FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 24, December, 2026, pp 72 – 78
DOI: https://doi.org/10.33003/fjs-2026-1024-6610

Investigating the Effects of Cybercrime on Money Laundering and Terrorism Financing in Nigeria

***[1,2]Victor U. Akuboh, Lasisi A. Monsuru, Oliver O. Aniebonam, Saifulahi S. Shitu, Amina Adebola, Catherine A. Abimuku, Badamasi A. Musa, Cecilia Ogheneovo and Ejima U. Innocent**

Department of Cyber Security, Nigerian Defence Academy, Kaduna State, Nigeria.

*Corresponding authors' email: vuakuboh@nda.edu.ng

Received: 23 Nov. 2026
Accepted: 24 Nov. 2026
Published: 25 Nov. 2026

ABSTRACT
The rapid expansion of internet connectivity in West Africa has increased opportunities for cybercrime, which can generate illicit proceeds that may subsequently enter money-laundering circuits or support terrorism financing. This study examines the relationship between cybercrime, money laundering and terrorism financing in Nigeria within the broader West African context. The investigation relies on secondary data and a doctrinal review of legal frameworks. It draws on publicly available reports issued by the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), the Nigerian Financial Intelligence Unit (NFIU), the United Nations Office on Drugs and Crime (UNODC) and related bodies, together with a purposive selection of 52 case typologies previously identified in those institutional sources. Regional evidence indicates that advance fee fraud accounts for approximately 40 per cent of documented cyber-enabled cases, while Nigerian assessments for 2025 highlight the prominence of romance scams and investment fraud. Institutional materials also describe multi-phase digital funding patterns associated with certain terrorist groups and point to vulnerabilities linked to virtual-asset service providers, weak know-your-customer controls and identity-masking practices. The national response is constrained by limited inter-agency interoperability. Because the analysis is based on secondary sources, it cannot independently quantify the share of terrorist funds derived from cybercrime; the findings therefore remain descriptive and risk-oriented rather than causal. Policy implications centre on improved intelligence sharing, strengthened asset recovery and clearer regulatory oversight of digital financial channels.

Keywords: Cybercrime, Money Laundering, Terrorism Financing, Virtual Assets, Nigeria, West Africa

INTRODUCTION

The rapid expansion of information and communication technology (ICT) across West Africa has transformed the conduct of commercial, governmental and social activities. While this digital transformation has generated substantial economic opportunities, it has simultaneously enlarged the attack surface available to criminal networks. Cyber-dependent and cyber-enabled offences now constitute a recognised threat to economic stability and national security in the sub-region, and particularly in Nigeria, which functions as both a major financial hub and a high-volume jurisdiction for certain forms of online fraud (United Nations Office on Drugs and Crime [UNODC], 2025; Inter-Governmental Action Group against Money Laundering in West Africa [GIABA], 2010).

A growing body of institutional and academic literature observes that cybercrime frequently operates as a predicate offence. The illicit proceeds generated through online fraud may subsequently be introduced into formal or informal financial systems through money-laundering (ML) processes, and in some instances may be redirected toward terrorism financing (TF) (Suchi & Wika, 2021). This potential continuum is facilitated by the anonymity and speed of digital channels, by the large informal and predominantly cash-based segment of West African economies estimated at 60–70 per cent of regional GDP and by uneven regulatory oversight of emerging financial technologies (GIABA, 2010).

Regional typology assessments have long identified advance fee fraud, commonly known as "419" schemes, as a leading category of cyber-enabled crime (GIABA, 2022b, 2023). More recent Nigerian reporting for 2025 has drawn attention to the prominence of romance scams and investment fraud within the cases examined by the Nigerian Financial Intelligence Unit (NFIU, 2025). Concurrently, terrorist organisations such as Boko Haram and the Islamic State West Africa Province (ISWAP) have been observed employing digital platforms for propaganda, recruitment and the movement of funds (NFIU, 2025; Suchi & Wika, 2021).

