OPEN ACCESS
Vol. 8, No. 2, Oktober, 2020
Page. 55-66
DOI: https://doi.org/10.21107/jaffa.v8i2.8350

JOURNAL OF AUDITING, FINANCE, AND FORENSIC ACCOUNTING
E-ISSN: 2461-0607 ISSN: 2339-2886
https://journal.trunojoyo.ac.id/jaffa

Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria

[1]Toyin Emmanuel Olatunji*; [2]Akinola Michael Aruwaji
[12]Department of Accounting, Ladoke Akintola University of Technology, Nigeria

Article Info:
Received: 21 August 2020
in revised form: 05 October 2020
Accepted: 21 October 2020
Available Online: 28 October 2020

Keywords:
Terrorist financing, forensic accounting, financial cybercrime, cryptocurrency

Corresponding Author*:
*Email: macfarade@gmail.com

Abstract; *This paper aims to examine forensic accounting (FA) investigation in tracking financial cybercrime (FC) and terrorist financing (TF) in Nigeria. It also verifies the associations between cyber criminality and terrorist financing. The sample composed of all Nigeria anti-graft agencies including the Nigeria Communication Commission (NCC). A quantitative method is used in a way to analyze the data. The results of the hypotheses revealed that forensic accounting has significant influence in disclosing the associations between financial cybercrime and terrorist financing. This study finds forensic accounting as a tool and deterrence to terrorist financing and associated crimes activities. The implications of this study emphasized that the government should strengthen enforcement on cybercrimes and provides security infrastructure (advanced technology) in tackling the precedence of financial cybercrime and terrorist financing in Nigeria.*

Abstrak; Makalah ini bertujuan untuk menguji investigasi akuntansi forensik (FA) dalam melacak kejahatan keuangan (FC) dan pendanaan teroris (TF) di Nigeria dan memverifikasi hubungan antara kejahatan dunia maya dan pendanaan teroris. Sampel terdiri dari semua lembaga anti-korupsi Nigeria termasuk Komisi Komunikasi Nigeria (NCC). Metode kuantitatif digunakan untuk menganalisis data. Hasil hipotesis mengungkapkan bahwa akuntansi forensik memiliki pengaruh yang signifikan dalam mengungkapkan hubungan antara financial cybercrime dan pendanaan teroris. Studi ini menemukan bahwa akuntansi forensik sebagai alat pencegahan pendanaan teroris dan aktivitas kejahatan terkait. Implikasi dari penelitian ini menekankan bahwa pemerintah harus memperkuat penegakan kejahatan dunia maya dan menyediakan infrastruktur keamanan (teknologi mutakhir) dalam menanggulangi kejahatan keuangan dan pendanaan terorisme di Nigeria.

INTRODUCTION

Terrorist embraced cyberspace as a vital opportunity and open source information tools for effective communication among cells. Terrorist organizations fund their activities by engaging in the traditional method of cyber criminalities, such as credit card fraud and intellectual property theft. In 2007, Younes Tsouli, Tariqal Daour and Maseem Mughal were charged for inciting murder, they used cyberspace to commit this menace. These terrorists used stolen credit card information to purchase goods, airplane tickets, and prepaid mobile phone cards to provide direct tactical support for terrorist operations. Therefore, the foremost objective of this study is to measure the attribution of forensic accounting techniques in breaking the nexus between cybercrime activities and terrorist financing in Nigeria. Other objectives are to investigate the effects of forensic accounting on cybercrime that linked with terrorist financing. Also, to determine the effect of forensic accounting on financial cybercrime.

Counter-Terrorism Implementation Task Force (CTITF, 2009) emphasized that terrorist organizations also used the internet in conducting their plans to raise funds, propagated their secured information. In Nigeria, terrorist organizations used cyberspace as a mechanism to extend their networks without boundaries including recruitment, financing, inducement, training, planning including secret communication and open-source information, radicalization and incitement of terrorist and execution of cyber-attacks. Bologna and Lindquistn (1987) described forensic accounting and investigation as the application of financial skills and investigative mentality to unresolved issues, conducted within the context of the rules of evidence. As a discipline, it encompasses financial expertise, fraud knowledge, and a strong understanding of business reality and legal system. Nir (2010a,b) defined cybercrime as a criminal activity in which computers or electronic gadgets are the principal tools of committing an offence or violating laws, rules or regulations. Cybercrime includes denial of service attacks (hacking), cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, identity fraud, cyber terrorism, and cyber extortions.

