian Judicial Review* 45; A Ayua, 'Modern Trends in Nigerian Evidence Law' (2018) 12 *Journal of Law and Practice* 78.

35 *Ibid*.

inadequate to meet these demands.[36] Limited funding affects not only the establishment of laboratories but also the sustainability of existing facilities, leading to outdated equipment and inefficiencies in operations. Furthermore, insufficient financial resources hinder research and innovation in forensic science, preventing Nigeria from keeping pace with global advancements in the field. Without adequate funding, efforts to strengthen forensic security will remain constrained, and the criminal justice system will continue to face challenges in effectively investigating and prosecuting crimes.

6. Comparative Perspective

A comparative analysis of forensic security across different jurisdictions shows that countries such as the United Kingdom and the United States have fully institutionalized forensic science as a central pillar of criminal justice and national security systems. However, emerging and conflict-affected states such as Israel, Russia, Iran, and Ukraine demonstrate how forensic security is increasingly integrated into military intelligence, cyber warfare, and national defence strategies.[37] In the United Kingdom and the United States, forensic security operates within structured legal and institutional frameworks, where scientific evidence is routinely used in criminal investigations and court proceedings. These countries maintain advanced forensic laboratories, national DNA databases, and strict evidentiary standards, ensuring that forensic evidence is accurate, reliable, and admissible. Forensic security in these jurisdictions supports not only investigation and prosecution but also crime prevention and intelligence-led policing, making it a proactive tool in maintaining public safety.[38]

In contrast, Israel represents a model where forensic security is deeply integrated into both criminal justice and national security op-

---

36 *Ibid*.

37 C McCartney, 'Forensic Science and the Criminal Justice System' (2011) 15 *International Journal of Evidence & Proof* 1; P Roberts and A Zuckerman, *Criminal Evidence* (2nd edn, OUP 2010) 23; M Williams, 'Forensic Science in International Security Contexts' (2019) 8 *Global Security Review* 66.

38 P Roberts and A Zuckerman, *Criminal Evidence* (2nd edn, OUP 2010) 75; Federal Bureau of Investigation, 'CODIS and National DNA Index System' (FBI Publication, 2020); UK Forensic Science Regulator, *Codes of Practice and Conduct* (2021); Daubert v Merrell Dow Pharmaceuticals 509 US 579 (1993).

erations. Institutions such as the Abu Kabir Forensic Institute play a central role in identifying victims of crimes and terrorist attacks, as well as conducting forensic medical and biological analyses. In addition, Israel is a global leader in digital forensics and cybersecurity, with private companies such as Cellebrite providing advanced tools for extracting and analysing electronic evidence. This demonstrates how forensic security can extend beyond traditional policing into cyber intelligence and counter-terrorism, making it a key component of national defence.[39]

Similarly, Ukraine has increasingly relied on forensic security in the context of armed conflict. Ukrainian forensic institutions conduct extensive analyses of weapons, drones, and digital data to trace the origin of military equipment and establish accountability in conflict-related crimes. These forensic efforts are not limited to criminal prosecution but are also used for intelligence gathering, war documentation, and international legal proceedings, illustrating the expanding role of forensic security in modern warfare. Furthermore, Ukraine has invested in the digitalisation of forensic systems and court processes, enhancing efficiency and coordination between investigative and judicial bodies.[40]

In the case of Russia, forensic security is closely tied to state security operations. Institutions such as the FSB Criminalistics Institute have been involved in investigating major incidents, including terrorist attacks and national emergencies. This reflects a model where forensic science is integrated into state intelligence and security apparatus, supporting both criminal investigations and national defence

39 Abu Kabir Forensic Institute, 'Annual Report on Forensic Services' (2019); D Fisher, 'Forensic Medicine and National Security in Israel' (2018) 12 *Journal of Forensic Sciences* 210; Cellebrite, 'Digital Intelligence Solutions Overview' (2022); E Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 98.

40 International Criminal Court, 'Guidelines on Evidence Collection in Armed Conflict' (2020); O Danchuk, 'Forensic Investigations in Ukraine Conflict Zones' (2022) 6 *Eastern European Law Review* 134; Council of Europe, 'Digitalisation of Justice Systems in Ukraine' (2021).

objectives.[41] However, the centralized and often secretive nature of such systems may raise concerns about transparency and accountability.