Nigeria has responded with a formal legal architecture that includes the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (as amended in 2024) and the Money Laundering (Prevention and Prohibition) Act 2022, together with the designation of the NFIU as an autonomous financial intelligence unit. Nevertheless, institutional assessments continue to highlight practical constraints, notably limited inter-agency coordination, incomplete technical capacity for blockchain and virtual-asset analysis, and a tendency toward fragmented case management (UNODC, 2025; Alabi et al., 2025). A further and persistent analytical difficulty is the scarcity of reliable quantitative evidence that would allow researchers to determine the precise share of terrorist operational funds that originates specifically from cybercrime proceeds a linkage that earlier literature has characterised as a "mysterious link" (Suchi & Wika, 2021).

This study aims to examine the relationship between cybercrime, money laundering and terrorism financing in Nigeria within the West African context, with particular emphasis on emerging digital financial vulnerabilities and the effectiveness of institutional and regulatory responses.

Literature Review

The literature on cyber-facilitated financial crime in West Africa has evolved considerably over the past decade and a half. Early regional assessments concentrated on traditional social-engineering schemes, especially advance fee fraud and identity theft, and treated these offences primarily as sources of illicit funds that could be absorbed into the informal cash economy (GIABA, 2010). Subsequent institutional reporting has documented a progressive increase in organisational sophistication, including the rise of business-email compromise (BEC), large-scale investment scams and romance fraud (NFIU, 2025; UNODC, 2025). In the Nigerian popular and official discourse, networks popularly labelled "Yahoo boys" have been described as moving from relatively simple deception into more serious criminal enterprises, including kidnapping and the laundering of proceeds on behalf of politically exposed persons (The Nation, 2024).

A second strand of literature addresses the methods used to launder the proceeds of cybercrime. Historical analyses emphasised the absorptive capacity of West Africa's extensive informal economy (GIABA, 2010). More recent work highlights the exploitation of virtual-asset service providers (VASPs), chain-hopping across blockchains, privacy-focused cryptocurrencies such as Monero, and the use of corporate or shell-company accounts that appear more legitimate to financial institutions (Søgaard Clausen, 2024; U.S. Department of the Treasury, 2026; Institute for Financial Integrity, 2023; Alabi et al., 2025). These developments expand the digital attack surface and complicate conventional audit trails, yet quantitative measurement of the volumes involved remains limited.

A third and still underdeveloped strand concerns the relationship between cybercrime and terrorism financing. Early GIABA assessments treated money laundering and terrorism financing as analytically distinct processes: the former seeks to legitimise criminal proceeds, whereas the latter may reverse this logic by channelling both licit and illicit funds toward violent ends (GIABA, 2010). Contemporary institutional reporting, however, points to a degree of practical convergence. Terrorist facilitators have been observed employing encrypted messaging applications, structured crowdfunding campaigns, and identity-masking practices such as gender-based proxy accounts and disconnected SIM–Bank Verification Number (BVN) linkages (NFIU, 2025; Suchi & Wika, 2021). Despite these qualitative observations, reliable quantitative evidence establishing the volume of terrorist funds derived specifically from cybercrime remains scarce (GIABA, 2022a; Suchi & Wika, 2021).

Institutional and legal scholarship has documented Nigeria's formal response in some detail. The Cybercrimes Act 2015 (amended 2024) and the Money Laundering (Prevention and Prohibition) Act 2022 provide the principal statutory foundations (UNODC, 2025; Alabi et al., 2025). At the same time, repeated assessments identify a siloed organisational model characterised by limited data interoperability among the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force National Cybercrime Centre (NPF-NCCC) and other agencies as a principal constraint on operational effectiveness (UNODC, 2025). The Egmont Group (2025) has likewise underscored the importance of robust information-sharing mechanisms among financial intelligence units as a prerequisite for disrupting cross-border illicit flows.

