Yamtara-Wala Journal of Arts, Management and Social Sciences **(YaJAMSS)**
Volume 3, Issue 3. December 2023 ISSN: 2971-5016

THE ROLE OF NIGERIAN FINANCIAL INTELLIGENCE UNIT (NFIU) IN CURBING MONEY LAUNDERING AND TERRORISM FINANCING 2005-2021

Julia O. Ogbaji, PhD
Department of History and War Studies, Nigerian Defense Academy, Kaduna – Nigeria
Author's E-mail: jooagbaji@nda.edu.ng

Abstract

The activities of terrorist groups in the West African sub-region is becoming increasingly complicated and sophisticated. In Nigeria, for example, several militant groups in the Niger Delta, secessionist agitation groups in the southeast, and Boko Haram in the north-eastern part of the country have caused massive and wanton destruction of lives and property, including the destruction of crude oil installations, over the years. Furthermore, considerable research indicates that al-Qaeda has a presence in Mali and Mauritania, and that Al-Qaeda in the Islamic Maghreb (AQIM) has networks in Mali and Senegal, while Hezbollah has a large fundraising network in West Africa. Financing terrorist operations is becoming easier due to the increasing prevalence of criminality—monumental corruption, oil theft, increased arms trafficking, people trafficking, frauds, cybercrime, drug trafficking, and many other types of crime. The study applies descriptive analysis of data. Data were collected from primary and secondary sources through unstructured interviews, books, journal and the internet. The research findings revealed that the Nigerian Financial Intelligence Unit (NFIU) and other agencies have not adequately implemented cybersecurity to disrupt terrorism financing due to an inadequate legal framework. Also, the NFIU and other agencies are faced with inability to control the activities of other intelligence agencies involved in intelligence acquisition and this often results in unhealthy inter-agency competition and rivalry. This weak synergy culminates in negative consequences which are ultimately counterproductive on national security objectives. Despite these shortcomings, there are prospects for improving cybersecurity as a strategy to disrupt terrorism financing in Training of NFIU personnel on the operations and use of GIABA framework for Anti-Terrorism Financing and Money Laundering and cyber security. On the whole, the study provides insight on the overall issue of cybersecurity as a strategy to disrupt emerging trends in terrorism financing and provided implementation plan for effective cybersecurity application to disrupt terrorism financing.

Key Words: Cyber Security, Financial Intelligence Unit, GIABA, Terrorism Financing

Introduction

Since the mid-1980s, most countries around the world have agreed that they need a modern plan to stop Money Laundering and Terrorism Financing (ML/TF). This trend can be seen as starting with the negotiations for the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. This was because of the realization that taking away the money that criminals make from their crimes is an important way to stop drug trafficking, terrorism and other serious trans-border crimes.

Terrorism Financing (TF) includes using cash to finance terrorism through donations from the public and the support provided using legitimate sources of income for businessmen who belong to or are loyal to terrorist groups. The finance derived by terrorist groups is used to execute terrorist operations in their name. (Esoimeme, 2017) The channels commonly used for terrorist financing are funds transfers through financial institutions (banks), Money Value Transfer Systems (MVTS) and physical transportation of cash. These funds are used to buy explosives, arms and the like. In addition, the funds raised are mainly disbursed to finance domestic terrorist events and provide terrorists with all the resources they need. A critical means of fighting terrorism financing has been identified as cyber security. Access to funds and financial services for persons that the government classifies as terrorists is

limited by a collection of laws, regulations, and other procedures known as Combating the Financing of Terrorism (CFT).