Terrorist organizations used cybercrime extensively to corroborate their vast network which is spread across the globe. Terrorist financing activities in cyberspace possesses all of these typical characteristics of benign forms of cybercrime, they are virtually untraceable, easy to conceal in the huge ungoverned spaces of the internet and they are accessible to a wide variety of criminals possessing technology which has now become readily available, such as keylogging software for identity theft. The link between terrorism and cybercrime, for instance, enable terrorists to gain swift and easy access to fraudulently obtained financial resources (currency sellers and unlicensed money transmitters) which require some sophisticated technology (Bilbeisi & Brown, 2015). It also serves as conduits for money laundering, allowing terrorists to by-pass traditional financial institutions policies to finance their activities. Thus, terrorism has extended the fields of battle from physical space to cyberspace (James, 2018). Krancher (2010) integrated fraud and diamond theories into terrorism triangle theory, explaining that fraud is the fundamental components of terror.

This theory focuses on the elements of fraud with more development, emplacing that terrorist activities exist only under the conditions of opportunity, ideological motivation (versus pressure), and ideological rationalization. Perhaps, terrorist seek for a save heaven for protection and attack, they utilize digitalism infrastructure for planning, pathways and implementations of terrorism. Jaishankar (2008) stated space transition as a virtual space that provides an individual with free space where an act of terror can be an outrage against anyone. The result of this study provides evidence that terrorists indeed use virtual space to do fund-raising and to perform financial cybercrime. The implications of this study emphasized that the government should strengthen enforcement on cybercrimes and provides security infrastructure (advanced technology) in tackling the precedence of financial cybercrime and terrorist financing in Nigeria.

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Forensic accounting and the links between cybercrimes and terrorist financing

The literature review highlighted a link between the terrorist group and organized crime. There are many types of tactical and strategic relationships between cybercrime and terrorist financing. Asogwa (2014), Madan (2013) and Krancher (2010) explained the concept of forensic accounting education and its application on fraud and organized crimes; existing literature (Bilbeisi & Brown, 2015) relates forensic accounting with cybercrime and terrorist financing. In an extension to available literature, this study purview the extent of forensic accounting investigation on cybercrime and terrorist financing as a gap to fill for literature. FATF Report (2013), stated that there is an emerging nexus between terrorist financing and trade-in that there is an increased likelihood of terrorist financiers using fraudulent trade-based practices to collect, transfer, and utilize funds and assets as well as the increasing reliance on trade-based money laundering by terrorist financiers.

Similarly, FATF (2013), notes the potential exploitation of the international trade system by terrorist financiers and criminal organizations by generating vast sums of money through false invoicing of imports, exports and cybercrime. The Organization for Economic Co-operation and Development (OECD) emphasized that Financial crimes, money laundering, and terrorist financing including tax evasion, destabilize and influences political and economic interests and pose a serious threat to national security (OECD, 2019). Levitt and Jacobson (2008), also attributed the evolution in financing sources to rapid globalization and sustained technological advances, which have enabled terrorist groups to raise, store, transfer, and distribute funds for their operations with ease. In particular, the advent of new technology has spurred changes in how money is transferred, with mobile and online money transfers becoming more commonplace. Dennis (2003), emphasized that in the early stages of the investigation of the event of September 11, 2001, it was the financial evidence that quickly established links between the hijackers and identified co-conspirators. Federal agents, law enforcement officials and forensic accountants have utilized financial investigative techniques for years to track criminals and solve crimes. However, the US Department of Homeland Security and Federal Bureau of Investigation (FBI) rely heavily on forensic accounting investigation techniques to combat terrorism by discovering and disrupting the funding that is critical to these extremists (UNODC, 2012).

Nexus between cybercrimes and terrorist financing

In this century, cybercrimes are being described as the drivers of organized crimes like terrorist financing. United Nation in 2001 prescribed that small criminal activities can provide terrorists with quick funds to purchase equipment and weapons. Criminals and terrorists have a great advantage through information and communication technologies to carry out crimes with minimal effort quickly generating funds from multiple small-value transactions, which could ultimately lead to the financing of terrorist organizations, individual terrorists and ultimately lead to a terrorist attack (FATF, 2013). There is a perception that most terrorism and cybercrime has a transnational link, however recent acts of terrorism have been characterized as locally grown, domestic or "lone-wolf" attacks. These attacks have become much harder to predict as they can be anyone, anywhere at any time and can be facilitated online through small terrorist cells (FBI, 2013). In 2011, a terrorist plot discovered in the English city of Birmingham. Rahin Ahmed dabbled in online trading, trading dollars and euros, raised through a fraud scheme, to raise money for a large scale terrorist attack on UK soil. His ability to engage in online forex trading illustrates the difficulty in detecting possible terrorist financing using conventional transaction monitoring. He was able to apply for an online account at Forex Capital Markets Ltd. by exaggerating his experience annual income and net worth. This highlights the importance of appropriate controls and the application of robust customer due to diligence procedures.

