The Role of Forensic Psychologists in Combating Cybercrime and Terrorism in Nigeria: Psychological Approaches to Crime Investigation

Enoch Daniel PhD[1]
Nigeria Security and Civil Defense
Corps National Headquarters Sauka Abuja.
enochdaniel631@gmail.com.
07063193242

Ungwa Emmanuel Vandekan PhD[2]; Yange Bemgba Alfred PhD[3]
General Studies Department,
Federal Polytechnic Wannune, Benue State-Nigeria
drungwa@fedpolywannune.edu.ng
07070514559 & 07036494463

https://doi.org/10.56201/ijssmr.vol.12no10.2026.pg105.114

Abstract
Cybercrime and terrorism have become complex security and justice challenges in Nigeria because offenders increasingly exploit digital technologies, social networks, anonymity, psychological manipulation and transnational connections. Conventional investigation that concentrates primarily on physical evidence and technical attribution may therefore be strengthened by systematic analysis of behaviour, motivation, cognition, interpersonal influence and victim responses. This qualitative study examined the role of forensic psychologists in combating cybercrime and terrorism in Nigeria, with particular attention to psychological approaches to crime investigation. The study adopted a qualitative documentary research design and used thematic analysis of scholarly literature, Nigerian legal and policy documents, and authoritative reports on cybercrime, terrorism, offender profiling and behavioural investigation. The analysis generated three major themes: behavioural profiling and psychological intelligence; psychological interviewing, deception assessment and victim/witness support; and prevention, risk assessment, rehabilitation and multidisciplinary collaboration. Findings indicate that forensic psychologists can contribute to investigative prioritisation by interpreting behavioural patterns, offender motivations, online communications and psychological risk indicators, while avoiding unsupported claims that a profile alone proves guilt. The findings also show that psychological expertise is particularly valuable in understanding social learning, moral disengagement, recruitment and radicalisation processes, and in supporting victims and witnesses. However, institutional limitations, shortage of specialised personnel, concerns about scientific validity, evidential admissibility, privacy and human-rights safeguards can restrict effective application. The study concludes that forensic psychology should be integrated into Nigeria's cybercrime and counter-terrorism architecture as a complementary not substitute discipline. It recommends

specialised training, multidisciplinary investigative units, standardised ethical protocols and stronger research partnerships among universities, security agencies and justice institutions.

Keywords: *forensic psychology, cybercrime, terrorism, offender profiling, psychological assessment, behavioural analysis, Nigeria*

Introduction

The expansion of digital communication, mobile technologies, social networking and online financial services has transformed both legitimate social interaction and criminal opportunity. Cybercrime can be perpetrated across jurisdictions, at high speed and with relatively low physical visibility, while terrorist organisations and violent extremist actors can use digital environments for propaganda, recruitment, mobilisation, fundraising and communication. INTERPOL's African Cyberthreat Assessment Report identifies ransomware, business email compromise, online scams and social engineering as significant and evolving threats in Africa, while stressing the need for stronger law-enforcement capacity and international cooperation (INTERPOL, 2024). Nigeria is particularly important within this environment because its large connected population, extensive digital economy and position within transnational criminal networks create both opportunities for innovation and opportunities for technologically facilitated crime. Nigeria has responded through legal and institutional mechanisms. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, provides the principal statutory framework for preventing and prosecuting a broad range of cyber offences. The Terrorism (Prevention and Prohibition) Act 2022 similarly provides a unified legal and institutional framework for the detection, prevention, prosecution and punishment of terrorism and terrorism financing. The Act also provides for cooperation, information exchange and other mechanisms relevant to counter-terrorism investigations (Federal Republic of Nigeria, 2022). These measures demonstrate the importance of law, technology and intelligence. Nevertheless, the increasing sophistication of offenders means that technical evidence alone may not always explain why an offence occurred, how an offender selected a target, what psychological processes supported persistence, or how a suspect's behavioural patterns relate to the available evidence. Forensic psychology offers a complementary perspective. Broadly, forensic psychology applies psychological knowledge to questions arising in law, criminal investigation and justice. Its contribution can include psychological assessment, behavioural analysis, interviewing, risk assessment, victim and witness support, offender rehabilitation, consultation and expert evidence. In criminal investigation, psychological profiling seeks to organise behavioural information into investigative hypotheses about an unknown offender. Adebisi and Olanrewaju (2021) argue that criminal profiling can help Nigerian investigators integrate psychological principles with crime-scene information, although the field remains less institutionalised in Nigeria than in some other jurisdictions. Contemporary forensic scholarship also emphasises the need for interdisciplinary practice rather than treating profiling as a stand-alone technique. The relevance of forensic psychology becomes even clearer in cybercrime because digital traces are produced by human beings whose choices are influenced by motivation, opportunity, cognition, emotion and social learning. Psychological profiling can help investigators interpret patterns in online communications, victim selection, persistence, escalation, deception and interaction with targets. Digital behavioural analysis has been proposed as a way of integrating behavioural evidence with conventional digital-forensic processes, particularly in interpersonal cybercrime where the interpretation of digital traces depends on understanding human behaviour (Rogers, 2016). The central point is not that psychologists can identify a cybercriminal from