Iran also demonstrates the evolving role of forensic security, particularly in the domain of cybersecurity and intelligence operations. Recent developments show that cyber activities including the exploitation of surveillance systems and digital infrastructure are increasingly used for intelligence gathering and military purposes.[42] This highlights the importance of digital forensics in both defensive and offensive cyber strategies, reinforcing the idea that forensic security is now a critical element of modern cyber warfare and national security. From a comparative perspective, these countries illustrate different models of forensic security:

The UK and USA model emphasizes legal standards, institutional independence, and scientific reliability.

The Israel model combines forensic science with advanced cybersecurity and counter-terrorism strategies.

The Ukraine model demonstrates the role of forensic security in conflict analysis, war crimes investigation, and digital transformation. The Russia and Iran model highlights the integration of forensic science into state security and intelligence operations.

General Recommendations for Strengthening Forensic Security in Nigeria

Invest in forensic infrastructure by establishing and upgrading modern laboratories for DNA, digital, fingerprint, and ballistic analysis. Develop national forensic databases, including DNA and biometric systems, to enhance identification and crime tracking.

Strengthen human capacity through specialized training, university programmes, and continuous professional development in forensic science.

Enhance legal and regulatory frameworks by creating clear guidelines and possibly an independent forensic regulatory body for standardization and accreditation.

---

41 A Soldatov and I Borogan, *The New Nobility: The Restoration of Russia's Security State* (PublicAffairs 2010) 121; M Galeotti, 'Russian Security and Intelligence Operations' (2019) 5 *Journal of Intelligence Studies* 44.

42 S Afshar, 'Digital Forensics and Cyber Intelligence in Iran' (2021) 9 *Middle East Security Journal* 88; E Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 210.

Improve chain of custody procedures by adopting standardized protocols and digital tracking systems for handling evidence.
Promote judicial education to increase acceptance and proper evaluation of forensic and electronic evidence in courts.
Integrate forensic science into national security strategies, including counter-terrorism, intelligence gathering, and cybersecurity operations. Increase funding and budgetary allocation for forensic science, technology, research, and institutional development.
Encourage inter-agency collaboration among law enforcement, security agencies, and forensic institutions for effective information sharing. Adopt international best practices and strengthen global cooperation to address transnational and cyber-related crimes.

8. Conclusion

In conclusion, forensic security has emerged as a critical component of modern criminal justice, national security, and cybersecurity systems worldwide. In Nigeria, while statutory frameworks such as the Evidence Act 2011, the Administration of Criminal Justice Act 2015, and the Cybercrimes Act provide a legal basis for the use of scientific and electronic evidence, practical challenges including inadequate infrastructure, shortage of skilled personnel, poor chain of custody management, judicial conservatism, and limited funding—continue to hinder its full potential.

Comparative perspectives from countries such as the United Kingdom, the United States, Israel, Ukraine, Russia, and Iran highlight the value of integrating forensic science into both criminal investigations and broader national security strategies. These jurisdictions demonstrate that forensic security is most effective when supported by modern laboratories, standardized procedures, professional expertise, national databases, and legal and institutional frameworks.
For Nigeria to strengthen its forensic security system, it must adopt a holistic approach that addresses infrastructural deficits, human capacity development, legal and regulatory reforms, and technological advancement, while fostering inter-agency collaboration and international cooperation. Properly implemented, forensic security can enhance the accuracy, efficiency, and credibility of investigations and adjudication, strengthen public trust in the justice system, and serve as a robust tool for crime prevention, intelligence gathering, and national security.

Ultimately, the development of a modern, reliable, and proactive forensic security system is not only a legal and technical necessity but also a strategic imperative for advancing justice, safeguarding citi-

zens, and promoting national stability in Nigeria. For instance, that attack that happened at Anguwan Rukuba Community, in Jos Plateau State capital on the 29th of March 2026, and other attacks in other parts of Nigeria would have been prevented or the attackers would have been arrested or identify using forensic gargets. Forensic security is indispensable in addressing modern defence challenges in Nigeria. While statutory provisions and judicial decisions have laid a foundation, significant improvements are required in infrastructure, expertise, and legal reforms. If properly implemented, forensic security will not only enhance criminal justice administration but also serve as a sustainable solution to Nigeria's evolving security challenges.