Cybercrime consists of the same financial frauds and scams we have known for years, they are just carried out by a more sophisticated type of criminal exploiting the internet and computers. There has been a large increase in the volume of cyber-attacks by organized criminal gangs and the lines between organized crime and terrorist financing are becoming blurred. It takes very little to finance a terrorist attack, for example, the UN estimated the total cost of the London bombings in 2005 was around $14,000 and Finance Minister Michel Sapin has reported the Paris attacks in November 2015 came to approximately $32,000. This contrasts with the larger scale attacks of 9/11 which were reported to have cost between $400,000 and $500,000 according to the final report of the National Commission on Terrorist Attacks. Financial Action Task Force (2013) reported that funds raised by members of Islamic State in connection with the Paris shootings in November of 2015 were raised by local criminals and have been partially linked to fraud schemes and other financial crimes. Reports indicate that money to finance the attacks was moved in tiny sums often using prepaid credit cards to pay for apartments, transport and weapons. It is important to note that as fraud begins to evolve into the cyber world by terrorists and criminals are evolving as well (FATF, 2001)

Theoretical framework

Albrecht (2003) stated that forensic accounting as a technique was developed to assist and evaluate accounting tools towards the conventional methodology of investigating fraud, those theories focused on fraud in the integration of financial crime; the differences on each of these theories open gaps of literature and framework for the forensic accounting techniques in investigating financial crime and tracking the financing routine of terrorist and activities of terrorism. This study embedded in criminological and sociological theories to explain cybercrime and terrorism. Terrorism Triangle Theory and Space Transition Theory were used to explore cybercrime and the basic composition of terrorist activities that eventually leads to terrorism.

Space transition theory

Virtual space provides an individual with such space where he can express his feelings and even vent out his outrage against anyone. Cyberstalking and cyber defamation are instances where offenders use online space because of its anonymity and widespread approach, it also argues that people behave differently when they move from one space to another. One of the important postulates of the theory is that People with repressed criminal behavior (in the physical space) have a propensity to commit a crime in cyberspace, which otherwise they would not commit in physical space due to their status and position (Jaishankar, 2008). Criminologist views the emergence of cyberspace as a new locus of criminal activity and therefore new theories are needed to explain the occurrence of cybercrime.

Terrorism triangle theory

This theory described that terrorist activities exist only under the conditions of opportunity, ideological motivation (versus pressure), and ideological rationalization. Inherently, the terrorist has the ideological motivation to inflict terror; likewise, most terrorist show little remorse and rationalize their activities based on their ideological beliefs, this observation is true not only for Al-Qaeda but also for Timothy McVeigh and Ted Kaczynski (the Unabomber). However, the opportunity may be the most important attribute for terrorist because without the opportunity to generate, move, and control cash flows, the financing of terrorism will not occur. (Krancher, 2010)

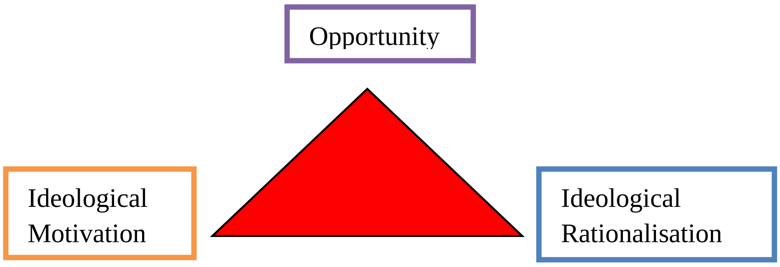

Figure 1 Terrorism triangle

These theories explain that modern and conventional method of fraud is a construct of defalcation, capital reduction, economic vitality and increases criminality behavior like terrorism. The combination of these theories hypothesized that forensic accounting investigation can expose the characteristics of fraud and elements of illegal financial transactions including money laundry, cybercrime and terrorist financing.

Hypotheses development

Many studies have investigated significance and relationship between forensic accounting and financial crimes. It was observed from the conclusions of these studies that forensic accounting investigations are related to reviews of financial crimes and more active in combating financial crime, but all of these scholars focused their intention on fraud. However, Bilbeisi and Brown (2015) linked forensic accounting, terrorism and terrorist financing. Bilbeisi and Brown (2015) used empirical research approaches to analyses the techniques and methods terrorists use to obtain funds for their operations. It concluded that technology improving and forensic accounting investigations will be a better approach in investigating terrorist financing, the findings were in line with the hypotheses of this study

H1: Forensic accounting investigation has a significant effect on financial cybercrime

H2: There is a relationship between forensic accounting, cyber criminality and terrorist financing

Conceptual framework

Forensic accounting techniques

Collin (2015) emphasized that digital forensic accounting techniques used many of the traditional methods like; interviews and interrogation, background research, confidential informants, undercover, laboratory analysis and analysis of transactions but increasingly exploit overabundance of electronic and physical surveillance, Computer Assisted Audit Techniques (CAATs) and/or other sophisticated tools and modern techniques such as Data Mining (big data), Full and-False Inclusion method, Genogram, Entity(s) Charts, Timeline Analysis, Link Analysis, Item Listing, (Modified) Net Worth Method, Source and Use of Cash Method, Proof-of-Cash Method, and Digital Analysis such as Duplicate Numbers Test (Rounded Numbers Test) and Benford's Techniques.

