Cybercrime and Terrorism Financing: Nigeria's Potential Vulnerabilities and Policy Options

Plangshak Musa Suchi and Peter Nungshak Wika

Department of Sociology, Faculty of Social Sciences, University of Jos, Jos-Nigeria

***Abstract* : Terrorism financing and the ways in which it intersects with organised criminal activities including drug trafficking, arms trafficking, trafficking in persons/smuggling of migrants, and kidnapping-for-ransom is increasingly attracting the attention of scholars and the international community. What is less explored however are the ways by which cybercrime facilitates terrorism financing globally. This paper attempts to fill this gap by utilizing secondary data from international, regional and national organisations as well as scholarly articles on the subject through content analysis to explaining the nexus between cybercrime and terrorism financing with specific emphasis on Nigeria. Understanding the linkages between cybercrime and terrorism financing is important for developing effective policy measures aimed at preventing and mitigating the negative impacts of these innovative crimes. The analysis revealed the mysterious links between cybercrime and terrorism financing in terms of how the former is feeding the latter through multiple channels including supply of funds from proceeds of cybercrime, as well as by making funds transfer among terrorist groups easier. The paper also highlights potential vulnerabilities in Nigeria's critical infrastructure including computer systems and networks, computer programmes, and communication systems; defence, banking, energy, and oil and gas, as well as potential vulnerabilities among individual internet users and the private sector which may be exploited by cybercriminals in conjunction with terrorist groups in the country. It concludes by proffering some policy options including boosting partnerships between law enforcement, the academic community and the private sector towards understanding and reducing cybercrime and terrorism financing in Nigeria.**

Keywords: **cybercrime, terrorism, terrorism financing, potential vulnerabilities, Nigeria**

I. INTRODUCTION

The convergence of transformations in information and communications technology (ICT) with increased access and dependence on the internet for education, business, commerce and governance on a global scale, has opened up new opportunities for cyber-criminal groups as well as terrorist groups to carry out their nefarious activities without being detected or identified, let alone prosecuted. Cornish (2009) notes, "The 21st century economy, and much of society itself, is dependent upon a broadband-enabled, cyber-knowledge complex" which creates vulnerabilities by opening up "an ever widening array of opportunities for the unscrupulous to exploit" (p.6).

Europol (2018b) notes that, "The sheer range of opportunities that cybercriminals have sought to exploit" due to the above development "is impressive[1]". Criminal groups are more and more utilizing new and sophisticated cybercrime tools to conceal their identity and location in order to evade detection while carrying out cyber-attacks on critical national infrastructure including economic and financial systems in ways that appear to be blurring the boundaries between cyber warfare, cybercrime and cyber terrorism (Wilson, 2008). According to INTERPOL (2018):

Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before. Complex criminal networks operate across the world, coordinating intricate attacks in a matter of minutes.

Cybercriminals are not only becoming more aggressive and confrontational but organised criminal groups including human, drug, and weapon traffickers are utilizing social networking and online classified sites such as Craigslist, Backpage, and Myspace to market, recruit and sell their criminal products and services (Latenaro, 2011). What is more, cybercrime and cyber-attack services are now available for hire from criminal organisations by anybody including terrorist groups which officials in government and industry recognized as a growing threat to national security, economic development and stability (Wilson, 2008; Jacobson, 2010).

In particular, terrorist groups are leveraging on cybercrime capabilities to finance and facilitate their nefarious activities. Jocobson (2010) observes that apart from its well-known use of the Internet for propaganda and recruiting purposes, Al Qaeda has also utilized the Internet for a variety of other purposes, including terrorist financing. Worst still:

[1] These range from using botnets (i.e. networks of devices infected with malware without their users' knowledge) to transmit viruses that gain illicit remote control of the devices, steal passwords and disable antivirus protection; creating "back door" on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets; through creating online fora to trade hacking expertise; to laundering traditional and virtual currencies; committing online fraud; various forms of online child sexual exploitation, and the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards and drugs, and hacking services among others (Europol, 2018b).

Al Qaeda is far from alone among terrorist organizations in exploiting the Internet for this type of activity. A wide range of other terrorist groups, including Hamas, Lashkar e-Taiba, and Hizballah have also made extensive use of the Internet to raise and transfer needed funds to support their activities (Jacobson, 2010, p. 353).

