Chapter 2: Cyber Terrorism and Cyber Security in Contemporary Nigeria

Mosud Y. Olumoye
ORCID iD: https://orcid.org/0000-0002-6584-6096

Stanley O. Ehiane
ORCID iD: https://orcid.org/0000-0001-6871-4526

Abstract

The evolution of Information and Communication Technology (ICT) has transformed the world into a global village. Today, the technological transformation has pervaded every facet of human endeavours. Ironically, the technology that was supposed to serve the needs of mankind, which of course they do serve, has suddenly become the biggest most prevalent threat. Africa and indeed Nigeria, have been caught up in the web of modernisation and the ICT revolution and have had their fair share of the benefits and the menaces of bridging the digital divide.

Considering the forgoing, this study seeks to explore the concepts of cyber terrorism and cyber security in an overview format. The study also highlights the cyber terrorism in Nigeria and its legislation thereon. The study also gives a snapshot into the elements of cyber terrorism; factors aiding cyber terrorism; techniques of attacks used by cyber terrorists; cyber terrorism in Nigeria; the impacts of cyber terrorism, and preventive measures for cyber terrorism. Lastly, the study addresses the effectiveness of cyber security to curb the threat of cyber terrorism. This is an explorative study with over-reliance on secondary data. The conclusion emphasises the significance of effective cyber security strategies to maximise the benefits inherent in ICT for the growth and development of mankind.

Keywords: Cyber-security, Cyber-terrorism, ICT, Nigeria

1 Background to the Study

The importance and roles played by Information and Communication Technology (ICT) and other auxiliary devices in organisations, institutions, government and our daily lives cannot be over-emphasised. Amongst the critical roles of ICT is the transformation of the whole world into a global village. The term ICT refers to a very versatile and powerful technology that is increasingly used as a strategic tool by people, organisations and nations to acquire, process, store and distribute information. Additionally, ICT has been identified as an indispensable tool to manage our daily lives and has become a necessity in our daily operations (Osho, Falaye & Shafi 2013). As the case may be, there has been a surge in the use of cyberspace in Nigeria, as the average citizens of the country use mobile phones while internet usage is steadily increasing.

However, the remarkable development in ICT skills and experience have created a new form of vulnerability popularly referred to as 'cyber terrorism' (Weimann 2004) which has been experienced and is still ongoing in both developed and developing nations of the world. Cyber terrorism has become a continuously evolving phenomenon with increasingly blurred boundaries in terms of definition. The development of ICT has meant that global development has suddenly become an instrument of destruction through the potential acquisition by terrorist groups. The terrorist groups such as the ISIS and Al Qaeda using cyberspace (Internet) have been able to conduct recruitments and propaganda radicalisation across the globe for network expansion and activities (Sinai 2016). The radicalisation and training of some Muslim Americans was conducted through the cyberspace (Internet) using social media like the Facebook. 'Nidal Hassan Abdul, a US army officer, [and] the radicalisation of Nigerian Omar Abdulmutallab, of British Airways were good examples' (Gabriela 2017:23). The terrorists, using various encryption technologies in operational functions, have been able to avoid the surveillance of the counter-terrorist advisories of the Americans and their European counterparts (Sinai 2017). In the past four decades, cyber terrorism has remained a catastrophic consequence for national security, due to sequences of synchronised attacks on the state's institutions and infrastructure such as the server of the CIA and British and Israeli security agencies (Gabriela 2017). The threat of cyber terrorism will be the biggest threat; this was the view of FBI Director Robert Mueller in 2012 (US Senate report 2014). The Senate report on the potential and imminent threat of cyber-attacks led to Barak Obama's administration's priority towards cyber security. The cyber-attacks have also

manifested in some countries like and Estonia (Gabriela 2017). In Iran a cyber-attack called 'Flame' hurt the Iran information system, and in May 2007 in Estonia two banks and the government IT infrastructure were paralysed (Gabriela 2017: 23).

Developing a cyber warfare capability requires personnel and technical knowledge, and it has been achieved through the recruitment of IT engineers and technicians by the terrorist groups. In certain situations, the terrorist groups contract the services of cyber attackers by paying mercenaries or state sponsors (Sinai 2016). This gives the terrorists the opportunity to launch an attack on any air traffic control and defence system. Also, it should be noted that the more advanced a country is technologically, the more its infrastructure becomes susceptible to cyber-attacks.