Taken together, the existing literature establishes that cyber-enabled fraud is a material source of illicit proceeds, which digital financial channels introduce new layering opportunities, and that terrorist facilitators have adapted certain digital techniques. It also reveals three persistent gaps: the absence of granular quantitative estimates of cybercrime-derived terrorist finance; limited empirical detail on the exploitation of tiered fintech accounts and related identity-masking practices; and insufficient evaluation of the practical effectiveness of inter-agency coordination mechanisms. The present study addresses these gaps through a systematic secondary-data synthesis rather than through primary fieldwork.

MATERIALS AND METHODS

This section sets out the research design, data sources, sampling procedure, analytical procedures and ethical considerations that guided the study. Because the investigation relies entirely on secondary institutional materials and doctrinal analysis of legislation, the design is best characterised as structured documentary research rather than classical mixed-methods triangulation.

Research Design

The study adopts a multi-phase documentary research design. The design proceeds from the formulation of the research problem, through the identification and screening of institutional sources, the purposive selection and classification of case typologies, the extraction and coding of quantitative and qualitative evidence, thematic synthesis, and finally the formulation of risk-oriented interpretations and policy recommendations. Figure 1 presents the overall process in schematic form.



Figure 1: Research design and analytical process (authors' construction)

Phase 1 established the conceptual boundaries of the inquiry and confirmed that the study would rely exclusively on publicly available secondary sources. Phase 2 involved the systematic identification of institutional reports, typology studies, risk assessments and academic publications relevant to cybercrime, money laundering and terrorism financing in West Africa and Nigeria. Phase 3 applied purposive sampling criteria to retain 52 case typologies previously documented in those sources. Phase 4 extracted quantitative indicators (percentages, risk ratings, reporting volumes) and qualitative descriptions of techniques and institutional constraints. Phase 5 organised the extracted material thematically and compared regional and Nigerian evidence. Phase 6 interpreted the findings in light of prior literature, acknowledged methodological limitations, and formulated recommendations and suggestions for future research.

Data Sources

The principal data sources are publicly disseminated institutional reports and open-access academic publications. They comprise the following categories: (a) Regional typology and annual reports issued by the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA, 2010, 2022a, 2022b, 2023); (b) Annual report compendia, National Inherent Risk Assessment materials and related analytical products of the Nigerian Financial Intelligence Unit (NFIU, 2022, 2025); (c) Country assessments and thematic studies published by the United Nations Office on Drugs and Crime (UNODC, 2025); (d) Guidance and annual reporting of the Egmont Group of Financial Intelligence Units (Egmont Group, 2025); (e) Selected publications of the Institute for Financial Integrity (2023) and the U.S. Department of the Treasury (2026) addressing cyber-enabled fraud and virtual-asset risks; (f) Peer-reviewed and thesis literature on cybercrime, money laundering and terrorism financing in the Nigerian and West African contexts (Suchi & Wika, 2021; Søgaard Clausen, 2024; Alabi et al., 2025); (g) Nigerian legislative instruments, principally the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (as amended 2024) and the Money Laundering (Prevention and Prohibition) Act 2022, examined for doctrinal content; (h) Contemporary media reporting that provides contextual illustration of official statements (The Nation, 2024).

Documents were retrieved from official institutional websites and recognised open-access repositories between late 2024 and early 2026. Inclusion criteria required that a document address cyber-enabled financial crime, money laundering or terrorism financing in West Africa or Nigeria and contain either quantitative indicators or sufficiently detailed case typologies to permit thematic coding. Documents limited to pure technical cybersecurity without a financial-crime dimension were excluded.

The 52 Case Typologies: Identification, Selection, Classification and Composition

A central element of the empirical base is a purposive sample of 52 case typologies. These cases were not independently investigated by the authors; they were previously identified, summarised and, in many instances, already classified by the institutional sources listed above, principally GIABA typology reports and NFIU analytical products. The figure of 52 represents the aggregate of distinct typologies and illustrative cases that met the inclusion criteria after screening.