Terrorists engage in criminal activities on the internet in order to raise funds. A classic example of this is the case of three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, who in 2007 pled guilty, and were sentenced for using the Internet to incite murder. According to Wilson (2008):

The men had used stolen credit card information at online web stores to purchase items to assist fellow jihadists in the field..., through using 110 different stolen credit cards. Another 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies. The group also laundered money charged to more than 130 stolen credit cards through online gambling websites. In all, the trio made fraudulent charges totalling more than $3.5 million from a database containing 37,000 stolen credit card numbers, including account holders' names and addresses, dates of birth, credit balances, and credit limits (p.16).

This worrisome trend in cybercrime underscores the need for law enforcement to keep pace with new technologies, to understand the possibilities they create for criminals and how the ICT can be used as tools for fighting cybercrime. This is particularly crucial because the problem posed by cybercrime affect all countries of the world due to its transnational nature and the fact that the world is now a global village. Nigeria in particular and Africa in general cannot be immune to these threats especially with the rapid increase in internet connectivity and access due to explosion of smart phones and availability/affordability of mobile broadband on the African continent.

Data from the Nigerian Communications Commission (NCC) for example indicates that over 100 million people in Nigeria were connected to the internet with 250,000 new subscribers logging on in the last quarter of 2019 (Russon, 2020). This number significantly increased in the first half of 2020 owing to the impact of COVID-19 pandemic which radically altered the nature of social interaction (from face-to-face to on-line interaction) across the globe. In February 2020 alone, a total of 3.3million new internet subscribers were added to the pool of internet users in the country bringing the total numbers to over 134 million users (Orija, 2020). This rapid increase in number of internet users suggests that more and more socio-economic, political and financial activities in the country are being accomplished online. This development has unfortunately opened up new vulnerabilities including the utilization of cyber technologies by terrorist groups for recruitment, propaganda, training, communication and raising funds to finance terrorist activities (Manu, 2017).

The issue therefore is not just that cybercriminals are becoming more organized but also that terrorist groups are increasingly utilizing cybercrime capabilities to carry out terrorist attacks with attendant devastations for national security, economic development and societal stability. This paper explores the possible connections between cybercrime and terrorism financing, and discusses the potential threats that this posed to national security, economic development and social stability in Nigeria.

Data Sources and Method

Data for the paper was derived from secondary sources including reports of national, regional and international organisations and agencies such as INTERPOL, Europol, the UN, UNODC, national legislations on cybercrime, and terrorism financing as well as scholarly articles and research reports on the subject. Content and thematic analysis was used to arrive at the findings which provided the basis for the analysis, discussion and conclusion.

II. LITERATURE REVIEW

Conceptualizing Cybercrime

Cybercrime is difficult to define in a way that can adequately capture the wide range of offences (including traditional computer crimes and network crimes) mentioned in regional and international legal approaches to describing the phenomenon (Gercke, 2012). This difficulty is further complicated by the fact that cybercrime could go beyond legal definitions to encapsulate other equally socially harmful activities- including certain forms of pornography and spamming taking place across the cyber space that are not strictly illegal (Suchi & Kassa, 2016).

Many studies in recent decades tend to focus more on providing a typology of cybercrime rather than a definition (See for example UNODC 2013; Nigeria's Cybercrime (Prohibition, Prevention, etc) Act, 2015; Europol, 2018a). The UNODC comprehensive study on cybercrime did not 'define' contemporary cybercrime as such. Instead, it describes it as a list of acts[2] which constitute cybercrime (UNODC, 2013). The study however suggests that today's cybercrimes are "activities that focus on utilizing globalized ICT for committing criminal acts with a transnational reach" (UNODC, 2013 cited in Suchi & Kassa, 2016, p. 275).

Similarly, the Cybercrime (Prohibition, Prevention, etc) Act (2015) which seeks among others to "provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria" (Cybercrime (Prohibition, Prevention, etc) Act 2015, Part I) did not offer any concise definition of cybercrime. Instead, it basically

[2] These includes acts against the confidentiality, integrity and availability of computer data or system (e.g. illegal access, interception or acquisition of computer data); computer-related acts for personal or financial gain or harm (e.g. fraud or forgery); and computer-content-related acts (e.g. computer related acts in support of terrorism offences).

describes in Part III a list of offenses and associated penalties that constitute cybercrime in Nigeria[3].