Presently, there is an unabated growth in the threat of cyber-attacks in Africa and with the evolution of cybercrime it has led to more uncontrollable and sophisticated attacks. In Africa cyber-attacks have left the government institutions and the banks most vulnerable due to the lack of independent ICT infrastructures, budgetary challenges, poorly trained staff, and a lack of and weak implementation of legislation. African countries struggle to address cybercrime despite the popular Pan African Legal (PAL) document in the convention of the African Union on Cybersecurity and Protection of Personal Data (AUCPPD). Nigeria is ranked among the worst nations regarding the abuse of ICT (Internet Crime Complaint Centre 2010); where terrorists, hackers and other forms of criminals and their agents use it as a tool to perpetrate their unlawful acts. It should be noted that a county with weak cyber security is potentially vulnerable to cyber terrorism, where terrorist groups operate. Consequently, this study basically explores the concept of cyber terrorism and cyber security. Also addressed in the study are the elements of cyber terrorism; factors aiding cyber terrorism; techniques of attacks used by cyber terrorist; cyber terrorism in Nigeria; impacts of cyber terrorism and preventive measures for counter attacks.

2 Concepts of Cyber Terrorism and Cyber Security

2.1 Cyber Terrorism

The term terrorism has been in existence since the 18th century prior to the incidence of the French revolution (Nadjib 2017). However, the act became well known after the September 11 2001 attack on the World Trade Centre in the United States. Hence, the US President, George Bush, declared war against the

terrorists across the globe. Responding to the declaration made by the US, the Al-Qaeda led terrorist group determined to challenge not only the Western countries which are considered to be their enemies; but other nations of the world such as Indonesia, Libya, Pakistan, and considered to have deviated from pure Islamic ideology (Nadjib 2017). Cyber terrorism according to Colarik (2006:46), is the 'premeditated, politically motivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs and data that result in violence against non-combatant targets'. This definition differentiates cyber terrorism from cyber-crime[1] and cyber warfare[2]. The whole excess of cyber terrorism is to induce fear and harm as a resort of political inclination. Colarik's proposition juxtaposes Abolurin's (2011:24) definition of cyber terrorism as the 'application of information technology to attack non-combatant and attract attention to their cause'. The whole idea of fear in this context is considered as violence and this has physical consequences as it portrays the purpose of the attackers (Janczewski & Colarik 2008:14). Imagine if a person gains access to an institution's clinical database and changes the patients' medication and a duty nurse comes in to administer the medication and discovers that the patients die after dispensing the medication. If the initiator threatens to commit more acts of this nature if his demands are not met, this is referred to as cyber terrorism. The context is based on the intention that drove the perpetrator's action and the use of information technology to perpetrate the act and not the action.

Furthermore, terrorism has become a global threat to all nations of the world encompassing lives and properties, government, economic and social realms. Contrary to the conventional terrorism which employs kinetic means such as the improvised explosive devices (IEDs) or suicide bombers (Gross, Canetti & Vashdi 2017) to accomplish their missions, the cyber terrorists employ ICT to advance their religious, ideological and political goals to psychologically and physically hurt the people, more especially the civilians. Cyber war and cyber-crime differ from the cyber terrorism under study. Cyber war connotes the use of viruses and malware to deactivate military setups (Canetti & Vashdi 2017); while cybercrime targets pecuniary benefits to make

[1] Cyber-crime is frequently used by law enforcement agencies and is an offence committed using information technology (Janczewski & Colarik 2008:14).

[2] Cyber warfare is a planned attack by nations or their agents against information and computer systems, computer programmes, and data which result in enemy losses (Janczewski & Colarik 2008:14).

a living, create criminal mischief or for personal pleasure (Olumoye 2011). Moreover, in this era of continued increases in cyber-attacks and terrorist activities, the fear of cyber terrorism has become prevalent and has come to stay. The term 'cyber terrorism' was first coined by Barny Collin in 1982 and was consistent with how the physical and cyber world were merged in relation to some aspects of terrorism (FBI 2011; Riglietti 2016). Cyber terrorism is not only a change from the conventional to a more modern terrorism, but a reflection of a technologically advanced and literate generation using high technology tools with all their sophisticated features such as speed, accuracy, mobility and connection to attack the cyberspace (Nadjib & Cangara 2017).