Identification proceeded by systematic reading of the GIABA typology volumes (especially GIABA, 2022b and 2023) and the NFIU report compendia (NFIU, 2022, 2025). Every distinct scheme or illustrative narrative that described a cyber-enabled method of generating or moving illicit funds was logged in a working matrix that recorded the source document, year, brief description, and any quantitative indicators supplied by the source. Selection applied three filters: (1) the case had to involve a digital or cyber-enabled component; (2) it had to have a discernible link actual or potential to money laundering or terrorism financing; and (3) sufficient descriptive detail had to be available to permit thematic coding. Cases that were purely technical (for example, malware descriptions without financial outcomes) or that lacked any financial-crime dimension were excluded. After de-duplication across overlapping institutional sources, 52 cases remained.

The exact composition of the 52 cases, classified into seven thematic categories that reflect the principal typologies reported in the source materials, is as follows: (1) advance fee fraud, including classic "419" schemes — 18 cases; (2) mobile-money-related fraud — 8 cases; (3) Ponzi and investment schemes — 7 cases; (4) hacking and system defrauding — 4 cases; (5) business-email compromise and related email fraud — 4 cases; (6) romance scams and related social-engineering fraud — 6 cases; and (7) residual or hybrid categories (card fraud, sextortion, and cases with an explicit terrorism-financing dimension) — 5 cases. These counts sum to 52. Approximately 50 of the 52 cases underpin the regional prevalence distribution presented in Section 4; the remaining cases supply additional qualitative illustration of techniques and institutional responses. The Nigerian-specific distribution reported by the NFIU for 2025 is treated as a separate evidence stream and is not merged arithmetically with the regional percentages derived from the 52-case set.

Sampling Procedure

The sampling strategy is purposive rather than probabilistic. Purposive sampling is appropriate for documentary research that seeks to capture the range of documented typologies and institutional assessments rather than to estimate population parameters. The sampling frame consisted of all publicly available GIABA and NFIU reports and related institutional assessments that address cyber-enabled financial crime in the period 2010–2025. Within that frame, every case typology that satisfied the inclusion criteria was retained. No random sampling or statistical power calculation was undertaken, because the objective was comprehensive coverage of the documented typology space rather than inferential generalisation.

Analytical Procedures

Analysis proceeded in two parallel streams. Quantitative indicators percentages of case types, sectoral vulnerability ratings on the 0.00–1.00 National Inherent Risk Assessment scale, reporting volumes (currency transaction reports, suspicious transaction reports), and published loss estimates—were extracted exactly as published by the source institutions and are reported without independent recalculation. Where regional and Nigerian percentages appear in the same section, they are clearly labelled as deriving from different exercises, different reporting periods and different case populations, and are not treated as directly comparable.

Qualitative material was coded thematically. Coding categories were derived from the classic money-laundering framework (placement, layering, integration) and from recurrent institutional descriptions of identity-masking practices, digital funding sequences, and inter-agency coordination constraints. Extracted themes were then synthesised and compared with the findings of prior academic and institutional literature. The four-phase digital funding sequence associated with certain terrorist facilitators is presented as an adaptation of existing NFIU descriptive material rather than as an independently validated causal model.

Ethical Considerations

Because the study relies exclusively on publicly disseminated institutional reports and open-access publications, no confidential operational files, classified intelligence products or non-public case files were accessed. No interviews, surveys or primary field collection were conducted. Ethical obligations therefore centre on accurate attribution of secondary sources, avoidance of any disclosure that could compromise ongoing investigations, and transparent acknowledgement of the limits of secondary analysis. All quantitative indicators and qualitative descriptions are traced to their institutional origins, and the manuscript does not present secondary findings as primary empirical discoveries.

RESULTS AND DISCUSSION

The findings are organised according to the study's thematic concerns: the distribution of cyber-enabled fraud typologies, digital financial vulnerabilities, observed patterns linking cyber techniques to terrorism financing, and the state of institutional and legal responses. All numerical indicators are drawn from the cited secondary sources. To avoid duplication, quantitative distributions are presented in tabular form only; schematic illustrations are reserved for the research design (Figure 1) and the multi-phase funding sequence (Figure 2).