For instance, the International Monetary Fund (IMF) is worried about the effects of terrorist financing and money laundering on the economy of its member countries. Increased volatility in international capital flows and a chilling effect on foreign direct investment are only two of the potential negative outcomes. (IMF, 2020) Egypt pursues several Terrorism Financing (TF) disruption patterns, including the collection, movement and use of funds. It cooperates with several local and external entities to identify and investigate TF cases, whether independently or as part of its investigations of terrorist cases. The sanctions applied for the commission of a TF offense are considered proportionate and dissuasive. (Kumar, 2020)

In Nigeria for example, terrorist activities continue to threaten the cooperate existence of the country. The Islamic State in West African Province (ISWAP), Boko Haram (BH), Yan Bindiga and Yan Tadda are the most dangerous terrorist groups that operate and mostly active in the Northern part of Nigeria, while the Indigenous People of Biafra (IPOB) is mostly active in the South Eastern part of Nigeria. There are a number of factors that help these terrorist groups to operate in their most active regions; these includes porous borders and difficult terrain, the trafficking of arms and weapons, the presence of illegal mining, poverty, unemployment, and extreme inequality.

However, Terrorism Financing (TF) is a major way that the groups have funded their criminal activities. These groups have kept taking advantage of the gaps near Nigeria's borders with Cameroon, Niger Republic, and Chad. In these border towns, illegal activities related to terrorism and funding for terrorism continue to happen across the border. (Kumar, 2020). This calls for the need to re-examine the way cyber security is used to address the challenge of terrorism financing in Nigeria. The purpose of this study is to examine cybersecurity as a strategy to disrupt terrorism financing and eradicated .

CONCEPTUAL CLARIFICATION

In this section, some of the concepts are hereby reviewed to enable a clearer understanding of the specific concepts. The concepts clarified include Cyber Security, Terrorism Financing (TF) and Financial Intelligence unit (FIU)

Cyber Security

There has been an increase in the number of data breaches each year as the global cyber threat evolves. An alarming 7.9 billion records were compromised by data breaches in the first nine months of 2019, according to a report from Risk Based Security. When compared to the amount of records that were compromised at the same time in 2018, this number is 112% higher. Most instances were caused by malicious criminals, and the most affected industries were healthcare, retail, and government. Cybercriminals find particular value in the banking and healthcare industries, but any company with an online presence is vulnerable to theft of client information, corporate sabotage, and customer attacks. (Schneider, 2021)

As the cyber threat grows, countries around the world are investing more money on cybersecurity measures. Spending on cybersecurity is expected to hit $188.3 billion in 2023 and more than $260 billion worldwide by 2026, according to research firm Gartner. Governments around the world have issued recommendations to businesses in response to the growing cyber threat. (Keesoony, 2016)

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing. Cybersecurity is the practice of defending information technology infrastructures such as computers, servers, mobile devices, electronic systems, networks, and data from intrusion. Cybersecurity can be broken down into two distinct categories: cyber and security. Systems, networks, programs, and data are all examples of cyber technology. Security is the study and practice of keeping computer systems, networks, applications, and data safe. Security in information technology or electronic information is known by a few other names. (Rider , Alexander, Bazley, & Bryant, 2021).

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks. With the scale of the cyber threat set to continue to rise, global spending on cybersecurity solutions is naturally increasing. Gartner (2022)

predicts cybersecurity spending to reach $188.3 billion in 2023 and surpass $260 billion globally by 2026. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices. (Rider, Alexander, Bazley, & Bryant, 2021)

Terrorism Financing (TF)

Terrorism is one of the main contemporary threats to international peace and security. Perpetrators of terrorist acts undermine human rights, fundamental freedoms and the rule of law, which are the pillars of national and international stability. In Nigeria, legal and regulatory efforts aimed at curbing terrorism and terrorist financing can be located within the Terrorism (Prevention) Act, 2011 (PTA, 2011).

The United Nations Security Council (UNSC) Counterterrorism Committee (CTC) notes that Terrorists require money to operate because without funding, they will be unable to procure weapons, equipment, supplies and services. The sources of funding may be licit or illicit and could be obtained from multiple small donations instead of one huge sum.

According to the Financial Action Task Force (FATF), Terrorist Financing (TF) is the financing of terrorist acts, and or terrorists and terrorist organizations. By implication, Terrorist Financing involves solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organization. It asserts that disrupting and preventing the terrorism-related financial flows and transactions is one of the most effective ways to fight terrorism.