Computer Assisted Auditing Tools (CAATs)

Computer-assisted audit techniques are the method of using a computer to assist the auditor in the performance of the computer audit. In the report of Braun and Davis (2003), on CAATs techniques, it estimated that CAATs include many types of tools and techniques, such as utility software, test data, integrated test facility (ITF), parallel simulation, embedded audit module, and generalized audit software (GAS).

Benford's Law

It is a mathematical tool and is one of the various ways to determine whether variable under study is a case of unintentional errors (mistakes) or fraud. Nigrini (2012), showed that Benford's Law could be used in forensic accounting and auditing as an indicator of accounting and expenses fraud. In practice, applications of Benford's Law for fraud detection routinely use more than the first digit. Nigrini (2012), explained the limitation of using Benford's Law in detecting fraudulent and used to detect manipulation in a single annual or interim report. The general conclusions are that accounting numbers and financial data conform to Benford's Law.

Data Mining Techniques

It is a set of assisted techniques designed to automatically mine large volumes of data for new, hidden or unexpected information or patterns. Data mining techniques are categorized in three ways: Discovery, Predictive modelling and Deviation and Link analysis. It discovers the usual knowledge or patterns in data, without a predefined idea or hypothesis about what the pattern may be, i.e. without any prior knowledge of the fraud. It explains various affinities, association, trends and variations in the form of conditional logic. Sharma and Panigrahi (2012), highlighted the classification of data mining techniques for financial accounting fraud detection. They are; Neural Networks, Bayesian Belief Network, Decision Trees, Regression Models, Nearest Neighbour Method, Expert Systems, Fuzzy logic and Genetic Algorithm.

Ratio Analysis

Albrecht, Albrecht and Albrecht (2008), stated that ratio analysis involves calculating both traditional and non-traditional financial ratios, such as accruals to assets, asset quality, asset turnover, days sales in receivables, deferred charges to assets, depreciation, gross margin, increase in intangibles, inventory growth, leverage, operating performance margin, per cent uncollectible, sales growth, SGE expense, and working capital turnover. Since ratios standardize firms for size and other factors, one would expect firms within an industry to follow similar trends. Early studies use statistical techniques like probit and logistic regression, while later studies have branched out to neural networks, classification schemes, and rule ensembles. Studies that use both internal and external data have proven more successful, but the goal of most of the research is to use only externally available data for analysis (limiting the research to data available to most stakeholders).

Concept of cybercrime

Cybercrime is a postmodern method of financing terrorist and it also a modern method of financing terrorism. The concept explains the nexus between cybercrime and terrorist financing and also examine the components of cybercrime (codes and ciphers, data hiding, steganography, web-encryption).

Codes and Ciphers

Codes and Ciphers are where each word in a message is replaced with a code word or symbol, whereas a cipher is where each letter in a message is replaced with a cipher letter or symbol. Code is referring to ciphers. Ciphers are broken into two main categories; substitution ciphers and transposition ciphers. Substitution ciphers replace letters in the plaintext with other letters or symbols, keeping the order in which the symbols fall the same. Transposition ciphers keep all of the original letters but mix up their order. The resulting text of either enciphering method is called the cipher text. Terrorists depend so much on these techniques to communicate with their local cells (Gaines and Miller, 2004).

Data hiding

Data hiding (Techopedia, 2016) is a software development technique specifically used in Object-Oriented Programming (OOP) to hide internal object details (data members). Data hiding ensures exclusive data access to class members and protects object integrity by preventing unintended or intended changes. Data hiding also reduces system complexity for increased robustness by limiting interdependencies between software components, it's also known as data encapsulation or information hiding.

Steganography

Steganography is the practice where terrorists concealing messages or information within other non-secret text or data. Anderson and Petitcolas (2008) stated that steganography as the hiding of a message within another so that the presence of the hidden message is indiscernible. The key concept behind steganography is that the message to be transmitted is not detectable to the casual eye

Web-Encryption

Kessler (2006) stated that web- encryption is a security technology that scrambles digital information using specialist mathematics. It is only people in possession of a specific unlock key or password can read the encrypted information. Militant wired web links to jihad.