Cyber-Enabled Fraud Typologies and Illicit Financial Flows

Regional assessments compiled by GIABA indicate that cyber-enabled fraud is a significant contributor to illicit financial flows in West Africa. Across the case typologies examined in those assessments, advance fee fraud accounts for approximately 40 per cent of documented instances, followed by mobile-money-related fraud (15 per cent) and Ponzi schemes (13 per cent) (GIABA, 2022b, 2023). Hacking and system defrauding, together with business-email compromise, each account for approximately 7 per cent, while residual categories (card fraud, sextortion and related schemes) account for the remaining 18 per cent. Table 1 summarises this regional distribution.

Table 1: Prevalence of Cyber-Enabled Fraud Typologies in West Africa

Typology	Prevalence (%)
Advance Fee Fraud (e.g., 419 Scams)	40
Mobile Money Related Fraud	15
Ponzi Schemes	13
Hacking & System Defrauding	7
Email Compromise (BEC)	7
Others (e.g., Card Fraud, Sextortion)	18

Source: Adapted from GIABA (2022b, 2023). Percentages reflect the distribution reported in the source typology assessments. No accompanying figure is presented in order to avoid duplication of the same information.

Within Nigeria, NFIU analysis for the 2025 reporting period assigns a larger share of examined cases to romance scams (50 per cent) and investment fraud (33 per cent), with business-email compromise accounting for 8 per cent and residual categories for the remainder (NFIU, 2025). Table 2 presents these Nigerian figures. Because the regional and

Nigerian percentages derive from different institutional exercises, different reporting periods and different case populations, they are not directly comparable; they are presented separately to illustrate the distinct emphases of the two evidence bases.

Table 2: Composition of Cyber-Enabled Fraud Cases Reported by the NFIU (2025)

Fraud Category	Percentage of Cases (%)
Romance Scams	50
Investment Fraud	33
Business Email Compromise (BEC)	8
Other Cyber-enabled Crimes	7
Child Sexual Abuse Material (CSAM)	2

Source: NFIU (2025). Figures reflect the distribution of cases analysed by the NFIU in the 2025 reporting cycle. No accompanying figure is presented in order to avoid duplication of the same information.

Institutional estimates of financial impact are substantial. UNODC (2025) cites cumulative Nigerian losses of approximately ₦1.1 trillion between 2017 and 2023 across banking, telecommunications and government sectors, with 2022 losses estimated at roughly USD 500 million. NFIU reporting volumes for 2025 include more than 41 million currency transaction reports and over 42,000 suspicious transaction reports (NFIU, 2025). These magnitudes underscore the scale of the predicate-offence problem. They do not, however, by themselves establish the proportion of proceeds that ultimately enter terrorist financing channels—an attribution that the available secondary sources do not support with reliable quantitative precision.

Digital Financial Vulnerabilities

Nigeria ranks among the highest jurisdictions globally for cryptocurrency adoption. The National Inherent Risk Assessment assigned virtual-asset service providers a vulnerability rating of 0.85 on a 0.00–1.00 scale, placing them in the high-vulnerability category alongside banking and real estate (both rated 0.90) (NFIU, 2022). Table 3 reproduces the published sectoral ratings. The ratings combine assessments of threat and vulnerability; the precise weighting methodology is set out in the original NIRA documentation and is not recalculated here.

Table 3: Sectorial Vulnerability Ratings to Money Laundering and Terrorism Financing

Sector	Vulnerability Rating	Risk Level
Banking Sector	0.90	Very High
Real Estate Sector	0.90	Very High
Virtual Asset Service Providers (VASPs)	0.85	High
Dealers in Precious Stones & Metals	0.85	High
Bureau de Change (BDC)	0.75	High

Source: NFIU (2022, 2025). Ratings follow the National Inherent Risk Assessment scale (0.00–1.00). No accompanying figure is presented in order to avoid duplication of the same information.