The Prevention of Terrorism Act (PTA) defines the act of financing of terrorism as:- A person who, directly or indirectly, provided or collected funds with the intention or knowledge that they will be used, in full or in part, in order to: Commit an offence in breach of an enactment specified in the Schedule to this Act; or (b) Do any other act intended to cause death or serious bodily injury to a civilian or any other person not taking active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a group of people or to compel a government or an international organization to do or abstain from doing any act, commits an offence under this Act and shall on conviction be liable to imprisonment for a maximum term of 10 years. The FATF is the international standard setter on measures to combat Money Laundering and Terrorist Financing defines terrorist financing as "Extending to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorists act(s); (b) by a terrorist organization; or (c) by an individual terrorist. (Gartner, 2022)

Financial Intelligence Units (FIUs)

In their simplest form, FIUs are agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyze them, and disseminate the resulting intelligence to local law-enforcement agencies and foreign FIUs to combat money laundering (IMF/WB, 2004). The creation of these specialized law enforcement agencies should be seen against the background of the larger phenomenon of an increasing proliferation of law enforcement agencies (Stessens, 2003). The first few FIUs were established in the early 1990s (IMF/WB, 2004). As at the end of July 2010 there were 121 FIUs (Egmont Group, 2010). This is an incredible achievement, given that 35 FIUs attended the July 1997 Egmont Group held in Madrid, Spain (Egmont Group, 2004a). The Egmont Group Chairperson for the 2009-2010 period, Mr Luis Urrutia, who is also the Director of the FIU in Mexico, in recognition of this achievement, opined that very few international initiatives have been able to take a diverse body of government entities (FIUs) and mature to form a global network of over 120 members strongly committed to exchanging sensitive information that would otherwise not be available to combat crime at a national level (Egmont Group, 2010).

MONEY LAUNDERING AND TERRORISM FINANCING IN NIGERIA (ML/TF)

Funding is required for individual terrorist operations as well as to cover the larger organizational expenses of establishing, sustaining, and providing an enabling environment for terrorist activities (Attah, 2019; OECD, 2019). Terrorists fund their operations in a variety of ways. Terrorism, for example, is funded through commerce and other lucrative operations. Non-governmental organizations (NGOs), consultancy businesses, and charitable groups also contribute to its funding (Teichmann, 2019). Terrorism is also funded by other crimes such as money laundering, smuggling, abduction for ransom, drug trafficking, and other similar activities (Okoli, 2019). Terrorism is reportedly sponsored in Nigeria by politically exposed individuals such as Ali Modu Sherrif, the former Governor and Senator of Borno State, who

has been identified as a funder of Boko Haram (Thurston, 2016). The aforementioned terrorist funding tactics and strategies are typically employed in Nigeria through tax evasion, money laundering, and cross-border cash smuggling via bureau de change and other cash couriers (Maza et al., 2020; Nelson, 2019; FATF and GIABA, 2019). Security personnel, in particular, recovered substantial quantities of money from Boko Haram couriers in Burkina Faso, Chad, and along the Nigeria-Niger border (FATF and GIABA, 2018). The monies confiscated from Boko Haram operators by security agents might have been the profits of money laundering and ransom payments. Detecting and shutting off terrorists' financial sources is a vital step in dismantling their unlawful operations (Attah, 2019). Apprehending, investigating, and prosecuting terrorist financiers, as well as collecting and seizing terrorist assets, will discourage perpetrators of money laundering and terrorism (FATF and GIABA, 2019).

The procedures used to launder money are substantially the same as those used to disguise terrorist funding sources (Schott, 2020). Nonetheless, funding used to assist terrorism may come from legitimate sources, criminal operations, or both (FATF and GIABA, 2013). If the source of the cash is hidden, the monies are still available for future terrorist funding actions. As a result, terrorists must disguise the source and use of funds in order for terrorist funding activities to go undetected (Schott, 2019).

