The Effect of Financial Technology in Combating International Terrorism Financing in Nigeria, 2009 – 2024

MURTALA ABUBAKAR, IRORO IZU

Abstract: *The global governance of international security by state actors in the international environment is becoming challenging because of the rising patterns and approaches of supporting the activities of terrorism. As a result of the rise of advanced Financial Technology (FinTech), state actors face the difficulties of regulating the financial inflow through the advanced Financial Technology. This paper therefore examines the effects of advanced financial technology in combatting international terrorism financing in Nigeria from 2009 to 2024. Adopting a securitization theory which argues that security is not just an objective condition but a speech act, the paper adopts thematic method of analysis to analyze the data gathered to understand the effect of financial technology in combating international terrorism in Nigeria. The paper concludes that Terrorism financing has continued to serve as fuel for terrorist outfits in Nigeria, despite the precautions put in place by the government and agencies, there is yet to be an impactful remedy to eradicate the scourge from the country's jurisprudence totally.*

Keywords: FinTech, Security, Terrorism Financing, Blockchain Technology, Financial Regulatory Agency

Introduction

In the world today, the importance of technology to society cannot be overemphasized. The evolution and growing progression in technology have revolutionized methods, techniques, and tactics of warfare. This phenomenon also applies to strategies adopted by non-state entities and terror organizations for the advancement of their illicit operations. From the use of social media for recruitment to communication by means of encrypted web protocols, this is terrorism of the new age where technology forms an integral part of terror operations. Illegitimate monetary transactions and money laundering have always been a challenge for crime syndicates and terrorist organizations since the digitization of money and related controls made it relatively impossible to transact discreetly. However, the emergence of cryptocurrency has opened a new venture of Terrorism Financing (TF) and Money Laundering (ML) for the tech-savvy terrorist organizations such as ISIS, Al-Qaeda and other transnational criminal outfits **(Weimann, G. 2016).** The financial system, from time immemorial, has been a user and early engine of technological development in response to the needs of the marketplace. It is no doubt that the

Murtala Abubakar (Sayyadimurtala1@gmail.com, 20222978@nileuniversity.edu.ng) Ph.d. Candidate, Department of Political Science and International Relations, Nile University of Nigeria, Abuja
Iroro Izu, Department of political science and international relations, Nile university of nigeria, Abuja

financial services landscape is being significantly reshaped by advances in information technology, consumer demand, volume, and scale of cash intermediation and process automation.

The global struggle to control and combat international terrorism has witnessed several successes and failures. One notable area where significant achievement has been registered is effectively curbing the funding of these violent activities. In Nigeria, combating terrorism politically and militarily requires just a strong will, and practical measures in meeting the financial challenge. Financial experts have identified significant structural and enforcement weaknesses in Nigeria's political, legislative, and regulatory financial environment. However, Nigerian law enforcement officers have always investigated, arrested, and prosecuted cases involving their own citizens and foreign visitors (Coker et al.2023).

Very strong local and international measures have also assisted in the suppression of domestically generated funding for the already defeated activities in Nigeria, such as crime and political corruption. Just as well, there is one special global financial notoriety that Nigeria shares with some other countries, although to a much lesser degree. Besides corruption and financial innovation being used to raise funds to wage the war on terrorism, the same financial innovation is being used to bypass current money laundering regulations and counter terrorism financing measures. Every country is involved, in one way or another. Nigeria also has come to rely on its domestic anti-money laundering regulations to determine the quality of its financial intelligence and gain access to reliable and original financial intelligence of other countries, as well as key regional and international financial centers (Ajide, 2023).

Terrorism remains one of the most significant contemporary challenges faced by individuals, governments, and international organizations because of its debilitating effects on human security, social stability, and global peace and development. The number of deaths from terrorism in Nigeria increased significantly in 2014, making it one of the most affected countries in the world. This is explained by the activities of fundamentalist groups in the Northeast, Indigenous Peoples in the Southeast, and the recent protests supervised by terrorists (Majekodunmi et al., 2022).

The proliferation of advanced financial technologies has revolutionized global commerce and financial systems. However, these advancements also present new avenues for the financing of terrorism. In Nigeria, terrorism financing (TF) is a significant challenge, exacerbated by porous borders, inadequate financial regulations, and the rise of technological innovations such as cryptocurrencies, mobile money, and online banking. This research seeks to analyze the challenges posed by these technologies in combating TF and recommend strategic solutions tailored to Nigeria’s unique socio-political and economic landscape.

Terrorism financing remains a critical challenge to national and global security, particularly in regions like Nigeria, where terrorist organizations such as Boko Haram and ISWAP operate with significant financial networks. While global counter-terrorism financing (CTF) measures have evolved, the rapid proliferation of advanced financial technologies (Fintech) between 2009 and 2024 has introduced new complexities. Cryptocurrencies, digital wallets, and decentralized finance (DeFi) platforms offer both opportunities and vulnerabilities in the fight against terrorism financing **(Olorunshola, & Adebayo, 2021)**

The war on terrorism is truly a financial war; terrorists need money to finance their corrupt and evil purposes. As the world stands united in its determination to condemn and destroy terrorists and those who sponsor them, the international community recognized the threat that terrorism posed to the international financial system. The international community, therefore, took measures to combat the financing of international terrorism by urging all its members to effectively criminalize terrorist financing and by taking measures to establish rules and regulations that stem the flow of money that goes into financing terrorism. Some of the measures taken by the international community included the establishment and operations of competent authorities made up of law enforcement and intelligence agencies such as supervisory authorities. (Ferreira & Sandner, 2021).