In its contribution, Europol (2018a) focused more on describing two different categories of cybercrime namely, *cyber-dependent* crimes and *cyber-enabled* crimes where the latter covers traditional crimes facilitated by the internet and digital technologies such as payment fraud and child sexual abuse and exploitation, while the former refers to "any crime that can only be committed using computers, computer networks or other forms of ICT" such as malware attack[4], distributed denial of service (DDoS) attack, and website defacement (Europol, 2018a, p. 15). The categorization indicates that cybercrime can take various forms including high-tech crimes, data breaches and sexual extortion.

Without going into details of definitional differences in the literature, this paper adopts UNODC (2019) conceptualization of cybercrime as "an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime (UNODC, 2019, E4J University Module Series: Cybercrime, Module 1). The major import of this conceptualization is that it includes elements common to existing cybercrime definitions including the legal dimension of the act and the role of ICT in the offence - whether it is the target of the offence or part of the method of operation of the offender. The definition also revealed the complex nature of cybercrime which the UNODC Global Programme on Cybercrime describes as "one that takes place in the borderless realm of cyberspace, is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime, and their victims, are often located in different regions, and its effects ripple through societies around the world" (UNODC n.d. cited in UNODC, 2019, E4J University Module Series: Trafficking in Persons & Smuggling of Migrants, Module 14).

Conceptualizing Terrorism Financing

Terrorism financing as employed in this paper simply refers to the provision or collection of funds and other material supports to/by terrorist groups to sustain and promote their activities in violation of the law. This conceptualization draws heavily on the meaning ascribed to the term by the International Convention for the Suppression of the Financing of Terrorism adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999. The Convention states:

Any person commits an offence ... if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out... act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an 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 population, or to compel a government or an international organization to do or to abstain from doing any act (UN, 1999, Article 2 Section 1b).

Building on the above, and acting under Chapter VII of the Charter of the United Nations, the UN Security Council in its Resolution 1373 of 2001 calls on States to prevent and suppress the financing of terrorist acts by criminalizing the provision and collection of funds for terrorist purposes (UN Security Council, 2001, Section 1a&b). According to the Council's Counter-Terrorism Committee Executive Directorate (CTED), terrorism financing is a global phenomenon that not only threatens Member States' security, but can also undermine economic development and financial market stability (UN Security Council CTED, n.d). It is therefore of paramount importance to understand its connection with cybercrime with a view to stemming the flow of funds to terrorist groups.

Theoretical Framework

Various theoretical perspectives on the causes and facilitating factors of criminal behaviour have been applied to explaining cybercrime and its connection to terrorism financing with varying degrees of successes. These range from classical theories of crime as a product of rational choice or free-will of individual criminals (Beccaria, 1764; Cohen & Felson, 1979), through positivistic theories which hold that criminal behaviour is determined (by internal or external factors in/to the individual criminal[5] to ethical perspectives that see crime as a reflection of a moral failure in decision making on the part of criminal individuals and groups (Narvaez, 2006; Albanese, 2016).

Due to the complex nature and transnational character of cybercrime and its intersection with terrorism financing, it is difficult to adequately understand and exhaustively explain its root causes, facilitating factors and prevention and control using a single theory. For example, cybercrime can be perpetrated by individuals, groups, businesses, and nation-states using similar tactics and attacking similar targets but with different motives and intent (Wall, 2007, as cited in UNODC, 2019 E4J University Module Series: Cybercrime, Module 1). It is therefore difficult to explain such conducts

[3] These include offences against critical national infrastructure, unlawful access to computer, unlawful interception of data, interception of electronic messages, emails, and electronic money transfers; computer related forgery, fraud and theft of electronic devices; unauthorized modification of computer systems, network data and system interference; cyber terrorism, identity theft and impersonation; child pornography and related offences, cyber stalking, cyber squatting, and racist and xenophobic offences.

[4] A malware attack is a form of high-tech crime in which malicious software, infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware (including Botnet, Rootkit, Warm, Trajan, File infector, Backdoor/remote-access Trajan (RAT), Ransomware, Scareware, Spyware and Adware), and they can complement each other when performing an attack (See Europol, 2018b for detail on these types of malware attack).

[5] See Mclaughlin and Muncie, 2013 for a range of these theories including medical/biological, psychological and sociological explanations.

using a single theory. Therefore, this paper utilized three theories namely: Space Transition Theory, Situational Crime Prevention Theory, and Routine Activity Theory in a kind of theoretical triangulation as its theoretical framework. The beauty of this approach is that it pulled together a number of factors including technological, economic, and socio-demographic in ways that help to make sense of the phenomenon.