The Scope of Money Laundering and Terrorism Financing (ML/TF)

There are various scopes through which terrorist's carryout their activities of ML/TF. According to the NFIU, some of the scopes is extensive and well organised that requires adequate responses from government. The specific scopes of ML/TF are as follows:

a. Use of Foreign Terrorist Fighters (FTF)

Information gathered about FTFs is often of a highly confidential nature and its classification makes information sharing challenging. Data held by FIUs needs to be combined with contextual and de-sensitized information from operational and intelligence authorities, and the private sector entities, to provide a full picture of FTF activity. (Morrow, 1994) Some of the ways the FTF is carried out is through

- Self-funding by Individuals
    - Funding by Recruitment/Facilitation Networks

b. Fund Raising through Social Media and Crowd-funding

Often, it is not possible to distinguish between the sympathizers, supporters and actual terrorists. It is also difficult to get evidence of the use of funds when transferred via the Internet. Social networks are used to show the relationships, but finding proof of TF is still difficult. Identification of persons contributing money is challenging. Some of the means this is carried out is through:

- Social Networks (such as Facebook, Twitter and Instagram)
- Mobile Apps for Communication (such as WhatsApp and Viber)
- Secure Communications Networks (such as Surespot and VoIP). (Martin, 2021)

c. New Payment of Products and Services (NPPS)

Rapid development, increased functionality, and growing use of New Payment Products and Services (NPPS) globally have created Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) challenges for Law Enforcement Agencies and Competent Authorities globally and specifically in Countries in West African Sub-region and private sector. Some of the means this is carried out is through:

- Virtual Currencies
- Prepaid Cards
- Internet-Based Payment Services

d. Exploitation of Natural Resources

The investigation of crimes associated with the natural resources sector, including TF-related investigations, are often complex and requires extensive financial analysis. It is often difficult to identify the entire criminal network and specific actors (including facilitators) who are committing these crimes. However, using mining of minerals such as gold especially in areas in Niger state and Zamfara have been identified as strategies that terrorists use to finance their activities.

THE ROLE OF NIGERIAN FINANCIAL INTELLIGENCE UNIT (NFIU) IN COMBATING TERRORISM FINANCING: 2005-2021

As mentioned earlier, Financial Intelligence (FIUs) are agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyse them, and disseminate the resulting intelligence to local law-enforcement agencies and foreign FIUs to combat money laundering (IMF/WB, 2004)

The Nigerian Financial Intelligence Unit (NFIU) is the central national agency in Nigeria responsible for the receipt and analysis of financial disclosures and dissemination of intelligence generated to competent authorities. The Unit was established in June 2004 and became operational in January, 2005. The NFIU is domiciled in the Economic and Financial Crimes Commission (EFCC) as an autonomously operational unit. (Jubrin, 2021)

In 2015 the Attorney General of the Federation and Minister of Justice, pursuant to his powers under Section 43 of the EFCC Act, ML(P)A 2011 (as amended) issued the NFIU Regulation of 2015 which clearly outlined the powers, operational autonomy and governance structure of the NFIU. The Unit is the Secretariat to the Nigerian Sanction Committee, the Inter Ministerial Committee on AML/CFT and the National Risk Assessment. (Innocent, 2021) The NFIU is headed by a director and six departmental heads. The NFIU receives funding through the EFCC's appropriation and has received support from international and domestic partners particularly the Inter- Governmental Action Body Against Money Laundering in West Africa (GIABA), International Monetary Fund (IMF), United Nations Office on Drugs and Crimes (UNODC), the American Embassy in Nigeria and the Department For International Development/Justice For All (DFID/J4A) in the area of technical assistance on operational restructuring, capacity building and strategic planning implementation measures. (Jumare, 2021; Isiaka, 2017)

The core functions of the NFIU are as follows:

1. Receipt of suspicious transaction reports from reporting entities including financial institutions and designated non-financial businesses and professionals.
2. Receipt of threshold-based transaction reports from reporting entities
3. Analysis of the received information, including connecting and accessing local and international databases to enrich the reports
4. Dissemination of the resulting intelligence reports to law enforcement, anti-corruption, security, intelligence agencies as well as regulatory and supervisory bodies for further investigation and prosecution.