Thereafter, various scholars in ICT and other fields of study came up with different definitions for cyber terrorism based on their experiences and views. Hence, different definitions have been attributed to cyber terrorism. However, this study adopts one of the most popular and cited definitions of cyber terrorism given by Professor Denning which states that cyber terrorism is a deliberate action taken against the computer system (hardware and software), networks and the information stored there in order to disrupt, degrade, deny access to or destroy (Denning & Denning 2010). Cyber terrorists use a computer network to pose harm to human life or destroy the important and national infrastructure in a way that will affect the citizens and paralyse the nation's economy (Kuboye & Osman 2014). This study aligns with the focus of Bogdanoski and Petreski (2013) that states that if drastic measures are not taken to tackle the increase in cyber terrorism, then the future terrorists will emerge in any of their attacks to destroy the infrastructure that depends largely on ICT without necessarily firing a shot.

2.1.1 Elements of Cyber Terrorism

Several cyber terrorism attacks that have taken place have some fundamental elements which have been identified by researchers in the academic community. According to Denning's (1999) definition, the elements required for cyber terrorism include: the partakers are non-state accomplices; attacks are basically computer-based with damages done on IT based installations; victims of attacks are either for social, religious or political reasons; a cyber terrorism attack is done only within cyberspace (Nadjib & Cangara 2017). In addition, other scholars identified five entities that make up cyber terrorism namely: target of the attacks; mission and reason (motivation) behind the attack; tools to launch the attack; domain to carry out the attack; and the impact of such attacks

(Ahmad, Yunos & Sahib 2012). Mackinnon *et al*. (2013) in their study state that most of the contemporary definitions on cyber terrorism only identify three elements, the terrorists' motivation; the cyber system under target and the impact of the attacks. This study discusses these elements of cyber terrorism in order to have a better understanding of the concept and to identify the profile of actions motivating the perpetrators.

2.1.2 Factors Aiding Cyber Terrorism

One of the critical factors aiding cyber terrorists is the anonymous nature offered by the internet which allows the identity of the evil perpetrators to be hidden. This supports Awan (2014) who states that the terrorists use the internet because it is a safe environment and a hidden platform for them to perpetrate their atrocities since their identities remain anonymous and they need not travel far to launch an attack. Moreover, the terrorists use fake identities during operations which are untraceable.

Another facilitating factor is the supportive nature of the internet. The internet is also referred to as an information super-highway because it connects several thousands of different networks from more than two hundred countries across the globe together (Olumoye 2011). The cyber terrorists use the internet because of this connectivity (supportive) characteristic in order to send messages to millions of people across the globe. According to Awan (2014), the terrorists use the platform to recruit interested people globally.

2.1.3 Techniques of Attacks Used by Cyber Terrorists

There are different techniques adopted by terrorists to unleash their attacks on ICT infrastructures. This was buttressed by Bogdanoski and Petreski (2013) who state that cyber terrorists carry out attacks in different ways. Some of these techniques are discussed accordingly.

Hacking

Hacking generally refers to the act of gaining unauthorised access to a computer, networks, websites or areas of a system (Olumoye 2013). According to Moffitt *el al.* (2012), hacking is the unauthorised access into or interference with a computer system, or any access in order to corrupt, alert, stall or destroy information using a computer or other similar information and communication

devices, without the knowledge and consent of the owner of the computer or information and communication system. This includes the introduction of computer viruses and the likes resulting in the corruption, destruction, alteration, theft, loss of electronic data messages or electronic document. Many of the hackers use 'brute force' which involves combining different letters and numbers until they can get the password that can be used to launch their devilish attack.

Eavesdropping

This method involves the use of software (password sniffers) to monitor packets, or wiretapping telecommunication links to read transmitted data. Eavesdropping can go undetected and it is called a passive attack (Olumoye 2013). Tools used to intercept communications can be cellular, scanners, radio receivers, microphone receivers, tape recorders, network sniffers and telephone tapping devices (Ibikunle 2005). This method is usually used for monitoring all the traffic in on an area network, which the terrorists install on the network system they plot to intrude, such as the ICT-based installations and telephone systems (Hassan, Funmi & Makinde 2012).