There is no single universally accepted definition of financial technology. However, many parties have taken the initiative to define it. The definitions tend to suggest that it refers to the sophisticated financial services that contribute to the move towards globalization of finance. It includes many financial products and services, including credit and e-wallet platforms that allow users to transfer money over the internet. Since it has started reshaping the financial industry in many parts of the world, Nigeria began using advanced financial technology in 2009 (Olawale, 2024).

While fintech provides innovative financial services, it also poses new challenges and risks to the financial services industry in the proximity of challenges associated with terrorist financing. These challenges manifest themselves in different facets. Overall, more connectivity means more vulnerability, so the more integrated the financial industry becomes in cross-border networks, the more sophisticated the network of terrorist financing becomes. Conversely, the financial sector is using technological advances to enhance security to withstand terrorism crimes, which has increased exponentially with high potential connected with information technology. The financial sector seeks out technology to improve its design in terms of customer identification and due diligence, enhance the infrastructure needed for anti-fraud measures, and use big data to detect and analyze unusual transactions or patterns. Modern anti-money laundering techniques are transforming significantly as artificial intelligence, machine learning, big data, and the technological approach focused on financial crime prevention are now evolving. The weakness of any infrastructure can dampen the effectiveness of anti-money laundering aimed at detecting and preventing the financial facilitation of international terrorism. The absence of a firm financial infrastructure indubitably facilitates terrorism (Tompihe, 2023).

Against the background, a key question that has arisen is: how do advanced financial technology tools available in the 21st century pose new challenges to all the existing and proposed rules and regulations that combat the financing of international terrorism? Despite ongoing national and international efforts to combat terrorism financing, Nigeria continues to face growing threats from terrorist organizations. Existing AML/CFT regimes in Nigeria were mostly intended for conventional banking institutions and sometimes struggle to properly handle the anonymity, speed, decentralization, and transnational nature of technology-enabled financial transactions (FATF, 2021).

The expanding usage of cryptocurrencies, mobile money platforms, and DeFi systems has created regulatory blind spots that terrorist actors can exploit to disguise financial traces and elude law enforcement detection (UNODC, 2020; Europol, 2021). Although Nigerian institutions have taken numerous regulatory and technological measures, issues exist in institutional coordination, technical capacity, legislative adaptation, and effective enforcement (ISS, 2021).

Furthermore, terrorism financing has substantial socio-economic effects for Nigeria, including undermining development, eroding governance systems, deterring investment, and aggravating insecurity (Zubrzycki, W. (2022). The lack of thorough empirical studies addressing the relationship between sophisticated financial technology and terrorism financing in Nigeria presents a crucial knowledge gap that this dissertation seeks to address.

1.2 Empirical Review

Empirical studies at the worldwide level reveal that terrorist organizations are flexible and responsive to changes in finance legislation and technology. FATF (2019, 2021) studies note the increased use of virtual assets, online payment systems, and crowdfunding platforms in terrorism financing schemes. Prior Nigerian research often focusses on terrorism or financial crime independently, with insufficient incorporation of fintech-specific analysis. This dispersion underlines the necessity for a comprehensive, technology-focused inquiry.

In the year 2013, Abdu Abubakar conducted research on "An Appraisal of Legal and Administrative Framework for Combating Terrorist Financing and Money Laundering in Nigeria" which presents a comprehensive examination of Nigeria's legal and institutional mechanisms aimed at countering terrorist financing and money laundering. The author emphasizes the necessity of robust anti-money laundering (AML) and combating the financing of terrorism (CFT) frameworks as critical elements in ensuring global financial stability.

Saulawa and Bello 2015 conducted research on "Cyberterrorism: A Comparative Legal Perspective" that offers a critical examination of the intersection between cyberterrorism and the legal frameworks designed to combat it, particularly in the context of Nigeria. The authors highlight the rapid development of the internet and the initial lack of regulation, which has allowed cyberspace to become a fertile ground for terrorist activities.

In their study "Cyber as an enabler of terrorism financing, now and in the future," (Carroll and Windle, 2019) provides a comprehensive examination of the evolving landscape of terrorism financing, particularly in the context of advanced financial technology. The authors emphasize that terrorism finance encompasses not only the direct funding of attacks but also the operational costs associated with sustaining terrorist organizations. Similarly, Sonnie Bowei (2019) argues that the inability to effectively curb terrorism in Nigeria stems from inadequacies in the application of technical and financial resources, as well as deficiencies in policy implementation. This perspective is particularly relevant in the context of combating the financing of international terrorism, as it highlights the interplay between resource allocation and operational effectiveness.

In the year 2024, Adewopo, Azumah, Yakubu, Gyamfi, Ozer, and Elsayed conducted research on "A Comprehensive Analytical Review on Cybercrime in West Africa" which provides a thorough examination of the evolving landscape of cybercrime in the West African region, with particular emphasis on Nigeria's challenges in combating financial fraud. The authors contextualize the issue within the framework established by the Economic Community of West African States (ECOWAS) in 2011, which aimed to create a legal structure for addressing cybercrime.