personality characteristics alone, but that psychological expertise can improve the formulation and testing of investigative hypotheses.

Research on Nigerian internet fraudsters illustrates why psychological analysis matters. In a qualitative study of young Nigerian internet fraudsters, Akinloye et al. identified peer influence, community and family support, and cognitive mechanisms such as neutralisation, entitlement, minimisation, rationalisation and dehumanisation in participants' narratives (Akinloye et al., 2022). Such findings suggest that cybercrime is not simply a technical problem. It can be embedded in peer networks, social norms and learned justifications. Understanding these processes can assist prevention and rehabilitation as well as investigation. Social learning theory provides a useful psychological foundation for understanding these patterns. Bandura (1977) proposed that people learn behaviours through observation, imitation and reinforcement, with cognitive processes mediating how environmental experiences influence behaviour. Applied to cybercrime, the theory suggests that individuals may acquire criminal techniques and favourable definitions through interaction with peers, online communities and successful models. Rewards may include money, social status, recognition, excitement or perceived power. Okocha et al. (2022), using a qualitative approach in Nigeria, similarly examined online social-network misuse through social learning theory and identified the importance of learned techniques and online opportunities in cybercrime. The same learning perspective can inform analysis of terrorism and violent extremism, although terrorism cannot be reduced to individual psychological abnormality. Radicalisation is shaped by interacting personal, social, political, economic and contextual factors. The digital environment can amplify exposure to extremist narratives and facilitate contact with recruiters. UNODC reports that the digital space is increasingly exploited for radicalisation and recruitment in Nigeria, especially among young people (UNODC, 2025). Forensic psychologists can therefore contribute by examining behavioural pathways, cognitive justifications, identity processes, susceptibility, group influence and risk indicators while maintaining the distinction between extremist beliefs, lawful expression and behaviour that constitutes a criminal threat.

The psychological approach is also important after an offence has occurred. Cybercrime and terrorism can cause fear, humiliation, financial loss, grief, trauma, distrust and other psychological consequences. Victims and witnesses may be reluctant to disclose information because of shame, intimidation or fear of retaliation. Psychologically informed interviewing can improve rapport and reduce unnecessary contamination of evidence, while victim-sensitive procedures can support cooperation with investigators. In terrorism cases, psychological expertise may additionally support assessment of trauma and rehabilitation needs. A justice system that focuses exclusively on the offender may therefore overlook the psychological needs of victims and the evidential value of their experiences. Despite these possibilities, forensic psychology in Nigeria faces challenges. There are limited numbers of specialists trained specifically in cyber behavioural analysis, counter-terrorism psychology and digital evidence. Investigators may have stronger access to technical specialists than behavioural specialists. There are also risks of overreliance on profiling, stereotyping, confirmation bias and unsupported inferences. A profile should generate testable investigative leads rather than substitute for physical, digital or documentary evidence. Psychological assessment must also respect informed consent where applicable, confidentiality boundaries, procedural fairness and the rights of suspects, victims and witnesses.

The legal environment creates an additional need for professional competence. Evidence used in criminal proceedings must be relevant, reliable and lawfully obtained. Psychological opinions that lack empirical grounding may be challenged. Consequently, the development of forensic psychology in Nigeria should involve clear standards for training, ethical practice, documentation,

peer review and expert testimony. Psychologists should work closely with digital-forensic analysts, police investigators, intelligence officers, prosecutors, social workers and other specialists.