Malware

Malware refers to malicious software such as viruses, Trojan worms and other software that gets onto a computer without the owner being aware it is there. Back in the early part of the century, most of such software's primary aim was for excitement (Olumoye 2013). The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for developing such software is generally more sinister and that is the reason it makes the list of the top five computer crimes (Anonymous 2012). Cyber weapons are now identified as the main software tools used by cyber terrorists to wreak havoc on any country and organisation in order for them to accomplish their mission such as manipulating computers and their networks, intrusion into systems, and sending spy (espionage) mails in the form of viruses.

Spam Messages

Spam refers to the release of unsolicited bulk messages. The cyber terrorists use spam messages as a tactic to launch their attacks**.** Though the attackers use

numerous forms of spam messages, the most frequently used ones are spam e-mails which can be disguised in the form of an advertisement for goods and services (Kuboye & Osman 2014). Once the recipient opens the mail, the password as well as the username are generated automatically which can later be used to intrude their mails and launch attacks (Gercke 2012).

2.2 Cyber Security

Defining cyber security at large is not trivial. The difficulty lies in developing a definition that is broad enough to be valid regardless of the system that is being described, yet specific enough to describe what security is (Olumoye 2013b). However, in a generic sense, security is 'freedom from risk or danger'. According to Laudon and Laudon, cyber or information system security can be described as 'the policies, procedures and technical measures used to prevent unauthorised access, alteration, theft, and physical damage to information system' (Laudon & Laudon 2001: 13). Cyber security, which is otherwise referred to as a preventive measure, is an offensive technique to combat cyber terrorism (Osho, Falaye & Shafi 2013). Whatever security method that may be adopted there is a need to ensure that only authorised users can access the organisation's information system, and that the users only perform the job and view the data they are authorised to access (Olumoye 2011). Securing the cyberspace is more important than ever before, just as the physical space is to the survival of mankind, which simply means that the security of the cyberspace is not only essential to prevent cyber-attacks but becomes indispensable to prevent other forms of attacks that can be done through the cyberspace (Osho, Falaye & Shafi 2013). Thus, cyber security turns out to be an intelligent tool for counter terrorism.

3 Cyber Terrorism in Nigeria and State Response

3.1 Terrorism

Terrorism is usually a direct consequence of the peoples' profound disappointment with government. The maltreatment or mismanagement of the critical issues have led to the emergence of various rebellious groups across the Nigeria geographical areas. These include the Bakassi Boys in the South-South; the Oodua People's congress (OPC) in South-West; The Movement for the Actualisation of the Sovereign State of Biafra and Independence People of Biafra (IPOB) in the South-East; the Movement for the Emancipation of the

Niger Delta (MEND) in the South-South; and the *Jama' Ahlus Sunnah Lid Da'awati Wal Jihad*, also known as Boko Haram in the North-East. The major actions of these groups have been perceived as a retaliation to the incapability of the government or society to meet their demands. According to Osho, Falaye and Shafi (2013), cyber terrorism trends in Nigeria have been enthused from the grievances motivated from mainly religious fundamentalism to socio-economic reasons. Without any doubt, cyber terrorism is still in its infancy stage in Nigeria and is being perpetuated by a small portion of the total populace; invariably, a small percentage of the nation's cyber space users. This was substantiated by Osho, Falaye and Shafi (2013) that the activities of terrorists in Nigeria are still mostly traditional in nature. For instance, the attack of some telecommunication masts (MTN and Airtel) were recorded in Bauchi, Borno, Kano, and Yobe State (Adeyemo, Joel & Tsenzhughul 2012). The terrorist attack on the telecommunication masts was mainly to limit the use of mobile technology in order to prevent communication of messages to the public and access to the internet. Moreover, before the 1st October 2010 Abuja bombing, the MEND revealed their strategies to the security agencies using the internet technology (Jeremy 2010). In a recent development, the terrorists have adopted another dimension of cyber terrorism. In this case, politicians, foreigners and people assumed to be rich are kidnapped, while the relatives or government representatives are contacted through phone calls. Intelligence reports have also revealed that Boko Haram has linked up with Al-Qaeda based in Algeria (*The Nation Newspaper* 2011). This implies that Boko Haram may be equally trained on the use of ICT to advance their operations and attacks.