Olatunji and Aruwaji (2020) conducted a quantitative study involving Nigeria’s anti-graft agencies, including the Nigeria Communication Commission (NCC), to assess the impact of forensic accounting investigations on tracking financial cybercrime and terrorist financing. Their analysis revealed that forensic accounting significantly discloses the associations between financial cybercrime and terrorist financing.

Olujobi and Yebisi (2023) critically examine Nigeria’s persistent challenges in combating money laundering and terrorism financing, despite the existence of several anti-corruption laws. The study adopts a conceptual legal approach, reviewing Nigeria’s legal frameworks-including the Money Laundering (Prohibition) Act, 2012 (as amended), and the Terrorism (Prevention) Act, 2013 (as amended)-and compares them with international best practices from countries like Canada, the UK, Hong Kong, and China. The authors find that Nigeria’s legal framework lacks clarity, especially regarding the criminal use of legitimate earnings for terrorism and cultism and is deficient in asset recovery and confiscation mechanisms.

All the reviewed literature were conducted to examine whether if their studies collectively underscore the multifaceted nature of combating terrorism financing in Nigeria, particularly in light of advancing financial technologies. But against the reviewed empirical studies, there exist gap of not studying combating international terrorism financing in Nigeria using Advanced financial technologies. Despite increased global attention to fintech-related financial crime, there remains a severe dearth in Nigeria-specific, qualitative, and longitudinal studies evaluating how modern financial technology support international terrorism financing. Existing literature often lacks:

In-depth qualitative observations from regulatory and security entities
Focus on DeFi and new technologies
Integrated analysis of technology, legislation, and socio-economic impact
This paper addresses these shortcomings by giving a complete qualitative analysis covering the period 2009–2024.

1.3 Literature Review

1.3.1 Financial Technology

Financial technology, generally referred to as FinTech, covers the application of digital technologies to deliver financial products and services in novel ways. These include mobile payments, digital banking, cryptocurrency, blockchain systems, peer-to-peer platforms, and decentralized finance (World Bank, 2020). FinTech has played a revolutionary role in boosting financial inclusion, particularly in developing economies such as Nigeria, where huge sectors of the population were historically excluded from formal banking systems (CBN, 2022). However, the same elements that improve accessibility—speed, low cost, anonymity, and cross-border reach—also offer weaknesses that can be abused for illicit financial transactions (FATF, 2021).

Financial technology, otherwise known as FinTech, refers to the rapidly evolving and innovative phenomenon that is transforming the financial services industry. Broadly speaking, FinTech includes a vast repertoire of technological innovations that aim to streamline financial processes and expand the range of financial services available. FinTech may apply to both the technology that financial institutions use for back-end operations and consumer financial behavior, including lending, digital payments, online banking, blockchain, and currency exchanges. The latest FinTech innovations are digital finance, the broadest term, including cryptocurrencies, neo-banking, and reg-tech—developments that can and do disrupt and transform traditional financial systems. Therefore, FinTech is a versatile phenomenon that encompasses not only the diversity of financial service providers but also the diversity of software, institutions, and services within the data-driven sphere (Kumari & Devi, 2022).

1.3.2 Advanced Financial Technology

Definition of Advanced Financial Technology (Fintech) The term financial technology is now a constantly changing concept with classical financial functions related to technologically advanced systems and new products that monitor and control financial systems. Advanced financial technology is a type of Fintech. Nonetheless, it is important to highlight this term here. Fintech is employed to describe innovation in traditional financial services. Expert studies have established that new innovative technology has brought Fintech into play for the context, which is analyzed in the present study. Advanced financial technology (AFT) provides an opportunity for traditional finance sectors to create digital programs. Identification of AFT capacity for the national security focus (combating terrorism financing). Financial transactions and services significantly improve with new systems. The remote device access user can carry out all the required operations (transfer, receipt, payment, and obtain loans and securities) via AFT systems faster than banks and mobile money systems. Innovative technology comprises connectivity, the internet, artificial intelligence, machine learning, speech recognition, and cryptographic technologies. The modern system of money movements related to these financial systems can create many new trends. Although these innovative advances in Fintech fields are cross-cutting and globally shaping, a study specially tailored for a developing country has not yet been undertaken to evaluate the threat of terrorism financing to advanced financial technologies and services (Kumari & Devi, 2022).

1.3.4 Cryptocurrencies and Terrorism Financing

Cryptocurrencies are digital assets that rely on cryptographic algorithms and distributed ledger technology to enable peer-to-peer transactions without centralized intermediaries. While cryptocurrencies give transparency at the blockchain level, they also enable pseudonymity and can be paired with privacy tools such as mixers and privacy coins (FATF, 2021).

Studies reveal that terrorist organizations have experimented with cryptocurrencies for fundraising and finance transfers, particularly through online propaganda channels and social media platforms (Europol, 2021). Although the size is smaller than traditional methods, the trajectory brings growing hazards.