Statement of the Problem

Cybercrime and terrorism in Nigeria create a complex mix of technological, behavioural, legal and security challenges. Offenders operate through anonymous or pseudonymous accounts, use encrypted communication, move across jurisdictions, and exploit legitimate digital services, while also employing social engineering and psychological manipulation to target victims. Terrorist and violent extremist actors exploit the same digital spaces for propaganda, recruitment, coordination and financing. INTERPOL (2024) notes that these digitally enabled threats are evolving rapidly across Africa, and Nigeria's ongoing need for coordinated investigations shows that technical capacity alone is not enough, it must be matched with intelligence and institutional collaboration.

At the core of this is a tendency for investigations to rely heavily on technical attribution while paying less attention to the human behaviour that generates digital evidence. A digital trace does not interpret itself. Without understanding why an offender chose a specific victim, how trust was built, what communication tactics were used, whether behaviour escalated, how networks influenced the act, and what psychological factors sustained it, investigators risk having vast amounts of data but no strong framework for prioritising behavioural leads.

This gap is compounded by the limited institutionalisation of forensic psychology in Nigeria's criminal justice system. Although psychological profiling has recognised investigative value, Adebisi and Olanrewaju (2021) observed that it remains underdeveloped locally. The shortage of specialised forensic psychologists and the weak integration of behavioural specialists into investigative teams reduces the contribution psychology can make to cybercrime and terrorism cases. At the same time, profiling is often misunderstood as a tool for directly identifying offenders from behaviour, when in fact psychological insights are probabilistic and contextual.

Prevention is also affected. Research by Akinloye et al. (2022) links Nigerian cybercrime to peer influence and cognitive justifications that make harmful acts seem acceptable, and similar processes of social influence, identity formation and online exposure drive radicalisation. The problem, therefore, is not just the presence of cybercrime and terrorism. It is the insufficient integration of psychological knowledge into how these offences are investigated, prevented and managed. This study addresses that gap by examining how forensic psychologists can contribute to behavioural profiling, interviewing, risk assessment, victim support, prevention and rehabilitation within Nigeria's legal and institutional context.

Research Objective

The study main objective is to examine the role of forensic psychologists in combating cybercrime and terrorism in Nigeria

Specific Objectives are:

1. To examine how forensic psychologists can use behavioural profiling and psychological intelligence to support the investigation of cybercrime and terrorism in Nigeria.
2. To explore the contribution of forensic psychologists to psychological interviewing, deception assessment, victim/witness support and interpretation of offender behaviour during crime investigation.
3. To examine how forensic psychologists can contribute to prevention, risk assessment, rehabilitation and multidisciplinary responses to cybercrime and terrorism in Nigeria.

Literature Review

Concept of Forensic Psychology

Forensic psychology is concerned with the application of psychological science to legal and justice-related questions. In investigative contexts, its functions can include behavioural consultation, psychological assessment, interviewing, risk assessment, victim support, offender rehabilitation and expert testimony. Eze et al. (2025) describe forensic psychology as an interdisciplinary bridge between psychology and criminal justice, with criminal profiling being one of its important applications. In Nigeria, the discipline is increasingly relevant because investigators confront offences in which behavioural information is dispersed across physical scenes, digital communications and social relationships.

Cybercrime and Psychological Processes

Cybercrime includes offences committed through or against computer systems and networks. Psychological processes are relevant because offenders use persuasion, deception, manipulation, impersonation and social engineering to influence victims. INTERPOL (2024) notes the growing importance of social engineering and online scams in Africa. Nigerian qualitative research also indicates that internet fraudsters can develop pro-criminal cognitions that neutralise moral objections and justify offending (Akinloye et al., 2022).

Terrorism, Radicalisation and Digital Environments

Terrorism involves the use or threat of violence and other prohibited conduct to advance ideological or political objectives. Modern terrorist and violent extremist organisations may use digital platforms for communication, recruitment and propaganda. UNODC (2025) highlights the increasing exploitation of digital spaces for radicalisation and recruitment in Nigeria. Psychological analysis can help identify behavioural pathways and risk factors without assuming that mental illness or a particular personality type automatically produces terrorism. Context, social networks, grievance, group identity, ideology, opportunity and learning all require consideration.