Terrorist financing

Terrorist financing is defined as a fund provides for terrorist activity, it may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as criminal sources (illegitimate) such as drug trade, smuggling of weapons and other goods, fraud, kidnapping and extortion. Two primary sources of terrorist financing are state sponsorship and revenue-generating from legitimate and illegitimate activities. Iran, Saudi Arabia, Syria, and others are often denoted as state sponsors of terrorism. Each of these countries, for differing reasons, awards resources to active terrorist organizations. Levitt and Jacobson (2008) emphasized that active state sponsorship is increasingly rare, states continue to provide terrorist groups with a tangible service by simply allowing terrorists to have access to their territory, facilitating their travel, or by turning a blind eye to their activities within their borders". Passas has noted that this can extend to minimal enforcement of oversight measures for financial transactions and charities. States can directly fund terrorist groups, supply them with weapons, or provide them with military training.

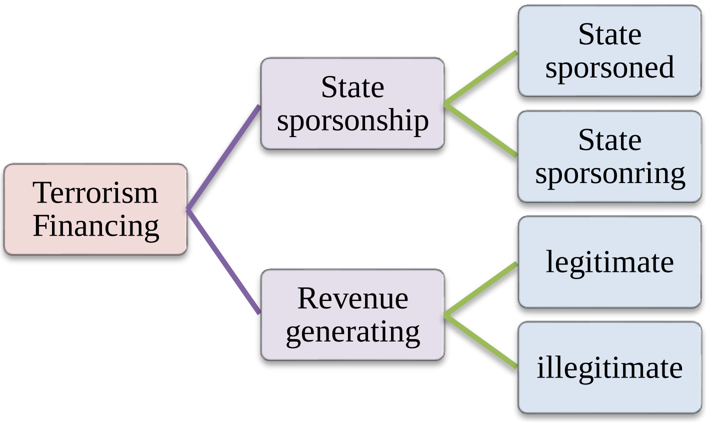

Figure 2 Source of terrorist financing

Hawala system

Financial Action Task Force (FATF, 2013) described the role of hawala and other similar service providers (HOSSPs) in money laundering and terrorist financing. HOSSPs are a subset of money or value transfer services which involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or another form to a beneficiary utilizing a communication, message, transfer, or through a clearing network to which the transfer provider belongs. Hawala has often been used as a "proxy" to provide a wide range of financial services to terrorist organizations. The transfer of money via a hawala banking system is extremely private and is unlikely to be reported or discovered by anyone other than the hawaladar's, the transferor and the transferee.

Cryptocurrency

Central Bank of Nigeria in 2012 defined cryptocurrency as a digital or virtual currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a national bank. Cryptocurrencies such as bitcoin now provide an outlet for personal wealth that is beyond restriction and confiscation. Terrorists used cryptocurrency as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages including information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Applications of cryptography include automated teller machine cards, computer passwords, and electronic commerce. Bitcoin is open-source; its design is public, no regulatory control on bitcoin and everyone can take part, this increased financial transactions of terrorists (OECD, 2019)

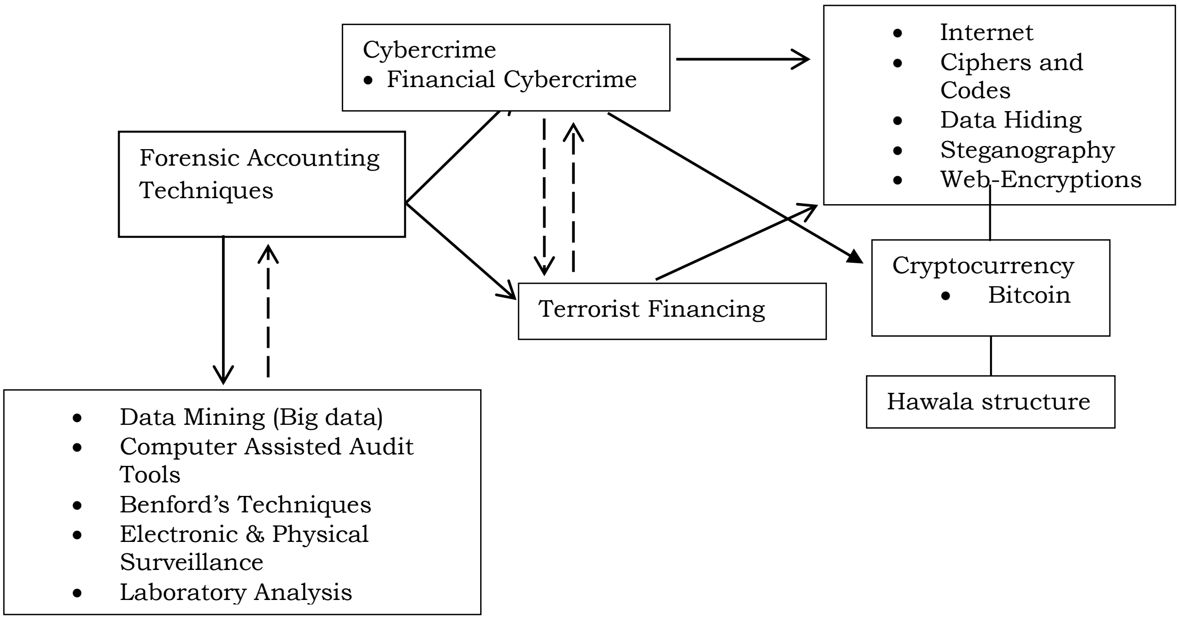

Figure 3 Conceptual framework of forensic accounting, financial cybercrime and terrorist financing.