In recent decades, studies have examined the role of "space" particularly online spaces and online communities in the cultural transmission of criminal and/or delinquent values that predispose individuals to committing cybercrime (Evans, 2001; Maras, 2016; Manu, 2017). Manu (2017) for example applied *Space Transition Theory* as postulated by Karupannan Jaishankar (2008) to explaining cyber-terrorism in Nigeria in terms of how "the anonymity in the cyberspace predisposes cyber-criminals to utilize the internet and computers in perpetrating cybercrimes or cyber-terrorism" (Manu, 2017, p.398). This explanation rests on certain assumptions including the notion that persons with repressed criminal behaviour are more likely to commit crime in cyberspace than in the physical space due to their social background, as well as the related assumption that identity flexibility, dissociative anonymity and lack of deterrence in the cyberspace create an enabling environment for criminals to commit offence than in the physical space. In addition, it is assumed that conflict of conduct norms and values in the cyberspace may likely breed cybercrime (Jaishankar, 2008, as cited in Manu, 2017, p. 398).

A major relevance of the theory to the present paper is its emphasis on the wide range of opportunities created by the internet for the unscrupulous including terrorist groups to exploit. In this sense, cybercrime serves as a facilitating factor of terrorism in ways that amount to financing. The theory however offers little or no insights on the specific strategies that must be taken to reduce the opportunities offered by the cyberspace for offenders to successfully carry out cybercrime and other criminal activities.

To address the above gap, this paper utilized insights from environmental criminology especially situational crime prevention (SCP) theory (Muhammad, et al., 2017; Ibrahim & Mukhtar, 2017) in examining possible measures that must be put in place to prevent and reduce the opportunities offered by the cyberspace for cybercriminals and terrorist groups to collaborate.

SCP and environmental criminology in general is anchored on the assumption that criminal opportunity plays important role not only in causing crime but also in preventing crime because the nature of criminal opportunities influences the amount, nature, and location of crime (Clarke, 1992, as cited in Muhammad, et al., 2017, p. 358). SCP theory in particular recommends the application of measures directed at highly specific forms of crime (such as cybercrime) including the design or manipulation and management of the immediate environment (such as the internet or cyber space) in a way that greatly reduces vulnerabilities and makes it very difficult for the unscrupulous to exploit (Ishaq & Rabiu, 2017).

In order to effectively prevent and reduce cybercrime therefore, law enforcement must understand "the opportunities which occur at the very point at which a crime would take place" because these situationally determined opportunities "are more susceptible to manipulators" than any crimogenic conditions (Muhammad, et al., 2017, p. 358). Understanding these opportunities entails mastering the *crime scripts* which Basamanowicz & Bouchard (2011) defined as "the analysis of a criminal event in the sequential and instrumental steps that must occur for the event to be successful" including, identifying the actors which must be available to complete their tasks; the appropriate tools; skills, and/or prerequisite for success in each step; and the action that must occur for advancement to the next step in the script (cited in Ibrahim & Mukhtar, 2017, p. 417).

Perhaps, nowhere else is the ability to master the crime scripts required of law enforcement than in the area of cybercrime especially cyber-dependent crimes such as hacking, malware attack, DoS attack, DDoS attack, and website defacement due to their novelty as emergent crimes. A single incident of cyber-terrorism or cyber warfare for example will require not only technical skills but a combination of that with analytical and organisational talents (Ibrahim & Mukhtar, 2017) as well as adequate planning and networking among motivated individuals and groups.

In addition to mastering the crime scripts, it is also important that law enforcement and the general public understand the conditions and situations that could increase one's likelihoods of cybercrime victimization. In this regard, this paper recognises the relevance of victim-centred theories particularly routine activity theory (RAT) and studies that relied on the theory in explaining specific types of cybercrime such as interpersonal cybercrime (e.g. online child sexual exploitation and abuse, cyber stalking, cyber harassment, and cyber bullying[6]).