Theory: Social Learning Theory

This study is anchored on Bandura's Social Learning Theory. The theory holds that behaviour can be acquired through observation, imitation and reinforcement, with cognition influencing whether observed behaviour is reproduced (Bandura, 1977). The theory is relevant to cybercrime because technical criminal skills are frequently learned from peers, online communities, mentors or other models. Behaviour that produces financial rewards, recognition or social status may be reinforced and repeated. Okocha et al. (2022) explicitly applied social learning theory to cybercrime in Nigeria and found that online criminal practices could be understood through learned behaviour and social influence. Social learning theory also provides a useful lens for understanding extremist recruitment. Individuals may observe models who portray violence or extremist participation as meaningful, heroic or justified. Repeated exposure can shape definitions favourable to violence, while peer approval and group belonging can reinforce participation. The theory does not imply that everyone exposed to extremist material becomes radicalised; rather, it provides a framework for examining how behavioural models, reinforcement and cognitive interpretation interact with individual and contextual factors. For forensic psychologists, the theory has practical value. During investigation, psychologists can examine the social sources of criminal learning, patterns of reinforcement, peer relationships, communication strategies and cognitive justifications. During

prevention, they can identify alternative sources of reinforcement and prosocial models. During rehabilitation, they can help offenders challenge pro-criminal beliefs and develop lawful behavioural repertoires. Thus, social learning theory links investigation, prevention and rehabilitation.

Research Design

The study adopted a qualitative research design, specifically qualitative documentary analysis. This design was considered appropriate because the study sought to understand meanings, roles, processes and institutional possibilities rather than estimate prevalence statistically. The unit of analysis was documented evidence concerning forensic psychology, cybercrime, terrorism, offender profiling, behavioural investigation, Nigerian legislation and relevant professional practice.

Sources of Data

Data were obtained from peer-reviewed scholarly publications, authoritative institutional reports and Nigerian legal/policy documents. The documentary corpus included literature on psychological profiling, digital behavioural analysis, Nigerian cybercrime, social learning, terrorism prevention and digital radicalisation. Key legal sources included the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024 and the Terrorism (Prevention and Prohibition) Act 2022. Authoritative material from INTERPOL and UNODC was used to contextualise contemporary cybercrime and terrorism threats.

Selection Procedure

Purposive selection was used. Documents were included when they directly addressed at least one of the following: forensic psychology; behavioural or criminal profiling; cybercrime investigation; terrorism or radicalisation; psychological interviewing; rehabilitation; or Nigerian legal/institutional responses. Preference was given to recent evidence while retaining foundational theoretical work where necessary. Documents without sufficient relevance to the study objectives were excluded.

Data Analysis

The study used thematic analysis. First, documents were repeatedly reviewed to identify statements relevant to the research objectives. Second, initial codes were generated around behavioural profiling, psychological intelligence, interviewing, deception, victim support, social learning, risk assessment, rehabilitation, professional limitations and multidisciplinary cooperation. Third, related codes were grouped into broader themes. Fourth, the themes were compared across scholarly and institutional sources. Finally, the themes were interpreted in relation to Social Learning Theory and the Nigerian legal context.

Results

Theme 1: Behavioural profiling and psychological intelligence

The documentary analysis showed that the strongest potential contribution of forensic psychologists is the systematic interpretation of behavioural evidence. The literature indicates that profiling can organise crime-scene and behavioural information into testable investigative hypotheses. In cybercrime, this may include analysis of communication style, victim selection, persuasion strategies, persistence, escalation, timing and patterns of interaction. Digital

behavioural analysis can complement conventional digital forensics by helping investigators understand what the digital traces may reveal about behaviour (Rogers, 2016).

The evidence also showed that profiling must be treated as an investigative aid rather than proof of identity. Nigerian scholarship identifies profiling as a useful but still underdeveloped component of criminal investigation (Adebisi & Olanrewaju, 2021). The appropriate role of the psychologist is therefore to provide structured behavioural hypotheses, identify inconsistencies, advise on investigative priorities and assist with interpretation of patterns while leaving factual attribution to corroborated evidence.

Theme 2: Psychological interviewing, deception assessment and victim/witness support

The second theme was the importance of psychologically informed interviewing. Crime investigation involves people who may be frightened, ashamed, deceptive, traumatised or uncertain. A forensic psychologist can help investigators understand memory, stress, suggestibility, rapport and communication dynamics. In cybercrime, victims may initially conceal losses or omit information because they fear embarrassment. In terrorism investigations, witnesses and victims may face intimidation or trauma. Psychological expertise can therefore improve the quality and sensitivity of information gathering.

The literature further suggests that psychological analysis can assist in evaluating behavioural indicators of deception, but deception assessment should not be treated as a simple method of identifying liars. Behavioural signs are context-dependent and can be affected by anxiety, trauma, cultural communication patterns and fear. Consequently, psychologists should support structured interviewing and corroboration rather than make categorical judgments based on isolated behaviours.