Given adequate tools and capacity, the NFIU is a good prospect for cybersecurity as a strategy to disrupt emerging trends in TF. The NFIU is staffed with personnel from diverse academic backgrounds ranging from accounting, insurance, economics, international relations, education, Statistics to state but a few. The Unit uses a secure Suspicious Transaction Reports (STR) reporting platform called the Global Anti Money Laundering (goAML) application. The goAML is an online secured reporting platform used for electronic reporting of large number of transactions by Reporting Entities (REs) with large number of records. (Hatlebrekke & Smith, 2020) Other REs use the web reporting portal available at the NFIU website to file single reports.

NFIU analysts carry out effective analyses of the reports received from the reporting entities. The capacity to carry out this function is further enriched by the regular tactical and strategic analysis trainings received. In 2012, the IMF/World Bank provided tactical and strategic analysis training to the NFIU analysts while in 2014, officers of the NFIU underwent training on insurance and capital market operations conducted by resource persons from the National Insurance Commission (NAICOM) and Securities and Exchange Commission (SEC) respectively. (Magoro, 2021)

Additionally, the NFIU is a member of the Egmont Group of FIUs and has access to their online secured platform for making and receiving requests from over 150-member countries. The NFIU further has access to a wide range of domestic databases which it leverages upon in its intelligence analyses, categories of which include; company registry, tax, land registry, financial transactions, national identity database e.t.c. The NFIU also receives reports of Currency Declaration Reports (CDR) for the Nigeria Customs Service (NCS). (Jones, 2020)

The NFIU is tasked with applying the provisions of the Nigerian Terrorism (Prevention) (Amendment) Act 2013. The Act specifically prohibits all acts of

terrorism and the financing of terrorism (Section 1 (1)). The emphasis placed on the financing of terrorism has been informed by the key role finance plays in terrorism. Terrorists need money to carry out their activities, including 'money to finance training, recruit members, support global travel, support and sustain global communications, purchase instruments of terror (including biochemical and other weapons of mass destruction), and sustain and support terrorist cells' (Gurule 2004: 114). Thus, cutting off the source of terror finance inhibits the capacity of terror groups to carry out terror attacks. It is in recognition of this that Section 13 specifically criminalises the provision of funds for terror groups by providing that any person or entity who, in or outside Nigeria: (i) solicits, acquires, provides, collects, receives, possesses or makes available funds, property or other services by any means to either terrorists 5 groups, directly or indirectly with the intention or knowledge or having reasonable grounds to believe that such funds or property will be used in full or in part in order to commit an offence under this Act or in breach of the provisions of this Act; (ii) possesses funds intending that they be used or knowing that they will be used, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act by terrorist or terrorist groups, commits an offence under this Act and is liable on conviction to imprisonment for life.

Section 13 of the Nigerian Terrorism (Prevention) (Amendment) Act, is in line with the provisions of the 1999 United Nations Convention for the Suppression of the Financing of Terrorism. The Convention also enjoined state parties to not only criminalise the financing of terrorism but to also provide for the forfeiture of funds provided or collected for terrorist purposes by adopting measures to discourage such financing and punish perpetrators.

The NFIU is also responsible for adopting the GIABA framework for its activities. The Economic Community of West African States (ECOWAS) Authority of Heads of State and Government formed the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) on December 10, 1999. At its establishment, the primary goal of GIABA was to defend West African economies and financial systems against money laundering. Following the terrorist attacks on the United States of America on September 11, 2002, the GIABA Statutes were updated in January 2006 to reflect the developing relationship between Money Laundering and Terrorist Financing. This is why Counter-Terrorism Financing was added to GIABA's mandate. So, in addition to reflecting the Authority of ECOWAS Heads of State and Government's determination to combat ML and TF, GIABA is also a Financial Action Task Force-Style Regional Body (FSRB).