3.2 Nigerian Government Legislation in Fighting Cybercrime: The Nigeria Cybercrime Act 2013

The objectives of this Act are to,

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
(b) ensure the protection of critical national information infrastructure; and
(c) promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

The application of this Act shall apply throughout the Federal Republic of Nigeria.

The Act prevent for Cyber terrorism and provides that any person who accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable to conviction of life imprisonment. The Act further provides for the purposes of this section, 'terrorism' shall have the same meaning under the Terrorism (Prevention) Act 2011, as amended. The Nigerian legislation on Cybercrimes Act 2013 clearly provides for cyber terrorism and the Act is an offshoot of the Council of Europe Convention Cybercrime and ECOWAS Directive on Fighting Cybercrime. The realisation of this Act by the Nigerian Government has addressed the complexity in Article 22 of the Council of Europe on the issue of nationality, territoriality and jurisdiction. The offences in the Convention, ECOWAS Directive all encompasses an established criminal law model for all the nations (The Nigerian legislation on Cybercrimes Act 2013).

4 Impacts of Cyber Terrorism

Cyber terrorism which is still advancing in Nigeria has many potential impacts when it is launched either against the organisations or nations. Some of the impacts of cyber terrorism are discussed accordingly.

4.1 Attacks on Computer-based Infrastructure

The advancement of any organisation or nation is dependent on the critical infrastructure upon which their work is carried out and the exchange of vital information. It becomes apparent that any attack launched on a nation's infrastructure would paralyse its economy. This is corroborated by Thuraisingham (2004) who states that cyber-attacks can be launched on any infrastructure such as the electronic, gas, power, telecommunication lines, food supplies, reservoirs and water supplies, and other vital things; which can lead to the total shut down of an organisation.

4.2 Attack on Businesses

Cyber terrorism has a tremendous impact on society. The impact of a single attack can be very devastating and culminate in huge financial losses. The overall monetary impact of cyber terrorism on individuals and government runs

into billions of dollars (Olumoye 2013). Also, there is a food chain effect when society finds out an organisation is vulnerable to cyber terrorism. Firstly, the company is made aware of their weaknesses. Customers and companies could potentially lose personal information that could then be sold for a profit. The company then loses credibility and profits begin to fall. Secondly, if the market falls, then demand decreases which reduces supply and demand, potentially shutting down a company or sending them into bankruptcy (Muffitt *et al*. 2010). Moreover, customers' trust is affected as the attack of terrorists may intrude into other cyberspace areas thereby discouraging and frustrating the customers or end users who usually visit the concerned page for their business dealings (Saini, Rao & Panda 2012).

4.3 Aggravation, Personal Insecurity and Loss of Life

According to Gross, Canetti and Vashdi (2017), cyber terrorism impacts on civilians by aggravating personal insecurity and anxiety. Moreover, cyber terrorism has rendered many homes to a dilemma which sometimes results in psychological trauma to the family's victims. This has also claimed many innocent lives. In support of this, Awan (2014) states that cyber terrorism can cause serious damages or loss of life, some of which has manifested in a number of ways through the attack of networks and computer usage resulting in different forms of explosions experienced by planes globally and culminating in the loss of many lives.

4.4 Intrusion into Data

It is apparent that processed data (or information) is required to perform numerous functions within an organisation. The intrusion or attack of a nation or organisation's information by cyber terrorists can lead to the loss of vital and critical information which may be difficult to recover. This view was strengthened by Koltuksuz (2013) who states that cyber terrorists can interrupt data availability and destroy its confidentiality as well as integrity.

5 Preventive Measures against Cyber Terrorism

In order to prevent the attacks of cyber terrorists in our society, the following preventative measures are recommended.

(i) Awareness and Training

This is the first set in alleviating cyber terrorism. The citizens, consumers and organisations should create the awareness of cyber threats and the actions they can take to protect their information. Also, continuous training is necessary for business clients in order to share the responsibility in fighting against cyber terrorism (Olumoye 2013b).