RESEARCH METHODOLOGY

As it is a descriptive study, the main source of information is the primary data, the questionnaire was as an instrument to obtain the data. To measure the extent of forensic accounting techniques in tracking financial cybercrimes and terrorism financing in Nigeria, the content of the questionnaire was validated by various academic experts, the construct validity is assessed using convergent and discriminant validity, and measurement model is then finalized. Thirty questionnaires were administered cross selected agencies that use forensic accountants which are related to this study. The questionnaire was administered individually to each forensic accountant. The questionnaire used a five-point Likert scale with response opinions ranging from 1 (strongly disagree) to 5 (strongly agree). The methodology followed in this paper is almost similar to Madan (2013). The techniques used for analyzing data include descriptive, and regression analysis. The study used descriptive statistics to summarize the coefficient and the entire population while the regression model is used to measure the effect of forensic accounting on the investigation of cybercrimes and terrorist financing. The construct variables used for this study were operationalized and quantified by the content of the research questions. The construct variables were conceptualized in Table 1.

Table 1 Measurement summary

Construct	**Scale themes**	**Sources**
Forensic Accounting (FA)	Data Mining (Big data) Computer Assisted Audit Tools Benford's Techniques	Sharma and Panigrahi (2012) Braun and Davis (2003) Nigrini (2012)
Financial Cybercrime (FC)	Ciphers and Codes Data Hiding Steganography Web-Encryptions	Gaines and Miller (2004) Techopedia (2016) Anderson and Petitcolas (2008) Kessler (2006)
Terrorist Financing (TF)	Cryptocurrency Hawala structure	OECD, (2019) FATF (2013)

Sample size

The sample composed of all the forensic accountants working directly with the selected agencies because the total number of all the forensic accountant's personnel were used for this study. The related agencies are the Economic and Financial Crime Commission (EFCC), Nigeria Financial Intelligence Unit (NFIU), Nigeria Joint Task Force (NJTF) and Nigeria Communication Commission (NCC). Therefore, thirty (30) personnel were used as the total sample for this study.

Model Specification

FA = f (FC, TF) 30

FA = β0 + β1 FC + β2 TF + ε0

Where, the a priori expectation is β1, β2 >0, FA = Forensic Accounting, FC = Financial Cybercrime, TFI = Terrorist Financing, β0 = intercept/ autonomous variable. It depicts the degree of the need for forensic accounting even without the existence of cybercrime. β1 = coefficient of cybercrime investigation. It depicts the degree of the need for investigation of cybercrime by applying forensic accounting technique. β2 = coefficient of terrorist financing investigation. It depicts the degree of the need for investigation of terrorist financing using forensic accounting technique.

FINDINGS AND DISCUSSION

Descriptive analysis

Table II reports the descriptive statistics for dependent and independent variables used in this study. This descriptive describes the characteristics of the variables. The results revealed that Data Mining (Big data), Electronic and Physical Surveillance with satistics value (M= 2.0229, SD = 1.12550, Var = 1.267 and 1.7477, SD = .82898, Var = .687), shows that the variables are suitabe as a techniques for FA. Internet, Data Hiding, and Steganography with a statistical value (M =3.7706, SD = .78150 and Var = .611, M =2.0229, SD = 1.12550 and Var = 1.267, M = 1.5459, SD = .54325 and Var = .295) estimated that these variables are relevant to financial cybercrime. Hawaladar (M = 3.8805, SD = .88250 and Var = .673) was ranked above cryptocurrency (M = 2.7477 SD = .72898 Var = .688) for sponsoring terrorist. From Table I, the variables were ranked according to their sophistication to this study.