Theme 3: Prevention, risk assessment, rehabilitation and multidisciplinary response

The third theme concerned prevention and post-offence intervention. Nigerian research indicates that cybercriminal behaviour can be associated with peer influence and pro-criminal cognitions, including rationalisation and neutralisation (Akinloye et al., 2022). Social learning theory therefore suggests that intervention should address the social environments and rewards that sustain offending. Forensic psychologists can contribute to risk assessment, behavioural intervention, rehabilitation planning and evaluation of change. For terrorism, psychological contribution includes assessment of radicalisation pathways, group influence, identity processes and disengagement need. UNODC (2025) notes the role of digital environments in radicalisation and recruitment in Nigeria. The findings support a multidisciplinary model in which psychologists work alongside intelligence, police, military, digital-forensic, legal and social-service professionals. No single discipline can adequately address the technological, social, psychological and legal dimensions of these threats.

Summary of Results

Across the three objectives, the qualitative synthesis indicates that forensic psychology can strengthen Nigerian crime investigation in three interconnected ways: by interpreting behavioural and psychological evidence; by improving human-centred investigative interactions; and by supporting prevention, risk management and rehabilitation. The analysis simultaneously identified important boundaries: psychological profiling is probabilistic, behavioural indicators are not inherently diagnostic of guilt, and psychological assessments must be integrated with corroborating digital, documentary and physical evidence.

Discussion of Findings

The first objective examined the use of behavioural profiling and psychological intelligence in cybercrime and terrorism investigations. The findings indicate that forensic psychologists can add value by converting behavioural information into structured investigative hypotheses. This is consistent with Adebisi and Olanrewaju (2021), who argued that criminal profiling can combine psychological principles with crime-scene analysis to support investigation in Nigeria. The finding also accords with Rogers (2016), whose work on psychological profiling in digital forensics emphasised that behavioural analysis can supplement traditional evidence collection by helping investigators interpret patterns of human activity. However, the finding should not be interpreted as support for deterministic profiling. A profile is not a diagnosis and cannot establish guilt. This limitation is especially important in Nigeria, where institutional capacity and evidential standards must continue to develop. Eze et al. (2025) emphasise the interdisciplinary character of forensic psychology, suggesting that profiling is most useful when connected to broader investigative and legal processes. Thus, psychologists should formulate hypotheses that can be tested against digital evidence, financial records, communications, witness accounts and other independent sources.

The second objective addressed psychological interviewing, deception assessment and victim/witness support. The findings suggest that forensic psychologists can improve investigation by bringing knowledge of memory, communication, trauma, suggestibility and interpersonal dynamics into investigative practice. This is particularly relevant in cybercrime because victims can experience embarrassment or self-blame after being deceived. A psychologically informed approach can encourage fuller disclosure without blaming victims. In terrorism cases, psychological support may help victims and witnesses communicate information while reducing the risk that investigators unintentionally intensify distress. The finding regarding deception assessment requires caution. A person may appear nervous, avoid eye contact or provide inconsistent information for many reasons unrelated to deception. Therefore, psychologists should avoid simplistic behavioural lie-detection approaches. The strongest contribution is likely to come from structured interviewing, corroboration and contextual interpretation. This approach protects the integrity of investigations and reduces the danger of confirmation bias. The third objective examined prevention, risk assessment and rehabilitation. The findings are strongly consistent with Nigerian research on internet fraud. Akinloye et al. (2022) found that young internet fraudsters described peer influence and cognitive mechanisms such as neutralisation, entitlement and rationalisation. These findings fit Social Learning Theory because criminal behaviour can be acquired and reinforced within social environments. Okocha et al. (2022) similarly demonstrated the relevance of social learning to online criminal behaviour in Nigeria. The implication is that enforcement should be complemented by interventions that disrupt harmful learning environments and strengthen prosocial alternatives. The findings also have relevance to terrorism. UNODC (2025) reports that digital spaces are increasingly exploited for radicalisation and recruitment in Nigeria. Social learning theory helps explain how repeated exposure to behavioural models and reinforcement within social groups may influence attitudes and conduct. Nevertheless, terrorism is multidimensional and cannot be explained by psychology alone. A responsible forensic psychological approach should therefore examine individual, interpersonal and contextual factors without equating political or religious belief with criminality.