(ii) Ethical and Moral Standards

Ethical standards should be upheld in organisations to ensure that confidentiality is maintained, and technology misuses are reduced. Computer ethics help us to identify offenders and create solutions to aid in the minimisation of computer crimes and technology misuse (Moor 1985; Olumoye 2013b).

(iii) Computer Forensics

Computer forensics technically refer to the use of procedure-centric approaches in the study of cyber-attack prevention, planning, detection and responses with the goals of counteracting and conquering hacker attacks by logging malicious activity and gathering court admissible chains of evidence using various forensics tools that reconstruct criminally liable actions at the physical and logical levels (Mandia *et al.* 2001; O'Connor 2003). According to Ibikunle (2005), an advanced computer forensics is the use of steganography, which is the art of hiding communications. Unlike encryption that uses an algorithm and a seed value to scramble or encode a message to make it unreadable; steganography makes the communication invisible. This takes concealment to the next level, which is to deny that the message even exists (Olumoye 2013b).

(iv) Cyber Crime Prevention Laws

According to Mc Connell (2000), National government remains the dominant authority for regulating criminal behaviour in most places in the world. If a nation has already struggled with and ultimately improved its legal authority after a confrontation with the unique challenge presented by cybercrime; it is crucial that other nations profit from this lesson and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations

will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat (McConnell 2000). The attackers' sophistication seems to be ahead of defensive tools. That is the nature of the war between hacker and defenders; the attackers are always a step ahead. However, by making the attackers' job harder and harder, and by increasing the length of jail sentences for cybercrime and improving international police co-operation and skill levels, defenders can combine to keep up with the attackers and over time begin to turn the tide (Paller *et al.* 2007).

(v) Encryption (or Cryptography)

This involves scrambling data into an unreadable format called cipher text before it is transmitted over a telecommunication link between two computers, and then unscrambling that data again when it gets to its destination computer. Only those who possess the secret key can decipher (or decrypt) the message into plain text. If data is not encrypted during transmission, it can easily be intercepted by an unauthorised party thereby enabling the third party to have access to the information. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking; although modern cryptography techniques are virtually unbreakable (Olumoye 2013b). Cryptography is used to protect e-mail messages, credit card information and corporate data.

(vi) Anti-Virus

Anti-virus is a software program that is used to protect computer systems against the menace of viruses. The effect of this software is to detect and remove a virus from a computer system before it does any damage to it. These software programs can readily be purchased from software stores or downloaded from the internet. Examples of antivirus software are: Shield Deluxe, CA anti-virus, BitDefender, Avira, Kaspersky, Avast, Norton, NOD32, Dr. Solomon, MCAFFEE, MSAV and AVG (Olumoye 2013b).

.

(vii) Firewall

Firewalls are made up of software and hardware placed between an organisation's internal and external networks to prevent outsiders from invading their networks. Firewalls are programmed to intercept and examine any

message packet passing between the two networks and reject unauthorised messages (Olumoye 2013b).

(viii) Passwords

Passwords are a unique set of characters that may be allocated to an individual, a system or facility that must be input to allow access. Passwords are a security measure used by computer users which allows only authorised users to gain access to the system. The lack of a password on a computer system increases the risk of unauthorised access. To prevent hackers and crackers from penetrating a network, it is recommended that one use passwords that are difficult to guess. It is better to make the password a mixture of letters, numbers and special characters such as: @! $, %, ‘, &, *, # etc. Moreover, one should always change one’s passwords at regular intervals and also set a minimal length for the passwords such as a minimum of six or eight characters (Olumoye 2011).