Cryptocurrencies like Bitcoin have emerged as tools for terrorism financing due to their pseudonymous nature and cross-border efficiency. Terrorist groups such as Boko Haram and ISWAP exploit unlicensed forex dealers and informal financial channels to move funds, often using cryptocurrencies to evade detection (Brill & Keene, 2014; NFIU, 2022). For example, a 2022 NFIU investigation revealed that ISWAP received $43 million via an unlicensed forex dealer, which was later traced to purchases of materials like fertilizers and solar panels used in terrorist operations (NFIU, 2022). However, blockchain analytics and AI tools have improved detection rates, with models achieving over 90% precision in identifying suspicious transactions (Agorbia-Atta et al., 2024).

Nigeria's AML/CFT framework has integrated advanced fintech solutions to counter terrorism financing. The Central Bank of Nigeria (CBN) mandates strict monitoring of fintech platforms and digital payments, requiring Suspicious Transaction Reports (STRs) and Customer Due Diligence (CDD) (CBN, 2021). The Nigerian Financial Intelligence Unit (NFIU) employs AI-driven systems to analyze transaction patterns, particularly in high-risk sectors like Bureau de Change (BDC) operations and NGOs (NFIU, 2022). For instance, AI algorithms flagged 35 million Naira in cash transfers linked to ISWAP, leading to arrests and frozen accounts (NFIU, 2022).

1.3.5 Terrorism and Terrorism Financing

Terrorism: Is usually defined as the use or threat of violence against civilians or non-combatants to achieve political, ideological, or religious aims. While definitions vary between agencies, there is broad understanding that terrorism relies largely on sustained financial resources (United Nations, 1999; FATF, 2019).

Terrorism finance: Refers to the gathering, movement, storage, and use of funds intended to assist terrorist operations or groups. Unlike money laundering, which often includes proceeds of crime, terrorism financing may originate from both criminal and legitimate sources, including donations, charities, and lawful economic activity (FATF, 2019; UNODC, 2020). This dual-source nature hampers detection and enforcement attempts. In Nigeria, terrorism financing has been linked to kidnapping for ransom, smuggling, cattle rustling, illicit taxes, charitable misuse, and increasingly, digital financial platforms (Onuoha, 2014; ISS, 2021). In this respect, terrorism is a somewhat slippery phenomenon. On a day-to-day basis, the term is often employed in a rather imprecise manner and rhetorically loaded. In academia, in the social sciences, and in political sciences in particular, a vast literature exists that seeks to uncover or explications the essence of terrorism without attaining precise results. Lack of consensus on a definition does not prevent scholars from joining in, however, referencing or alluding to definitions as if there were general agreement on the issue. In recent years, teleological approaches have gained popularity; while perhaps intuitively understandable, their wisdom is nevertheless disputable. The search for a clarification of terrorism is made more complicated by the breadth of the concept.

Theoretical Framework

This paper adopts securitization theory, developed by scholars of the Copenhagen School—particularly Barry Buzan, Ole Wæver, and Jaap de Wilde which offers a framework for understanding how issues become framed as matters of security, rather than mere policy or economic concerns. The central premise of the theory is that security is not just an objective condition but a speech act: a process by which state actors declare an issue as an existential threat to a valued referent object (such as national security, sovereignty, or public order). When such framing is accepted by the relevant audience, it legitimizes the adoption of extraordinary measures outside normal political procedures. Securitization theory illustrates how states frame certain challenges as security risks needing extreme measures (Buzan, Waever, & de Wilde, 1998). The classification of terrorism financing as a national and international security issue necessitates intensified surveillance, regulation, and international collaboration.

This paper applies Securitization Theory to examine how the misuse of advanced financial technology (FinTech) has been discursively constructed as a threat to Nigeria's national security, particularly in the context of terrorism financing. Although FinTech was initially introduced to enhance financial inclusion and economic efficiency, recent developments—such as the rise in cryptocurrency adoption, anonymous mobile money transfers, and the use of peer-to-peer platforms—have prompted security and regulatory actors in Nigeria to reframe these innovations as facilitators of terrorism financing.

Methodology

This paper is a part of Ph.D. dissertation, that is section as part of requirements for the award of Ph.D. degree. As such, the methodology has no difference with the method employed in the main Ph.D. dissertation.

3.1 Research Design

This paper utilizes qualitative research design. Qualitative research is particularly ideal for studies that seek to study complex social, institutional, and security-related issues where meanings, perceptions, and contextual understanding are key. The qualitative approach provides an in-depth investigation of how terrorist groups exploit financial technology, how regulatory institutions respond to these risks, and how policies are formed and implemented within Nigeria's counter-terrorism finance architecture. This approach coincides with the interpretivist school in international relations and security studies, which emphasizes understanding social reality via the views of relevant actors.

3.2 Source of Data

The paper adopts the combination of both primary and secondary sources of data. The secondary source is the one in which the data is sourced from textbooks, journals, articles,

newspapers, magazines, internet, and the use of our modern-day artificial Intelligence like ChatGPT, and gamma, that are relevant to the research problem under study which are gathered for the purpose of knowledge. On the other hand, the primary source of data is the one that data is sourced using researchers' participants. Data here is sourced using direct involvement of the researcher, and the data is generated specifically for the purpose of this study. The primary data for this research paper is gathered through counter-terrorism financing and financial regulation in Nigeria.
Economic and Financial Crimes Commission (EFCC),
Nigerian Financial Intelligence Unit (NFIU),
Central Bank of Nigeria (CBN),
Relevant security agencies.