Conclusion

Cybercrime and terrorism in Nigeria are not only technological and security challenges but also complex behavioural and psychological phenomena influenced by social, economic and institutional conditions. This study concludes that forensic psychologists can make valuable contributions to combating these threats through behavioural profiling, psychological intelligence, investigative interviewing, victim and witness support, risk assessment and rehabilitation. Behavioural profiling can assist investigators in identifying patterns and generating investigative hypotheses, provided that profiles are treated as complementary tools and supported by independent evidence. Forensic psychologists can also improve investigative interviewing by helping investigators understand trauma, fear, memory, suggestibility and behavioural responses among victims, witnesses and suspects. Deception assessment should, however, be approached cautiously and supported by corroborating evidence. The study further concludes that psychological interventions can contribute to prevention and rehabilitation by addressing pro-criminal beliefs, peer influence, harmful online environments and radicalisation pathways. Nigeria therefore requires stronger collaboration among forensic psychologists, law-enforcement agencies, digital-forensic experts, intelligence organisations and legal institutions. Such multidisciplinary integration can promote more evidence-based investigation, prevention, rehabilitation and public protection.

Recommendations

Based on the findings, the following recommendations are made:

1. Nigerian law-enforcement, intelligence and counter-terrorism agencies should establish or strengthen multidisciplinary behavioural-analysis units involving qualified forensic psychologists, digital-forensic experts and investigators. Relevant personnel should receive specialised training in cyber behavioural analysis, offender profiling, risk assessment and interpretation of digital behavioural evidence. Psychological profiles should be treated as investigative hypotheses and corroborated with independent digital, physical, financial or documentary evidence to minimise stereotyping, confirmation bias and wrongful suspicion.
2. Investigative agencies should integrate forensic psychologists into the planning and conduct of complex cybercrime and terrorism interviews, particularly where victims and witnesses experience trauma, fear, shame or intimidation. Investigators should receive evidence-based training on memory, rapport, trauma-informed interviewing, suggestibility and the limitations of behavioural deception indicators. Appropriate psychological assessment, support and referral mechanisms should also be provided to protect victims and witnesses while preserving the reliability and evidential value of their accounts.
3. Forensic psychologists should be incorporated into evidence-based prevention, risk assessment and rehabilitation programmes addressing pro-criminal beliefs, peer influence, moral disengagement, harmful online environments and radicalisation. Universities, law-enforcement agencies, technology organisations and justice institutions should establish collaborative research and intervention programmes that generate Nigerian evidence on cybercrime, online radicalisation, behavioural risk and rehabilitation while ensuring that lawful beliefs or expressions are not wrongly interpreted as evidence of terrorism.

References

Adebisi, K. S., & Olanrewaju, D. N. (2021). Psychological profiling of criminals in violent crime investigations in Nigerian criminal justice system. International Journal of Criminology and Sociology, 10, 208–218. https://doi.org/10.6000/1929-4409.2021.10.25

Akinloye, A. A. (2022). How do internet fraudsters think? A qualitative examination of pro-criminal attitudes and cognitions among internet fraudsters in Nigeria. The Journal of Forensic Psychiatry & Psychology, 33(3). https://doi.org/10.1080/14789949.2022.2051583

Bandura, A. (1977). Social learning theory. Prentice-Hall.

Eze, S. M., Alabi, K. J., Ibrahim, S. O., Yusuf, A. O., Hamzat, F. O., Abdulrauf, A., Atoyebi, A. T., Lawal, I. A., Ibrahim, O. A., Imam-Fulani, A. Y., & Dare, B. J. (2025). Forensic psychology and criminal profiling. Journal of Forensic Science Research, 9(1), 92–96. https://doi.org/10.29328/journal.jfsr.1001085

Federal Republic of Nigeria. (2022). Terrorism (Prevention and Prohibition) Act, 2022 (Act No. 15). Federal Government Printer.

Federal Republic of Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended in 2024. Office of the National Security Adviser.

INTERPOL. (2024). African cyberthreat assessment report 2024. International Criminal Police Organization.

Okocha, D. O., Esther, O., & Agaku, T. (2022). Online social networks misuse, cyber-crimes and counter-mechanisms in Nigeria. Journal of Communication and Media Studies, 28, 62–78.

Rogers, M. K. (2016). Psychological profiling as an investigative tool for digital forensics. In Digital forensics: Threatscape and best practices (pp. 45–58). Elsevier. https://doi.org/10.1016/B978-0-12-804526-8.00003-4

United Nations Office on Drugs and Crime. (2025). Country programme for Nigeria 2024–2028. United Nations Office on Drugs and Crime.