Institutional analyses further identify three recurring technical enablers of cyber-facilitated money laundering. First, obfuscation techniques such as chain-hopping (the successive exchange of assets across different blockchains) and the use of privacy-focused coins reduce the transparency of audit trails (Søgaard Clausen, 2024; U.S. Department of the Treasury, 2026). Second, tiered fintech accounts that impose comparatively light know-your-customer requirements facilitate rapid placement and layering of funds (NFIU, 2025). Third, identity-masking practices—including disconnected phone registrations and pre-registered SIM cards designed to break the linkage between SIM cards and Bank Verification Numbers—sever conventional identity trails (NFIU, 2025; Institute for Financial Integrity, 2023). These mechanisms expand opportunities for layering; their quantitative contribution to overall laundering volumes remains unmeasured in the available secondary sources.

Observed Patterns Linking Cyber Techniques to Terrorism Financing

NFIU risk assessments assign ISWAP a "Very High" terrorism-financing threat rating and Boko Haram a "High" rating; other designated groups receive comparable classifications (NFIU, 2022). Table 4 summarises these institutional ratings.

Table 4: Terrorism Financing Inherent Risk Ratings for Designated Groups

Terrorist Organization	Overall Threat Rating
Islamic State West Africa Province (ISWAP)	Very High (VH)
Boko Haram	High (H)
Yan Bindiga / Yan Taadda	High (H)
Indigenous People of Biafra (IPOB)	High (H)

Source: NFIU (2022). Ratings reflect the National Inherent Risk Assessment classifications.

Institutional reporting describes a recurring multi-phase pattern used by certain facilitators: global solicitation via encrypted applications and social media; consolidation into accounts held by intermediaries, often abroad; fragmentation into sub-threshold transfers through international money-transfer operators and local money mules; and final conversion into cash or dual-use goods for field use (NFIU, 2025). Gender-based proxy accounts—accounts opened in the names of women to distance male operatives from visible transactions—are also noted in the same materials. Figure 2

presents this sequence schematically as an adaptation of existing institutional descriptions.

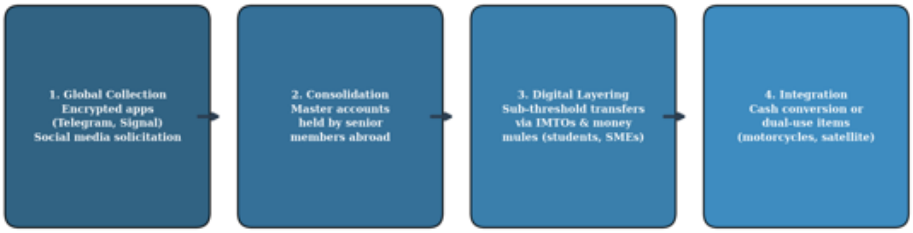


Figure 2: Four-phase cyber-facilitated terrorism financing funding model (adapted from NFIU, 2025)

These descriptions are adapted from existing institutional evidence; they are not independently validated field models. Critically, the secondary sources do not supply a reliable quantitative estimate of the share of terrorist funds that originates specifically from cybercrime, as opposed to kidnapping, taxation of local populations or other sources (GIABA, 2022a; Suchi & Wika, 2021). The observed patterns therefore support a risk-oriented rather than a causal interpretation.

Institutional and Legal Responses

Nigeria's principal legislative instruments—the Cybercrimes Act 2015 (as amended 2024) and the Money Laundering (Prevention and Prohibition) Act 2022—provide a formal basis for investigation and prosecution (Alabi et al., 2025; UNODC, 2025). The NFIU disseminated 1,398 proactive intelligence reports in 2025 (NFIU, 2025). Conviction statistics published by the EFCC indicate several thousand successful prosecutions in recent years; however, conviction counts should not be read as conviction rates without corresponding data on total prosecutions initiated (Alabi et al., 2025; The Nation, 2024).