3.3 Method of Data Analysis

Data has been collected from engaged experts from the Defense Intelligence Agency (DIA), Department of State Service (DSS), Federal Ministry of Justice (FMOJ), National Intelligence Agency (NIA), Nigeria Police Force (NPF), Nigeria Security and Civil Defense Corps (NSCDC), and Office of the National Security Adviser (ONSA). The researcher reviewed data and information acquired from interviews with the above-mentioned stakeholders, accessed case studies from the NFIU database and the database of stakeholders above. The investigation also relies on the results of thorough analysis of scholarly publications and open-source documents. During the investigation, the researcher held multiple meetings with the working group. The limitations encountered by the researcher include lack of timely response and, in some cases, no response at all from stakeholders.

Advanced Financial Technology (FinTech) and Combating International Terrorism Financing in Nigeria

The data presented in this section is a result of data gathered from the field of interview, and other relevant scholarly writings with reference to international terrorism financing. Data obtained for this analysis generally from: CBN, EFCC, NFIU among other relevant agencies.

4.1 Regulators understanding of Terrorism Financing

Before examining the effects of FinTech on terrorism financing from regulatory Perspectives in Nigeria, the research investigates the knowledge of regulators on terrorism financing. In doing so, the research referred to the definition of terrorism financing from the literature, which has defined as:

> Terrorism financing refers to the act of soliciting, receiving, providing, or using funds or financial support by any means directly or indirectly willfully and unlawfully with the knowledge or intention that such funds will be used, in whole or in part, to commit terrorist acts, support terrorist organizations, or assist individual terrorists

Further study of the data from the respondents using thematic analysis, the following themes have been found which served as the most popular digital financial products utilized for terrorism financing in Nigeria:

Cryptocurrencies and virtual currencies: These digital currencies, which operate on decentralized networks and frequently provide a degree of anonymity, have been implicated with money laundering operations owing to the difficulties in tracking transactions and identifying the genuine owners of cash.

Online payment platforms: These platforms, such as e-wallets or peer-to-peer payment services, offer rapid and efficient means for sending payments. Criminals may exploit these services to shift illegal monies across accounts or perform anonymous transactions.

Digital remittance services: These services enable consumers to transmit money electronically across borders. Criminals may utilize these services to transfer illegal payments, taking advantage of the speed and probable lack of sufficient identification or due diligence requirements.

Online banking: While internet banking itself is not intrinsically utilized for terrorism financing, criminals may use it as a tool to shift cash between accounts or perform fraudulent transactions,

The respondents were then asked if the introduction of bitcoin had increased the effects of FinTech on terrorism financing. They stated that the introduction of cryptocurrencies has undoubtedly provided new possibilities and concerns regarding money laundering. While cryptocurrencies provide several advantages such as decentralized networks and speedier transactions, they also have some traits that might be abused by money launderers. For instance, a respondent from NFIU revealed that:

> "The rise of cryptocurrency has brought forth both fresh prospects and challenges in the realm of money laundering. Cryptocurrencies provide decentralized networks and swift transactions, but they also harbor traits susceptible to exploitation by money launderers, primarily anonymity. Cryptocurrency transactions employ pseudonyms, making it difficult to ascertain the real identities involved, a feature that can be alluring to terrorism financiers (terrorism financing Control Expert NFIU)"

4.1.1 Cryptocurrency and regulatory agencies

A review of the comments from specialists in terrorism financing and FinTech-related regulatory agencies found the following themes in connection to why the advent of cryptocurrencies increased the influence of FinTech on terrorism financing:

Anonymity: Cryptocurrencies may give a certain amount of anonymity since transactions are conducted using pseudonyms, making it hard to identify the real-world individuals behind the transactions. This anonymity might be enticing to terrorism financiers.

Borderless Transactions: Cryptocurrencies allow borderless transactions without the requirement for intermediate financial institutions. This functionality may make it simpler for terrorism financiers to move monies across borders swiftly and discreetly.

Lack of Regulation: The regulatory frameworks surrounding cryptocurrencies are continuously evolving, and in certain countries, they are still forming. This may generate gaps and loopholes that terrorism financiers may exploit.

Tumbling and Mixing Services: terrorism financiers employ tumbling and mixing services to further disguise the origins of bitcoin transactions. These services split up transactions into tiny chunks, mix them with other transactions, and redistribute funds to hinder tracking.

However, it is vital to emphasize that the rising use of cryptocurrencies has also triggered significant efforts by regulators, governments, and financial institutions to address the concerns connected with terrorism financing. Many countries have established or are proposing rules to compel cryptocurrency exchanges and service providers to apply anti-money laundering safeguards and conduct sufficient client due diligence. Furthermore, developments in blockchain analysis and forensic technology are being employed to track illegal transactions and discover patterns linked with terrorism financing operations inside the cryptocurrency industry. Collaborative initiatives between the corporate and governmental sectors are continually growing to increase the openness and integrity of cryptocurrency transactions.