Challenges and Prospects of NFIU in Combating ML/TF

There are a number of challenges hindering the NFIU from effectively achieving the objective of addressing the issue of ML/TF, these issues are explained below:

Institutional Bureaucracy: bureaucracy slows the process of decision making in the NFIU, as there are several levels of clearance before an intelligence can be utilized in the cases where TF is discovered. Institutional bureaucracy and organizational culture of intelligence sharing by the NFIU and other agencies to fight TF shape their techniques, practices and abilities to collaborate. These agencies such as NFIU, Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and other related Offences (ICPC) The Department of Intelligence Agency (DIA), Department of State Security (DSS) and National Intelligence Agency (NIA) have different terms of reference that makes coordination challenging. This is as a result of inter-agency rivalry and the absence of trust. This has prompted undermining alignment with national prerequisite.

Poor Technological Capability: Nigeria continues to grapple with the challenge of poor technological capability and this affect the activities of NFIU. Yet, in the 21st Century, technology has turned out to be a critical component in intelligence process. Technology has the capacity to assist the NFIU to drive proper collection, processing, dissemination and sharing of intelligence. Svendsen contend that in the domain of intelligence sharing, growing emphasis is set on technology (Svendsen, 2010). This is as a result of the fact that Information Communication Technology (ICT) permits effectual accumulation and sharing of information for cybersecurity which can be used to curb TF.

Poor Human Capacity: Human Capacity in can be described as the ability of personnel who are expected to drive intelligence agencies such as the NFIU in order to accomplish their set goals and objectives. In order to achieve addressing the challenge of TF, it is important to have human resources which have the required skills to perform. (Anderson 2021) In many cases, the information that

is been acquired from other agencies, is needed in order to be analyzed by specialized analysts. However, in many cases, the NFIU lack adequate human capacity to carry out such analysis thereby hindering their efficiency. This implies there is a need for analysts and operatives with the required ability and professionalism. Therefore, in order to be able to address the challenge of TF, it is paramount to have human resources with the adequate skill in both analysis and operations.

Conclusion

Money Laundering and Terrorism Financing (ML/TF) poses serious risk to national security as terrorists use finance to enable their activities. In Nigeria, legal and regulatory efforts aimed at curbing terrorism and terrorist financing can be located within the Terrorism (Prevention) Act, 2011 (PTA, 2011). The Nigerian Financial Intelligent Unit (NFIU) have been saddled with the responsibility of intercepting ML/TF and to a considerable extent their activities have enhanced the potential of Nigeria to address the issue of ML/TF. However, the agency is confronted with numerous challenges such as poor human capacity, institutional bureaucracy among others. Some critical steps that can be taken to harness the potentials of the NFIU include the training of NFIU and related agencies such as EFCC and ICPC on existing and emergent Anti-Terrorism Financing and Money Laundering and cyber security strategies. There is a need for the training of NFIU personnel on the operations and use of GIABA framework for Anti-Terrorism Financing and Money Laundering and cyber security. There is a need for employment of local and international Researchers to boost manpower on cybersecurity.

REFERENCES

Adomako N., Mohammed E., Kshteri K. (2018) "China's central bank will regulate virtual currency", 13 January, available at: www.world-check.com/articles/2007/01/13/chinas-central-bank-will-regulate-virtualcurrency/ (accessed 15 June 2023).

Attah N. (2019) "Terrorist financing", Financial Transactions and Reports Analysis Centre of Canada, available at: www.fintrac.gc.ca/multimedia/education/c1/1-5-eng.asp (accessed 9 October 2022).

Egmont Group (2004) Money laundering and terrorism financing in virtual environments: a feasibility study. Journal of Money Laundering Control 17:1, 50-75.

Emmanuel, I.A. (2021). Protecting Nigeria's Critical Infrastructure: The Role of the SSS. Abuja: Triple S, A Publication of the SSS, No. 7 2021.

Engen A. (2020) Are the financial transactions conducted inside virtual environments truly anonymous?. Journal of Money Laundering Control 16:1, 6-40

Esoimeme E (2017) A critical analysis of the effects of the central Bank of Nigeria on money laundering control Journal of Money Laundering Control 5(3) 15-23

FAFT-GIABA-GABAC (2016) "Will 5 new unregulated virtual banks become money laundering centres?", 12 January, available at: www.world-check.com/articles/2007/01/11/will-5-newunregulated-virtual-banks-become-money-/ (accessed 15 June 2023).