Concluding Remarks

This manuscript was commenced bearing in mind that the current threat of cyber terrorism seems not to be noticeable and has recently virtualised in Africa, particularly Nigeria, where the terrorist group called Boko Haram have gained their stronghold. In the United States, Europe and the Middle East cyber terrorism remains an existential threat to the critical infrastructures, and steps are being taken through the application of cyber security to safeguard the country’s facilities. The invisible nature of cyber terrorism allows ample and considerable time for the perpetrators to escalate the lethality of their warfare in a more convergent manner. The African continent, particularly Nigeria, needs to understand the various nomenclatures regarding cyber terrorism in the wake of the ongoing traditional terrorist attacks. In light of the foregone, this study contextualised cyber terrorism and cyber security as two sides of the coin in terms of threat and protection. The study further examined factors aiding cyber terrorism and techniques used to unleash the menace across the globe, along with the potential and physical impacts. This study serves as an early warning to Africa and Nigeria in particular, because West Africa has become a ‘safe haven’ for Boko Haram now branded the Islamic State of West Africa Province (ISWAP). However, beyond the Cybercrime Act of 2013 enacted by the Nigerian government to protect the cyberspace and the potential impacts of

cyber terrorism capable of crippling the nation's infrastructure, the government should address the current challenges of cyber security in the country. The protection of cyberspace will prevent the terrorist group from winning the asymmetric war without the use of arms and ammunitions.

References

Abolurin, A. 2011. *Terrorism: Nigerian and Global Dimensions.* Nigeria: Golden Gems Unique Multiventures Publishers.

Adeyemi, K., D. Joel & A. Tsenzughul, September 2012. Gunmen Attack MTN, Airtel Masts in Kano, Borno, Bauchi, Yobe. *The Nation Newspaper.* Available at: http://www.thenationonlineng.net/2011/news/60494-gunmen-attack-mtn-airtel-masts-in-kano-borno-bauchi-yobe.html (Accessed on 06 September 2019.)

Ahmad, R., Z. Yunos & S. Sahib 2012. Understanding Cyber Terrorism: The Grounded Theory Method Applied. In Cyber Security, Cyber Warfare and Digital Forensic CyberSec 2012 International Conference. *IEEE and American Foreign Policy Decision Making*. San Francisco: The World Affairs Council. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (Accessed on 28 July 2016.) https://doi.org/10.1109/CyberSec.2012.6246081

Anonymous 2012. *Top Five Computer Crimes and How to Protect Yourself from Them*. Available at: http://www.makeuseof.com/tag/top-five-computer-crimeprotect (Accessed on 17 August 2012.)

Awan, I. 2014. Debating the Meaning of Cyber Terrorism: Issues and Problems. *Internet Journal of Criminology* 1 - 14.

Bogdanoski, M. & D. Petreski 2013. Cyber Terrorism – Global Security Threat. *Contemporary Macedonian Defense – International Scientific Defense, Security and Peace Journal* 1324: 59 - 73.

Colarik, A.M. 2006. *Cyber Terrorism: Political and Economic Implications.* London: Idea Group Publishing. https://doi.org/10.4018/978-1-59904-021-9

Denning, D. [1999] 2001. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla, J. & D.

Ronfeldt (eds.): *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation.

Denning, P.J. & D.E. Denning 2010. Discussing Cyber-attack. *Communications of the ACM* 539: 29 – 31. https://doi.org/10.1145/1810891.1810904

Gabriela, S.L., March 2017. Manifestations of Contemporary Terrorism: Cyberterrorism. *Research and Science Today* 1,13. Available at: https://www.rstjournal.com/wp-content/uploads/2017/03/RST-1-2017.pdf (Accessed on 30 September 2019.)

Gercke, M. 2012. Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU, UNESCO.

Gross, M.L., D. Canetti & D.R. Vashdi 2017. Cyber Terrorism: Its Effects on Psychological Well-being, Public Confidence and Political Attitudes. *Journal of Cyber Security* 3: 49 - 58. https://doi.org/10.1093/cybsec/tyw018

Hassan, A.B., D.L. Funmi & J. Makinde 2012. Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology* 27.

Ibikunle, A. 2005. *Investigation of Computer Crime in the Information Technology Industry*. Unpublished Master's dissertation, Ladoke Akintola University of Technology.

Internet Crime Complaint Center 2010. Internet Crime Report. Available at: www.ic3.gov/media/annualreport/2010_ic3report.pdf (Accessed on 04 September 2019.)

Jenczewski, L. & A.M. Colarik 2008. *Cyber Warfare and Cyber Terrorism*. USA: IGI Global. https://doi.org/10.4018/978-1-59140-991-5 PMid:17605410

Jeremy, W. 2010. Nigeria Explosion: Independence Celebrations Marred by Violence. Available at: http://www.csmonitor.com/World/Africa/Africa-Monitor/2010/1001/Nigeria-explosion-Independence-celebrations-marred-by-violence (Accessed on 30 September 2019.)