Through the interview, the research further tries to identify the issues connected with the use of technology in combatting terrorism financing in Nigeria. It was observed that the employment of technology to counter terrorism financing in Nigeria confronts various hurdles. For instance, a responder from CBN disclosed that:

> "One of the significant challenges is an ever-changing regulatory environment which lies in the constant evolution of the regulatory landscape for technology and anti- terrorism financing measures. Adapting current regulations to incorporate new technologies and digital platforms, while maintaining effective oversight, presents challenges and necessitates close collaboration between regulatory bodies, financial institutions, and technology providers. (terrorism financing Control Expert – CBN)".

4.2 Role of Regulation in Curtailing Financial Technology Induced Terrorism financing

The finding of this paper indicates that efforts have been undertaken to formulate and enforce laws and rules aimed at combating terrorism financing, especially those which transpire via financial technology. In this regard, a representative from the Central Bank of Nigeria disclosed that:

> "The primary legislation governing anti-money laundering efforts in Nigeria is the Money Laundering (Prohibition) Act 2011 (as amended in 2012), along with other related regulations issued by the Central Bank of Nigeria (CBN) and the Economic and Financial Crimes Commission (EFCC). However, the adequacy of these laws

> in curtailing financial technology-induced money laundering can vary depending on several factors (Terrorism Financing Control Expert – CBN)"

Subsequent examination of the comments via theme analysis indicated that, in Nigeria, as in many jurisdictions, the rapid progress in financial technology poses persistent issues for regulatory frameworks. Eventually, the topics were analyzed consequently arriving at some prospective areas where the current laws in Nigeria may confront issues in limiting financial technology-induced terrorism financing include:

4.2.1 Cryptocurrencies: The laws of Nigeria do not give explicit rules for cryptocurrencies. This may cause difficulty in successfully addressing the risk connected with cryptocurrency-based terrorism financing.

4.2.2 Digital Identity Verification: Adequate digital identity verification plays a significant role in combating terrorism financing, However, there may be issues connected to the adoption and enforcement of standardized digital identity verification methods in the Nigerian financial ecosystem.

4.2.3 Cross-Border Transactions: terrorism financing sometimes includes cross-border transactions, which necessitate international collaboration. Although Nigeria has engaged into many agreements to improve international cooperation, issues linked to jurisdictional limits and differences in regulatory frameworks may still exist.

4.2.4 Ongoing technical advancements: The quick speed of technical advancements necessitates ongoing modification of laws and regulations to keep pace with rising terrorism financing dangers and innovative ways adopted by criminals.

It is crucial to highlight that to address these difficulties, Nigerian authorities have been expanding their efforts, including continuous cooperation with foreign entities and organizations, to enhance the legal and regulatory frameworks. This involves continual amendments to regulations and the creation of specific rules linked to financial technology and money laundering. Furthermore, it can be deduced that the efficiency of laws and regulations in mitigating financial technology-induced terrorism financing also rides on enforcement efforts, capacity building, and partnership among different stakeholders, including financial institutions, regulatory bodies, and law enforcement agencies.

Additionally, respondents were asked if there are laws created solely to handle technology-based terrorism financing; nevertheless, it was determined that such laws do not exist in the nation.

On this, an expert from CBN revealed that*:*

> "In Nigeria, there is no specific law that exclusively focuses on technology-based terrorism financing. However, current rules and regulations, such as the terrorism financing (Prohibition) Act 2011 (as modified in 2012). The terrorism financing Acts prohibits

> terrorism financing operations regardless of the methods used to perpetrate the violation. It comprises all types of money laundering, including those that involve financial technology. The Act sets requirements on financial institutions, including banks and other specified non-financial entities, to conduct anti money laundering measures and report suspicious activities. (Terrorism Financing Expert –CBN)"

Therefore, it can be concluded that while there is no specific law tailored solely to technology-based terrorism financing, the existing laws and regulations are designed to be comprehensive and adaptable enough to address terrorism financing risks, including those coming from advancements in financial technology. However, it is vital for regulators and authorities to regularly examine and update these laws in response to growing threats and technical innovations or to establish special laws relating to technology-induced terrorism financing.

4.3 Effectiveness of Existing Laws and Regulations in Preventing Terrorist Financing

Although there is a strong legal and regulatory structure in place to stop terrorist financing, there are questions over how effective these measures are.

Implementation and Enforcement: Although Nigeria has passed rules and regulations to combat the funding of terrorism, there are questions over how well they are being carried out. This could be the result of corruption in the relevant agencies, insufficient funding, or a lack of capability.

Interagency Coordination: The NFIU, CBN, and law enforcement authorities must work closely together to prevent terrorist financing. Nevertheless, there have been cases of poor coordination and exchange of information between various organizations, which could make it more difficult for them to successfully stop the funding of terrorism.

Capacity Building and Training: To improve their capacity to identify and stop terrorist financing, financial institutions and pertinent agencies must receive ongoing training and capacity building. This entails enhancing risk awareness, putting in place efficient AML/CTF procedures, and making sure that pertinent rules and regulations are followed.

Financial Inclusion and Informal Financial Channels: A large percentage of Nigerians are either underbanked or unbanked, which could result in a greater reliance on unofficial financial channels. These routes, like cash couriers or the hawala system, may be more susceptible to being used to finance terrorism.