More recently Tade & Adeniyi (2020) apply the RAT as propounded by Cohen & Felson (1979) to explaining electronic fraud in Nigeria's cashless ecosystem. From the perspective the theory offers, crime risk increases upon the convergence of a motivated offender (potential cybercriminal), a suitable target (such as a girl child with access to the internet or a billionaire that is careless online with his banking details), and the absence of a capable guardian (which could be a conscious parent, school teachers, effective law enforcement agencies, experienced bank officer, etc). These three factors appear to have converged perfectly in the cyberspace with all the anonymity it offers to internet users thereby facilitating cybercrime (UNODC, 2013).

[6] See Ibrahim & Mukhtar, 2017, p. 417 for example of such studies including Choi (2011), Marcum, 2011 and Williams, 2015.

III. FINDINGS, ANALYSIS AND DISCUSSION

Linkages between Cybercrime and Terrorism Financing

Cybercrime is potentially linked to terrorism and by implication terrorism financing in a number of ways. First, cyber-technology or the ICT can be used to facilitate the commission of terrorist-related offenses, or it can be the target of terrorists (UNODC, 2019, E4J University Module Series: Cybercrime, Module 14). Cyber-terrorism for example, which Denning (2001) defines as "... politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (cited in Wilson, 2008, p. 4) often depends on technology to materialize while also making the ICT its primary target. The UNODC's (2012) publication on 'the use of the internet for terrorist purposes' indicates that terrorists use the internet to spread propaganda (including recruitment, radicalization and incitement to terrorism); raise funds, train members, plan and execute attacks and for cyber-attacks.

Secondly, a cyber-attack can be carried out by cybercriminal groups with a view to committing a 'profitable' crime, as well as by terrorist groups with a view to causing terror. Wilson (2008, p. 4) observes, "If a terrorist group were to launch a cyber-attack to cause harm, such an act also fits within the definition of a cybercrime". The primary difference between the two will be in the intent of the attacker, "and it is possible for actions under both labels to overlap".

Thirdly, "linkages do exist between terrorist groups and cyber criminals that allow terror networks to expand internationally through leveraging the computer resources, money laundering activities, or transit routes operated by criminals" (Wilson, 2008, p. 16-16). Following the 2005 U.K. subway and bus bombings for instance, London police officials reportedly believe that terrorists obtained high-quality explosives used for the bombings through cyber-criminal groups based in Eastern Europe (Walsh 2005 cited in Wilson, 2008, p. 16) which points to a major link between cybercrime and terrorism.

The significant link between cybercrime and terrorism financing is aptly illustrated in the earlier cited 2007 trial of three British residents namely Tariq al-Daour, Waseem Mughal, and Younes Tsouli in which the trio pled guilty and were sentenced for using the internet to incite murder (Wilson, 2008). A related challenge is the increasing use of the cyberspace by terrorist groups to exploit charity organisations and NGOs for variety of purposes.

In fact "some charities are founded with the express purpose of financing terror, while others are existing entities that are infiltrated by terrorist operatives and supporters and co-opted from within" (Jacobson, 2010, p. 356). Such Charities and NGOs including the Global Relief Foundation (GFR) designated in 2002 by the US Treasury for its ties to Al Qaeda and the Taliban; the Al Qaeda–linked NGO, the Al-Haramain Islamic Foundation, a Saudi-based NGO that was designated by the United States in November 2008 for its ties to Al Qaeda; and the Holy Land Foundation, a Texas-based charity, whose leaders were convicted in 2008 for supporting Hamas all have charitable fronts such as websites operating online through which they openly advertise their activities and solicit for funds (Jacobson, 2010).

Furthermore, in a study that examined the role of forensic accounting investigation in tracking financial cybercrime and terrorism financing, Olatunji & Aruwaji (2020) verified the association between cyber criminality and terrorism financing and concluded that forensic accounting is suitable in investigating terrorist's financial transactions and proceeds of cybercrime.

Today, terrorist groups such as the ISIS, ISIL, Boko-Haram, and the Islamic State of West African Province (ISWAP) continue to use the internet to spread propaganda and to inspire acts of terrorism. The Europol (2018a) Internet Organised Crime Threat Assessment (IOCTA) reported on how the take down campaign carried out by law enforcement in association with industry is forcing terrorists groups underground thereby pushing their sympathisers into using encrypted messaging apps such as Threema, Signal and Telegram as well as the dark web which offer private and closed chat groups the opportunity to communicate and share dangerous information online without being detected. It is therefore crucial to take into consideration the impact of cybercrime on terrorism financing in any legal, technical and policy measure directed at effectively stemming the tide of terrorism financing in Nigeria.