Gartner, K (2022) Walking the walk: practical measures to undermine the business of organised crime. Journal of Financial Crime 22:2, 199-207.

Gurule G. (2004) Institutionalization of risk management framework in Islamic NGOs for suppressing terrorism financing. Journal of Money Laundering Control 17:1, 96-109.

Hatlebrekke K.A. and M.L.R Smith (2020). Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure, Intelligence and National Security, Vol.25 No.2, 2020, p.158.

International Monetary Fund (IMF) (2020) The fight against Money laundering and terrorism https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism

Jubrin, A.T. (2021). Former Director of Military Intelligence, interviewed on "Intelligence Sharing and Internal Security in Nigeria", 6 Apr 14.

Jummare, M.M. (2021). Issues and Problems in Nigeria Defence Policy. Nigerian Army Journal, Vol. 8, p. 63.

Karambu F. (2021) Special Recommendations (SR) on Terrorist Financing (TF), available at: www.fatf-gafi.org/document/9/0,3746,en_32250379_32236920_3403207 (accessed 20 May 2023).

Kumar, V.A. (2020) Money laundering concept, significance and its impact. European Journal of Business and Management, 2, 113-119.

Magoro, M. (2021). Chairman, Senate Committee on Intelligence and National Security, National Assembly, interviewed on "Intelligence Sharing and Internal Security", at National Assembly Complex Abuja on 17 Mar 14.

Makarenko, T. (2020). Terrorist Threat to Energy Infrastructure Increases. Retrieved from <http://bdi.mfa.government.bg/info/Module%2004%20Diplomacia%20i%20sigurnost/dopalnitelna%20literatura/energy%20terrorism.pdf >

Martin, R. (2021). Overview of Organized Crime in Germany, A brief delivered to Participants of Team 1, EIMC 6, at the BKA office, Berlin, 2021

OECD (2019) "Identifying and disrupting funding streams to thwart terrorist financing and organized criminal operation", available at: www.ipsaintl.com/newsand-events/articles/pdf/lormel-identifying-and-disrupting-funding.pdf (accessed 15 June 2023).

Okoli F. and Okpaleke U. (2014) "Global money laundering & terrorist financing threat assessment", available at: www.fatf-gafi.org/dataoecd/48/10/45724350.pdf (accessed 15 June 2023).

Okoli P. (2019) "Organised crime groups in cyberspace: a typology", Trends in Organized Crime, Vol. 11 No. 3, pp. 270-95.

Shulsky, A. and Schmitt, G. (2020). Silent Warfare: Understanding the World of Intelligence. Third Edition. Brassey's: Washington, D.C.

Stessens N. (2003) Malaysian DNFBPs' Perceptions on Awareness, Perceived Impact and Views on the AML/CFT Requirements. Procedia Economics and Finance 31, 595-600.

Svendsen, A. (2020). Connecting Intelligence and Theory: Intelligence Liaison and International Relations. Intelligence and National Security, Vol 24. P.724

Svendsen, A. (2020). Intelligence Cooperation and the War on Terror: Anglo-American Security Relations After 9/11", Intelligence and National Security, Vol. 25 No 4, 2020 p. 715.

Teichmann FMJ, (2019) "Department of Justice launches new law enforcement strategy to combat increasing threat of international organized crime", available at: www.justice.gov/opa/pr/2008/April/08-opa-330.html (accessed 16 June 2023).

Terrorism Prevention Act (2011) Laws of the Federal Republic of Nigeria https://docs.iza.org/dp4860.pdf

Thurston S. (2016) "Money laundering and the financing of terrorism", Financial Supervision Commission, available at: www.fsc.gov.im/aml/ (accessed 9 May 2023).

World Bank (2017) Reference Guide to Anti-money Laundering and Combating the Financing of Terror, Terrorism Financing, International Monetary Fund, Washington, DC.