Proliferation of Terrorist Groups: Fighting terrorist financing is made extremely difficult by the presence of multiple terrorist organizations in Nigeria, including Boko Haram, the Islamic State in West Africa (ISWAP), the Indigenous People of Biafra (IPOB), Yan Bindiga, and Yan Ta'adda. These organizations have been known to adopt numerous and intricate financing ways, making it difficult for authorities to uncover and interrupt their activities.

Overall, there is a need for improved implementation and enforcement of current legislation, enhanced interagency cooperation, capacity building, and addressing the issues posed to strengthen the effectiveness of the counter terrorist finance regime.

4.4 Knowledge Sharing and Partnership with Internal and External Stakeholders in Addressing Technology-induced Terrorism Financing

Authorities were asked to share thoughts on whether collaboration with internal and external stakeholders aid in combating technology-induced terrorism financing. One of the respondents from NFIU explained that:

> "Nigeria has taken steps to combat tech-based terrorism financing through internal and external partnerships. Domestically, agencies like the EFCC and NFIU work to combat terrorism financing using technology. Nigeria also interacts with the private sector, especially banks and FinTech companies, to improve anti- terrorism financing efforts and protect digital transactions, decreasing tech-related laundering risks. Nigeria has built worldwide alliances in its battle against terrorism financing. As a member of the Egmont Group, a worldwide network of financial intelligence units, Nigeria provides information and combats terrorism financing, especially tech-related incidents, across borders. The government also partners with international groups like FATF and UNODC to design and implement anti- terrorism financing measures, notably those involving technology-driven terrorism financing. (Terrorism Financing Control Expert – NFIU)"

Analyzing the responses from all the respondents via thematic analysis created two themes of partnerships, which are internal and external cooperation.

Internal Collaboration: Internally, the Nigerian government has created organizations and regulatory agencies such as the Economic and Financial Crimes Commission (EFCC) and the Nigerian Financial Intelligence Unit (NFIU). These agencies aim towards combating terrorism financing and criminal financial activities, especially those performed via technological platforms. Additionally, Nigeria has collaborated with the business sector, including banks, FinTech companies, and technology service providers, to build effective terrorism financing measures. These partnerships seek to strengthen the security and integrity of digital financial transactions, therefore minimizing the danger of technology-induced terrorism financing

International Collaboration: Nigeria has also formed international alliances to tackle terrorism financing. The nation is a member of the Egmont Group, which is a worldwide network of financial intelligence units that work to exchange information and fight money laundering and terrorism funding. This membership enables Nigeria to share information with other nations to investigate and prevent terrorism financing, especially those connected to technology. Furthermore, Nigeria engages with international organizations such as the Financial Action Task Force (FATF) and the United Nations Office on Drugs and Crime (UNODC). These collaborations assist Nigeria develop and execute anti- terrorism financing measures, especially those unique to technology-induced terrorism financing.

> Overall, the regulatory authorities in Nigeria understand the necessity of collaborations with both internal and external players in tackling technology-induced terrorism financing. These collaborations assist in boosting the country's capabilities to fight terrorism financing using technological platforms and secure its financial system.
> Additionally, the respondents were also requested to share some views on the success of these internal and external partnerships.

In this, a respondent from NFIU provides the following insights:

> "Partnerships in Nigeria have been highly effective in addressing technology induced terrorism financing. Agencies such as NFIU and EFCC play crucial roles in investigating and prosecuting financial crimes, especially those utilizing technology. Nigeria's involvement with the Egmont Group gives access to crucial information networks, enhancing investigative capacity and global collaboration against terrorism financing. This relationship supports Nigeria in preventing terrorism financing notably via internet platforms. Collaborations with the business sector facilitate the implementation of KYC and AML compliance procedures, boosting the identification and prevention of illegal financial transactions using technological platforms. (Terrorism Financing Control Expert – NFIU)"

The findings demonstrate that FinTech has both good and bad impacts on money laundering. The research also highlighted cryptocurrencies and virtual currencies, online payment platforms, digital remittance services and online banking as the most popular FinTech instruments utilized in continuing terrorism financing by criminals. It was also shown that introduction of cryptocurrencies intensified the influence of FinTech on money laundering owing to problems of anonymity, borderless transactions, lack of regulation, and tumbling and mixing services.

Conclusion

Terrorism financing has continued to serve as fuel for terrorist outfits in Nigeria. Despite the precautions put in place by the government and agencies, there is yet to be an impactful remedy to eradicate the scourge from the country's jurisprudence totally. Considering the enormous diversity of obstacles encountered in combating terrorism financing, it leaves no element of surprise as to the ineffectiveness of counter-terrorism finance measures non-Nigeria. It is vital to emphasize that understanding the mechanics of terrorism financing is the first step in arriving at viable methods and techniques to nipping the menace in the bud. This is so because the findings of the investigation have showed that terrorist organizations and their sponsors are miles ahead of the established institutions burdened with the job of tackling the threat. Similarly, technology and digital tools have become increasingly advantageous to terrorist organizations, making it impossible to maintain track of their actions. Thus, there is a pressing need for concerted effort and intervention to equip the authorized agencies with the requisite prowess to defy and predict terrorist outfits.