Nigeria's Vulnerabilities to Cybercrime and Terrorism Financing

The foregoing analysis has generated useful insights on the mysterious links between cybercrime crime and terrorism financing largely in terms of how the former fuels the latter. It will be noted from the analysis that cybercrime appears to be playing the role of an independent variable in the relationship, while terrorism financing is the dependent or explanatory variable.

Overall, the analysis has shown that cybercrime and terrorism financing are interrelated growing security problems to all countries of the world including Nigeria. This is due to their transnational character, growing internet connectivity and access, as well as the problem of/or difficulties associated with tracing these crimes. More fundamentally, it points to certain identifiable vulnerabilities of Nigeria to cybercrime and terrorism financing including the following:

First, as the independent variable in the identified relationship, cybercrime can be used not only to facilitate terrorism but also in itself to cause serious financial and economic damage to the country. Apart from the enormous financial loss and economic impact of cybercrime to individual victims and their families, financial institutions and their customers, as well as the national economy, its social impact on the country's law

enforcement, citizens, and the government in terms of reputational damage in the eyes of the international community can best be imagined than described (Suchi & Kasa, 2016).

Unless the law enforcement agencies including the Nigeria Police Force (NPF), Economic and Financial Crimes Commission (EFCC) and the Department for State Security (DSS) as well as the private sector are ahead in their game, cybercriminals can easily identify new vulnerabilities not only in individual internet users and organisations but in Nigeria's critical infrastructural systems to exploit. These critical infrastructure include computer systems and networks, computer programmes, and communication systems that are vital to the operation of sensitive sectors of the society such as defence, banking, oil and gas, energy, and transportation that their "incapacitation will have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters" (Cybercrime [Prohibition, Prevention, etc] Act, 2015, p.6).

In regards to the USA for instance, Wilson (2008) indicates that the possible effects of a successful exploitation of a major vulnerability in the infrastructure of the internet in 2002 such as a flaw in the Simple Network Management Protocol (SNMP) would have enabled attackers to take over Internet routers and cripple network telecommunications equipment globally. But for the private sectors' swift response, such security flaw could have been exploited to cause many serious problems, such as bringing down widespread telephone networks and also halting control information exchanged between ground and aircraft flight control systems with devastating consequences (Gellman, 2002, cited in Wilson, 2008, p.21).

Other vulnerabilities identified in that study that may be applicable to Nigeria include the Supervisory Control And Data Acquisition (SCADA[7]) system vulnerabilities; the unpredictable interaction between the computer systems that operate the different critical infrastructure of the country; and the civilian technology that support the military as well as the insider threat, which pertains to the ease with which data can be copied and carried outside using a variety of storage devices such as a flash drive which can be abused by staff members of an organisation (Wilson, 2008). All these are possible areas of vulnerability to hacking, botnets, and cyber attacks that Nigeria should also watch out for.

Second, cybercrime's links to terrorism has further rendered the organisational structure of terrorist groups more complex thereby making it difficult for criminal justice officials to detect and prosecute their illicit behaviours (Dugan & Gibbs, 2009). Analysis of the role of organisational structure in the control of corporate crime and terrorism indicates that diffuse organisational structure makes it more difficult to detect terrorism participants (Dugan & Gibbs, 2009). For example, after al-Qaeda lost its training and operational infrastructure in Afghanistan, members relied on associated groups for survival making it nearly impossible to target the group as a whole (Gunaratna, 2004 cited in Dugan & Gibbs, 2009, p. 116).

It should not be surprising therefore to find in the context of Nigeria that the banditry, cattle rustling, kidnappings for ransom and abduction of school children ravaging parts of the country especially the north-east, north-west and north-central are connected with Boko Haram or ISWAP associates scattered all over the country as a result of the military operations which displaced them from their strongholds in Maiduguri. If that turns out to be the case, then one cannot agree less with Thony (2000) on the view that criminal assets and terrorist assets represent the same threats to financial systems and public institutions.

Last, despite the potential links between cybercrime and terrorism financing analysed in this paper, it is difficult to determine the proportion of cybercrime that can be directly or indirectly attributed to terrorist just as it is hard to establish the volume of terrorist funds that can be attributed to the proceeds of cybercrime. It appears that terrorists' activities are more directly linked to cybercrime when terrorists utilize cyber capabilities to commit organised crimes such as drugs trafficking, smuggling of migrants and kidnapping for ransom with a view to financing terrorism than when they are perpetrating terrorism.