Table 2 Descriptive statistics

Descriptions	Mean (M)	Standard Deviation (SD)	Variance (V)	Rank (R)
Forensic Accounting (FA)				
1. Data Mining (Big data)	2.0229	1.12550	1.267	1
2. Computer Assisted Audit Tools	1.5459	.54325	.295	3
3. Benford's Techniques	1.3945	.52615	.277	4
4. Electronic & Physical Surveillance	1.7477	.82898	.687	2
Financial Cybercrime (FCC)				
5. Internet	3.7706	.78150	.611	1
6. Ciphers and Codes	1.1101	.31372	.098	5
7. Data Hiding	2.0229	1.12550	1.267	2
8. Steganography	1.5459	.54325	.295	3
9. Web-Encryptions	1.3945	.52615	.277	4
Terrorist Financing (TF)				
10. Bitcoin	2.7477	.72898	.688	2
11. Hawala structure	3.8805	.88250	.673	1

The regression model established that the application of forensic accounting techniques has a significant effect in investigating cybercrimes linked with terrorist financing. This result showed that forensic accounting techniques were appropriate in tracking cybercrime (β1 = 0.410). The model also estimated that the positive value of the coefficient (β2 = 0.445) revealed that forensic accounting techniques have a significant influence in investigating cybercrime and terrorism financing. The regression model revealed that p = 0.020 > 0.05 which estimated that forensic accounting techniques have a significant effect in breaking (detecting, preventing and tracking) the relationship between cyber criminality and terrorist financing. Kendall's correlation matrix model reported that there is a positive correlation between the two variables at 52% statistical significance level. The result further stated that forensic accounting is appropriate in investigating financial cybercrime and terrorist financing.

Table 3 Summary of regression analyses for the tested hypothesis

Variables	β_0	β_1	β_2	F	R^2	P-value	Comment
Cybercrime Reduction	2.998	0.410	0.445	6.280	0.307	0.020	Sig.

Tabel 4 Kendall's correlation matrix of the among forensic accounting, cybercrime and terrorism financing

Variables	Forensic accounting techniques	Cybercrime associated with terrorism financing
Forensic accounting techniques	1	0.52
Cybercrime linked with terrorist financing	0.52	1

Note: level of Significance 0.05

In table V below, the summary statistics of the analyses of the forensic accounting on cybercrime and terrorist financing showed the correlation coefficient (R = 0.685), coefficient of determination (R2 = 0.418) and standard error (0.32186), these indicated that forensic accounting contributes 41.8% in exposing cybercrime and terrorist financing at 95% confidence interval. Analysis of Variance ((F (2, 41) = 92.091; P= 0.001)) disclosed that forensic accounting techniques contributed significantly to investigating the menace of cybercrime activities and terrorist financing. The value of Durbin-Watson (0.538) showed that no auto-correlation within the variables.

Table 5 Model Summary

Model	R	R Square	Adjusted R	Std. Error of the Estimate	Durbin-Watson
1	.685a	.418	.510	.32186	.538

a. Predictors: (Constant), Forensic Accounting

b. Dependent Variable: Fraud detection and prevention

Tabel 6 Analysis of Variance (ANOVA) for the relationship between the two variables

Variable Source	Sum of squares	Mean Squares	Calculated Value of T	Level of Significance
Regression	17.459	17.459	92.091	.001^b
Error	11.869	.188		
Total	29.328			

a. Dependent Variable: Cybercrime and Terrorism Financing

b. Predictors: (Constant), Forensic Accounting

In table VI, the regression model estimated that forensic accounting (β = 0.885; t = 9.943; P<.05) has a positive significant influence on breaking the nexus between cybercrime and terrorist financing. This implies that if forensic accounting techniques were appropriately applied, it will reduce financial cybercrime.

Table 7 Regression equation coefficients

	Non-Standardized Coefficient		Standardized Coefficient		
Model	Beta	Std. Error	Beta	Coefficient	Significance
Fixed	1.335	0.429		4.352	.001
Forensic accounting	0.84	0.86	0.885	9.943	.000

a. Dependent Variable: Cybercrime and Terrorism Financing
b. Predictors: (Constant), Forensic Accounting

Discussion

Descriptive statistics result in purview the characteristics of the variables from the result of Table II, data mining, electronic and physical surveillance appears to be most relevant techniques of forensic accounting investigations in dealing with financial cybercrime and terrorist financing. The mean value proved that the two variables are suitable than other variables; Benford's techniques, electronic and physical surveillance with mean value respectively. For financial cybercrime; the mean value showed that internet, data hiding, steganography and web-encryptions posed more effect than ciphers and codes to debug financial crime. Furthermore, Table I summarizes the basic statistics for each variable of terrorist financing, From the descriptive statistics, Hawaladars method of funding is widely used by terrorist than virtual (bitcoin) method of funding. Table III and VII summarize the result of regression analysis. The p-value for FA is significant. Showing that FA is suitable for the investigation of FCC and TF. Table IV summarizes Kendall's correlation matrix, estimated that there is a positive relationship between the variables and while Table VII also indicated that forensic accounting influences cybercrime and terrorist financing. Table VI Summarizes Analysis of Variance (ANOVA) which established that is a relationship between financial cybercrime and terrorist financing.