Persistent constraints include limited interoperability among the EFCC, NPF-NCCC and other agencies, resulting in duplication of effort and uneven deployment of scarce forensic capacity (UNODC, 2025). Heavy reliance on plea bargaining has also been criticised for producing comparatively lenient outcomes and for diverting attention from comprehensive asset recovery (Alabi et al., 2025). The Egmont Group (2025) continues to stress that effective disruption of cross-border illicit flows depends on timely, structured information exchange among financial intelligence units. Taken together, the secondary evidence suggests that legal architecture has outpaced operational coordination and technical capacity, particularly with respect to virtual-asset monitoring and digital-evidence handling.

Discussion

The institutional record confirms that cyber-enabled fraud is a material source of illicit proceeds in Nigeria and the wider sub-region, which digital financial channels introduce new layering opportunities, and that terrorist facilitators have adapted certain digital techniques. The implications of the tabulated evidence are considered here:

Implications of the Typology Distributions (Tables 1 and 2)

Table 1 indicates that advance fee fraud continues to dominate the regional typology space. This persistence suggests that social-engineering schemes retain operational utility for criminal networks even as more technologically sophisticated methods emerge. Table 2, by contrast, shows that within the subset of cases examined by the NFIU in 2025, romance scams and investment fraud account for the large majority. The divergence between the two distributions underscores the importance of treating regional and national evidence streams separately; it also suggests that Nigerian enforcement and intelligence priorities may usefully give heightened attention to romance and investment fraud without neglecting the continuing regional significance of advance fee schemes. The policy implication is that resource allocation and public-awareness campaigns should be calibrated to the specific typology mix prevailing in each jurisdiction rather than to a single regional average.

Implications of Sectoral Vulnerability Ratings (Table 3)

Table 3 places banking, real estate and virtual-asset service providers at the upper end of the National Inherent Risk Assessment scale. The elevated rating for VASPs is particularly consequential given Nigeria's high rate of cryptocurrency adoption. The implication is that regulatory and supervisory attention to virtual-asset service providers should be regarded as a core component of the national anti-money-laundering and counter-terrorism-financing architecture, not as a peripheral or experimental domain. At the same time, the continued high ratings for banking and real estate caution against any assumption that traditional sectors have been rendered secondary by the rise of digital assets.

Implications of Terrorism-Financing Patterns (Table 4; Figure 2)

Table 4 confirms that designated terrorist groups operating in and around Nigeria are assessed at high or very high threat levels for terrorism financing. Figure 2, adapted from institutional descriptions, illustrates a multi-phase digital funding sequence that exploits encrypted communications, intermediary accounts, sub-threshold transfers and local money mules. The implication is that detection and disruption efforts must address each phase of the sequence—solicitation, consolidation, layering and integration—rather than focusing exclusively on the final conversion into cash or dual-use goods. The documented use of gender-based proxy accounts further implies that identity-verification and beneficial-ownership controls must be sensitive to the possibility that accounts held in the names of women may be used to distance male operatives from visible transactions. These implications remain risk-oriented; they do not rest on a quantified attribution of terrorist funds to cybercrime.

Implications of Institutional Constraints

The secondary evidence on institutional performance points to a structural imbalance: legal architecture has advanced more rapidly than operational coordination and technical capacity. Limited interoperability among the EFCC, NPF-NCCC and other agencies produces duplication of effort and uneven forensic coverage (UNODC, 2025). Heavy reliance on plea bargaining risks under-emphasising asset recovery (Alabi et al., 2025). The implication is that incremental

improvements in statutory wording will yield limited returns unless accompanied by investments in shared case-management systems, specialised blockchain-analytical capacity, and a clearer institutional priority on the recovery and management of illicit assets.