At this juncture, it is important that terrorist organizations do not rely simply on a certain channel or source of finance but use different techniques to generate, move and utilize monies. They interchange these ways to ensure that regulatory bodies find it difficult to keep pace with their actions. Consequently, the timing of this research is excellent as it draws the attention of the government, agencies, and stakeholders in the country to obtain insight into the mode of operation of terrorist organizations, particularly in terms of terrorism financing. Thus, the procedures mentioned herein should be thoroughly researched to establish effective policies and tactics that will match modern exigencies and have the desired impact in preventing terrorism financing and damaging their networks inadvertently**.**

Terrorist financing has detrimental repercussions on both Nigeria's economy and national security. It leads to the loss of lives and assets, weakens the rule of law, and discourages potential foreign investments due to the instability generated by terrorist activities. Terrorism financing affects economic growth in several ways, including decreased foreign direct investment, suspension of economic activities in affected areas, and the deployment of significant resources towards counter-terrorism efforts that might have been used for other development projects and social services.

References

Weimann, G. (2016). The emerging role of social media in the recruitment of foreign fighters. In Foreign fighters under international law and beyond (pp. 77-95). The Hague: TMC Asser Press.

Coker, J. O., Uzougbo, N. S., Oguejiofor, B. B., & Akagha, O. V. (2023). The role of legal practitioners in mitigating corporate risks in Nigeria: a comprehensive review of existing literature on the strategies and approaches adopted by legal practitioners in Nigeria to mitigate corporate risks. Finance & Accounting Research Journal, 5(10), 309-332.

Ajide, F. (2023). Anti-Money Laundering Regulations and Entrepreneurship: The Case of Africa. Concepts and cases of illicit finance.

Majekodunmi, T. A., Akintola, J. O., Idahosa, M. E., Ikubanni, O. O., & Aidonojie, P. A. (2022). The causes of the Rising incidence of Terrorism occasioning Deprivation of the Right to Life in Nigeria. NIU Journal of Humanities, 7(2), 129-138.

Olorunshola, A. A., & Adebayo, S. O. (2021). Financial technology and terrorism financing in Nigeria: Emerging threats and countermeasures. African Security Review, 30(4), 345–361.

Ferreira, A. & Sandner, P. (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. Computer Law & Security Review.

Olawale, A. (2024). The impact of capital market on the economic growth of Nigeria. GSC Advanced Research and Reviews.

Tompihe, J. G. (2023). Financing Terrorism with Fintechs in West Africa, In Exploring the Dark Side of FinTech and Implications of Monetary Policy (pp. 118-143). IGI Global.

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF.

Canton, H. (2021). United Nations Office on drugs and crime—UNODC. In The Europa directory of international organizations 2021 (pp. 240-244). Routledge.

European Union Agency for Law Enforcement Cooperation (Europol). (2018). Internet organised crime threat assessment (IOCTA). https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Institute for Security Studies (2019). Economics of terrorism in Lake Chad Basin. Retrieved October 24, 2020, from https://issafrica.org/amp/iss-

Zubrzycki, W. (2022). The financing of terrorist activities. Internal Security, 14(1), 183-194.

Abubakar, I. A. (2013). An appraisal of legal and administrative framework for combating terrorist financing and money laundering in Nigeria.

Saulawa, M. A. A., & Marshal, J. B. (2015). Cyberterrorism: A Comparative Legal Perspective. JL Pol'y & Globalization, 33, 1.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. Journal of Policing, Intelligence and Counter Terrorism, 13(3), 285-300.

Delfour, M. (2021). Human security and the Nigerian counterterrorism policy: Is the Nigerian counterterrorism policy human security centred?.

Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2024). A comprehensive analytical review on cybercrime in West Africa. arXiv preprint arXiv:2402.01649.

Olatunji, T. E., & Aruwaji, A. M. (2020). Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria. Journal of Auditing, Finance, and Forensic Accounting, 8(2), 55-66. https://doi.org/10.21107/jaffa.v8i2.8350

Olujobi, O. J., & Yebisi, E. T. (2023). Combating the crimes of money laundering and terrorism financing in Nigeria: A legal approach for combating the menace. Journal of Money Laundering Control, 26(3), 672–690

Kumari, A. & Devi, N. C. (2022). The impact of fintech and blockchain technologies on banking and financial services. Technology Innovation Management Review.

Brill, A., & Keene, L. (2014). Cryptocurrencies: The next generation of terrorist financing? Defence Against Terrorism Review, 6(1), 7-30.

Agorbia-Atta, C., Atalor, I., Agyei, R. K., & Nachinaba, R. (2024). Combating terrorist financing in cryptocurrency platforms: The role of AI and machine learning. World Journal of Advanced Research and Reviews, 23(3), 1477–1486.

Emeh, I. E., Isah, A., Olise, C. N., & Ikeanyibe, M. O. (2021). Countering insurgency in Nigeria with Terrorist Resource Model; a focus on Boko Haram sect. African Journal of Terrorism & Insurgency Research (AJoTIR), 2(2).

Musa, H. S. E., Yunusa, A., & Yaro, N. M. The Role of Nigerian Financial Intelligence Unit in Fighting Money Laundering for Financing Terrorism in Nigeria.