From the result, it can be inferred that forensic accounting is can reduce financial cybercrime and terrorist financing. This result is in accordance with terrorism triangle theory and shows that enhancement of forensic accounting can mitigate the bad effect of financial cybercrime and terrorist financing in Nigeria. For fund-raising or financing the terrorist activity hawala systems is more preferred than bitcoin. It is due to the nature of hawala system that more secretive than bitcoin, so this system is can guarantee the confidentiality of money laundering and terrorist financing. Hawala systems is almost unlikely to be discovered by government regarding who is the hawaladar's, the transferor and the transferee.

CONCLUSION AND SUGGESTIONS

The paper investigates the effect of forensic accounting investigations on financial cybercrime and terrorist financing, from the findings, it was concluded that forensic accounting is suitable in investigating terrorist's financial transactions and procedures of cybercrime. The implications of this study emphasized that the government should strengthen enforcement on cybercrimes and provides security infrastructure (advanced technology) in tackling the precedence of financial cybercrime and terrorist financing in Nigeria. The Government should establish a National Forensic Investigation Commission in fighting fraud and terrorist financing in Nigeria. However, this study offers the following contributions; this study provides statistical evidence that financial cybercrime aids terrorist financing. Statistical evidence shows that forensic accounting can track financial cybercrime and terrorist financing adequately.

REFERENCES

Albrecht, W. S. (2003). *Fraud Examination Mason.* Ohio, Thomson and South- Western.

Albrecht, W. S., Albrecht, C.O. & Albrecht, C. C. (2008). Current trends in fraud and its detection. *Information Security Journal: A global perspective*, *17*, 1-32.

Anderson, R. & Petitcolas, F. (2008). On the Limits of Steganography. *Journal of Selected Areas in Communications, 16*(4), 474–481.

Asogwa, I. (2014). The Use of Forensic in Fraud Detection and Control. *International Journal of Research in Management, 5*(4), 61-71.

Bilbeisi, K. M. & Brown, R. T. (2015). How forensic accounting is used to combat terrorism in the United States. *The Forensic Examiner. Retrieved from http://www.theforensicexaminer.com/2015/Bilbeisi_Brown_777.php*

Bologna and Lindquistn. (1987). Fraud auditing and forensic accounting: new tools and techniques. *European Journal of Accounting Auditing and Fiancé Research.*

Braun, R. L. & Davis, H. E. (2003). Computer-assisted Audit Tools and Techniques: Analysis and Perspectives. *Managerial Auditing Journal, 18*(9), 725-731.

Collin, G. (2015). Incorporation "Cutting Edge" Forensic Accounting Techniques/ Methodologies into College/University Audit, *Annual Conference*. Indianapolis.

Counter-Terrorism Implementation Task Force (CTITF) Office. (2009). Guide to UN Counterterrorism, New York, USA. *https://www.ipinst.org/wp-content/uploads/2012/06/pdfs_terrorism-directory_3-CTITF-AlQaida.pdf.*

Dennis, P. (2003). Terrorism's War with America: A History. Westport, Conn.: Praeger.

FATF Report (2013) the Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing, Andre Pascal, France.

FBI (2013) Terror Financing: Tracking the money trails. (2013, July 5). *FBI News. Retrieved from* *https://www.fbi.gov/news/stories/terror-financing-tracking-the-money-trails1*.

Gaines, L. K. & Miller, R. L. (2004) *Criminal Justice in Action*. Thomson Wadsworth: Belmont, CA, United States.

https://www.techopedia.com/definition/14738/data-hiding

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet*, 283-301.

James D. B. (2018). The Clinton administration's development and implementation of cybersecurity strategy (1993–2001).

Kessler, G. C. (2006). *An Overview of Cryptography*. Accessed at http://www.garykessler.net/library/crypto.html.

Krancher, R. (2010). *Introduction to Fraud Examination and Financial Forensics*. New York, USA.

Levitt, M., & Jacobson, M. (2008). The Money Trail: Finding, Following, and Freezing Terrorist Finances, *Washington Institute for Near East Policy,* Washington DC, United States.

Madan, B. (2013). An Empirical Investigation of the Relevant Skills of Forensic Accountants: Experience of a Developing Economy. *European Journal of Accounting Auditing and Finance Research Training and Development UK, 1*(2), 11-52.

Nigrini, M. J. (2012). *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection*. John Wiley & Sons, Inc.: New Jersey.

Nir, K. (2010a). *The Global Cybercrime Industry*. Springer: New York.

Nir, K. (2010b). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer: USA.

OECD. (2019). Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors, OECD, Paris.

Sharma, A. & Panigrahi, P. K. (2012). A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *International Journal of Computer Applications, 39*(1), 37-47.

United Nations Office On Drugs And Crime (UNODC). (2012). Vienna. The use of the internet for terrorist purposes. United nations, New York

Albrecht, W. S., Albrecht, C.O. and Albrecht, C. C. (2008). Current trends in fraud and its detection, Information Security Journal: A global perspective, Vol.17, pp.1-32