Synthesis

Overall, the findings support a risk-oriented reading of the cybercrime–money-laundering–terrorism-financing nexus in Nigeria. Cyber-enabled fraud generates substantial illicit proceeds; digital financial channels expand layering opportunities; and certain terrorist facilitators have adapted digital techniques. The secondary evidence does not, however, sustain strong causal claims about the volume of terrorist funds derived specifically from cybercrime. Policy and research priorities should therefore focus on strengthening the informational and institutional conditions under which such attribution might eventually become feasible, while simultaneously closing the most evident operational gaps.

CONCLUSION

Drawing exclusively on secondary institutional sources and doctrinal analysis of Nigerian legislation, this study has examined the relationship between cybercrime, money laundering and terrorism financing in Nigeria within the West African context. Regional typology assessments indicate that advance fee fraud remains the most frequently documented cyber-enabled predicate, while Nigerian reporting for 2025 highlights the prominence of romance scams and investment fraud; institutional materials further describe multi-phase digital funding patterns and identity-masking practices associated with certain terrorist groups, together with elevated vulnerability ratings for virtual-asset service providers and related sectors. The national legal framework is comparatively developed, yet operational effectiveness continues to be constrained by limited inter-agency interoperability and incomplete technical capacity. Because the analysis relies on purposively selected secondary materials, it cannot independently quantify the share of terrorist funds derived from cybercrime and therefore advances a risk-oriented rather than causal interpretation; the principal contribution lies in the systematic synthesis of existing evidence, the clarification of conceptual linkages, and the identification of priority areas for intelligence sharing, virtual-asset oversight and asset recovery. On the basis of the foregoing analysis, Nigerian authorities should prioritise a centralised interoperable case-management platform among the NFIU, EFCC and NPF-NCCC; strengthen regulatory and supervisory capacity for virtual-asset service providers, including specialised blockchain-analytical training; tighten know-your-customer and beneficial-ownership controls on tiered fintech accounts and SIM–BVN linkages, with attention to gender-based proxy accounts; rebalance institutional incentives so that asset recovery receives attention comparable to conviction statistics; and expand specialised judicial training in the handling and admissibility of digital evidence in support of the 2024 Cybercrimes Act amendments.

REFERENCES

Alabi, L. M., Agbu, D. A., & Adesina, S. T. O. (2025). The role of EFCC and related institutions in the prosecution of cybercrimes in Nigeria. International Review of Law and Jurisprudence, 7(3), 129–139.

Egmont Group. (2025). Annual report 2024–2025. Egmont Group of Financial Intelligence Units.

Institute for Financial Integrity. (2023). Cyber-enabled fraud. Institute for Financial Integrity.

Inter-Governmental Action Group against Money Laundering in West Africa. (2010). GIABA report: Threat assessment of money laundering and terrorist financing in West Africa. GIABA.

Inter-Governmental Action Group against Money Laundering in West Africa. (2022a). 2022 annual report. GIABA.

Inter-Governmental Action Group against Money Laundering in West Africa. (2022b). Typologies of money laundering and terrorist financing linked to cybercrime in West Africa. GIABA.

Inter-Governmental Action Group against Money Laundering in West Africa. (2023). Annual report 2023. GIABA.

Nigerian Financial Intelligence Unit. (2022). 2020–2022 annual report compendium and National Inherent Risk Assessment. NFIU.

Nigerian Financial Intelligence Unit. (2025). 2025 annual report. NFIU.

Søgaard Clausen, C. C. (2024). Crypto laundering on the dark web: Characteristics and modus operandi [Master's thesis, Malmö University]. DiVA Portal.

Suchi, P. M., & Wika, P. N. (2021). Cybercrime and terrorism financing: Nigeria's potential vulnerabilities and policy options. International Journal of Research and Innovation in Social Science, 5(7), 420–427.

The Nation. (2024, May 16). Yahoo boys bringing shame to Nigeria – EFCC Chairman. The Nation.

U.S. Department of the Treasury. (2026). 2026 national money laundering risk assessment. U.S. Department of the Treasury.

United Nations Office on Drugs and Crime. (2025). Cybercrime assessment – Nigeria 2025. UNODC.

©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.