For example, cybercriminals have reportedly "made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where illegal drug funds or other profitable activities such as credit card theft, are used to support terrorist groups" and the money from drug trafficking in Afghanistan, the Middle East and elsewhere is in turn used to help fund terrorist and insurgent groups that operate in those countries (Bergen, 2006, cited in Wilson, 2008, p. 16).

Nevertheless, there is a sense in which cybercrime can be said to potentially have direct links to terrorism financing particularly where terrorist and their sympathisers use the internet to facilitate funds transfers (mostly in form of crypto currencies) and laundering, share instructional videos or share tutorials. As Europol (2018a) notes:

IS sympathisers have shared instructional videos offering tips about encryption and discussing the surveillance capabilities of hostile governments. Other tutorials have included advice on how to sign up Twitter or Facebook without having to register a mobile phone number and how to deactivate GPS tagging when taking or posting a photo" (p.52).

Nigeria therefore is highly vulnerable to Boko Haram's illegal use of the internet to facilitate fund transfers, money laundering and exchange of sensitive instructional videos among their members largely due to lack of proper and reliable data base about its population. To reduce its vulnerabilities to the foregoing threats, the need for measures

[7] SCADA systems are the computers that monitor and regulate the operations of most critical infrastructure industries (such as the companies that manage the power grid) in the US.

to address terrorist financing in a more effective and comprehensive manner including tackling cybercrime in all its manifestations cannot be over emphasized.

IV. CONCLUSION AND RECOMMENDATION

In conclusion, given the extent of Nigeria's vulnerability to the threats posed by the linkages between cybercrime and terrorism financing to national security and economic development, it is very important that the country prioritises these crimes as interlinked areas with a strong cross-border dimension, where serious investment should be made to significantly reduce the vulnerabilities. This will entail not just strengthening legislation and the capacity of law enforcement agencies in this regard but more fundamentally, also constantly educating the citizens on the nature and trend of these crimes and the connection between them with a view to inculcating in the population practices that will reduce the country's vulnerability. Other important measures that should be taken towards curtailing the problem of cybercrime and terrorism financing include boosting partnerships between law enforcement, the academic community and the private sector because by their very nature, these are not the phenomena that can be dealt with in a fragmented way.

AUTHOR NOTE

We have no known conflict of interest to disclose Correspondence concerning this article should be addressed to Plangshak Musa Suchi, Department of Sociology, Faculty of Social Sciences, University of Jos, PMB 2084 Jos, Plateau State- Nigeria.

REFERENCES

[1] Agwanwo, D. E. & Iwarimie-Jaja, D. (2017). Transnational organized crime and illicit drug abuse in Nigeria: Dilemmas and prospects. In D. Iwarimie-Jaja & D.E. Agwanwo (Eds.), *Contemporary criminality in Nigeria: Challenges and options*. Stirling-Horden Publishers (pp. 255-276).

[2] Albanese, J. S. (2016). *Professional ethics in criminal justice: Being ethical when no one is looking* (4th ed.). Prentice Hall.

[3] Albanese, J. (2020). We find the organized crime we are looking for. https://criminologists-without-borders.org/commentary

[4] Alemika, E. E.O. (ed.) (2013). *The impact of organized crime on governance in West Africa*. Friedrich Ebert Stiftung.

[5] Beccaria, C. (1764). *On crimes and punishments*. Bobbs-Merrill.

[6] Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44, 588-608.

[7] Cornish, P. (2009). *Cyber security and politically, socially and religiously motivated cyber-attack*. European Parliament. http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

[8] European Parliament and Council (2017). Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on "Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA" http://data.europa.eu/eli/dir/2017/541/oj.

[9] Dugan, L. & Gibbs, C. (2009). The role of organisational structure in the control of corporate crime and terrorism. In S.S. Simpson & D. Weisburd (eds.), *The criminology of white-collar crime*. Springer (pp. 111-128).

[10] European Commission (2015). The European agenda on security. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions /*COM/2015/0185 final*/. https://eur-lex.europa.eu/legal/-content/EN/TXT/?uri=celex:52015DCO185

[11] European Commission (n.d.). Fight against the financing of terrorism. https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/fight-financing-terrorism_en.

[12] Europol (2018a). Internet organized crime assessment. European Union Agency for Law Enforcement Cooperation. www.europol.europa.eu

[13] Europol (2018b). Cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[14] Federal Government of Nigeria (2015). *Cybercrime (prohibition, prevention, etc) act*, 2015.