Koltuksuz, A. 2013. Use of Cyberspace and Technology by Terrorists. *Technological Dimensions of Defence against Terrorism* 115: 106. https://doi.org/10.3233/978-1-61499-317-9-106

Kuboye, O.S. & W.R.S. Osman 2014. Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. *International Journal of Computer Science and Mobile Computing* 35: 1082 - 1090.

Laudon, K.C. & J.P. Laudon 2001. *Essentials of Management Information Systems*. New Jersey: Prentice Hall.

MacKinnon, L., L. Bacon, D. Gan, G. Loukas, D. Chadwick & D. Frangiskatos 2013. Cyber Security Countermeasures to Combat Cyber Terrorism. In Akhgar, B. & S. Yates (eds.): *Strategic Intelligence Management: National Security Imperatives and Information and Communication Technologies.* London: Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-407191-9.00020-X

McConnell 2000. *Cyber Crime … and Punishment? Archaic Laws Threaten Global Information*. McConnell International. Available at: http://www.mcconnellinternational.com/services/cybercrime.htm (Accessed on 08 August 2005.)

Moffitt, T., C. Pannatia, B. Prosenbeck, E. Scott & D. Siversen 2012. *The HRE Online Experience - Technology Misuse and Cyber Crime*. Available at: https://sites.google.com/site/tommoffittportfolio/the-hre-online-experience/technologymisuse-and-cyber-crime (Accessed on 20 October 2013.)

Nadjib, M. & H. Cangara 2017. Cyber Terrorism Handling in Indonesia. *The Business and Management Review* 92: 274 - 283.

O' Connor, T., March 2003. *Glee, Elation and Glory as Motives for Cyber Crime*. Annual Meeting of the Southern Criminal Justice Association. Nashville. Available at: http://faculty.ncwc.edu/toconnor/gleeelation_glory.htm (Accessed on 15 August 2005.)

Olumoye, M.Y. 2011. *Information and Communication Technology and Data Processing*. Lagos, Nigeria: Heralds of Hope Publishers.

Olumoye, M.Y. 2013. Cyber-crime and Technology Misuse: Overview, Impacts and Preventive Measures. *European Journal of Computer Science and Information Technology* 13,3: 10 - 20.

Osho, O., A.A. Falaye, A.A. & M.A. Shafi 2013. Combatting Terrorism with Cyber Security: The Nigerian Perspective. *World Journal of Computer Application and Technology* 14: 103 - 109. https://doi.org/10.13189/wjcat.2013.010401

Riglietti, G. 2016. Defining the Threat: What Cyber Terrorism Means Today and What it Could Mean Tomorrow. *The Business and Management Review* 83: 12 - 19.

Saini, H., Y.S. Rao, Y.S. & T.C. Panda 2012. Cyber-crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA*) 22: 202 - 209.

Sinai, J. 2016. Threat Convergence: A New and More Lethal Category of Terrorist Warfare. *The Journal of Counter Terrorism* 223.

The Nation Newspaper, 16 November 2011. Boko Haram has Links with al-Qaeda – Algerian Minister. Available at: http://www.thenationonlineng.net/2011/index.php/news-update/26240-boko-haram-has-links-with-al-qaeda-algerian-minister.html (Accessed on 18 September 2019.)

The Nigerian Legislation on Cybercrimes Act 2013.

Thuraisingham, B. 2004. Data Mining for Counter-terrorism. *Data Mining: Next Generation Challenges and Future Directions* 157 - 183.

Weimann, G. 2004. Cyberterrorism: How Real is the Threat? United Nations Institute of Peace: Special Report. https://www.usip.org/sites/default/files/sr119.pdf (Accessed on 20 September 2019.)

Mosud Y. Olumoye
Webster University
George Herbert Walker School of Business & Technology
St. Louis, Missouri
USA
myolumoye@yahoo.com
yinusamosud@webster.edu

Stanley O. Ehiane
University of Botswana
Department of Political Science and Administrative Studies
Gaborone
Botswana
stanleyehiane@yahoo.com
ehianes@ub.ac.bw