[15] Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response.
ITU Report, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[16] Guy, J., Halasz, S., DiDonato, V. & Tuysuz, G. (2020). Italian police seize over $1 billion of 'ISIS'-made' captagon amphetamines. CNN July 1, 2020. https://amp-cnn-cdn.ampproject.org/v/s/amp.cnn.com/cnn/2020/07/01/europe/isis-drug-seizure-italy.scli-intl/index.html?

[17] Ibrahim, B. & Mukhtar, J.I. (2017). Emerging cyber-terrorism threats in Nigeria. In P.N.

[18] Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader*. Ahmadu Bello University Press (pp. 415-428).

[19] International Crisis Group (2020). Violence in Nigeria's north west: Rolling back the mayhem. *Africa Report* No. 288, May, 2020.

[20] Interpol (2018). Cybercrime. www.interpol.int/Crimes/Cybercrime

[21] Jacobson, M. (2010). Terrorist financing and the Internet. *Studies in Conflict and Terrorism* 33(4), 353-363. https://doi.org/10.1080/10576101003587184

[22] Lewis, J. (2007). Emerging threats, cybersecurity, and science and technology. Testimony before the House Committee on Homeland Security sub-committee on, April 15, 2007.

[23] Mclaughlin, E. & Muncie, J. (2013). *Criminological perspectives: Essential readings* (3rd ed). Sage Publication.

[24] Manu, Y. A. (2017). Globalization, cyber-terrorism and Nigeria's national security. In P.N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* Ahmadu Bello University Press (pp. 395-414).

[25] Muhammad, S.I., Ishaq, M.A. & Rabiu, I. (2017). The Nigerian cybercrime (prohibition, prevention, etc.) act 2015: A critical analysis. In P.N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* Ahmadu Bello University Press (pp. 351-366).

[26] Narvaez, D. (2006). Integrative ethical education. In M. Killen & J. Smetana (Eds.), *Handbook of moral development*. Erlbaum.

[27] Olatunji, T. E. & Aruwaji, A.M. (2020). Forensic accounting: Breaking the nexus between financial cybercrime and terrorist financing in Nigeria. *Journal of Accounting, Finance and Forensic Accounting* 8(2), 55-66. DOI: https://doi.org/10.21107/jaffa.v8i2.8350.

[28] Orija, B. (2020). 3.3m new users push Internet users' database to 134 million. *The Guardian*, 15 May, 2020. https://m.guardian.ng/technology/3-3m-new-users-push-internet-users-database-to-134million/amp/

[29] Oyelude, O. (2020). Nigerian Army inaugurates operation Sahel sanity to end banditry.

[30] *Punch* July 7, 2020. https://punchng.com/nigerian-army-inuagurates-operation-sahel- sanity-to-end-banditry/

[31] Russon, M.A. (2020). How internet access is improving in Nigeria. *BBC News* 20th February 2020. https://www-bbc-com.cdn.ampproject.org.

[32] Suchi, P.M. & Kasa, A.G. (2016). Impact of cybercrime on the socio-economic development of Nigeria: A challenge to democratic governance. In D. Tamen, P.M. Suchi & M.J. Onobe (Eds.), *Nigeria: Journeying in socioeconomic and political development*. Topaz Publishing House (pp. 271-287).

[33] Tade, O. & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology*, 0(0), 1-24. DOI: 10.1177/0306624X20928028.
[34] Thony, J.F. (2000). Money laundering and terrorism financing: An overview. Paper delivered on May 10, 2000 while serving as a Judge with the Court of Appeals, Versailles, France.
[35] United Nations (1999). International convention for the suppression of the financing of terrorism, adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999, https://www.un.org/law/cod/finterr.htm.
[36] United Nations (2001). Resolution 1373, adopted by the Security Council at its 4385th meeting, on 28 September 2001. https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373(2001).
[37] United Nations Office on Drugs and Crime (2012). *The use of the Internet for terrorist purposes*. United Nations.
[38] United Nations Security Council Counter-Terrorism Committee Executive Directorate (n.d.).
[39] The CTED factsheet about terrorism financing. https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/
[40] Wall, D. (2007). *Cybercrime: The transformation of crime in information age*. Polity
[41] Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. Congressional Research Service Report for Congress.