The War must be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria

Macpherson Uchenna Nnam,[1]
Alex Ekwueme Federal University, Nigeria

Benjamin Okorie Ajah[2]
University of Nigeria, Nigeria

Christopher Chukwu Arua,[3] ***Groupson-Paul Okechukwu,***[4] ***& Cornelius Ofobuisi Okorie***[5]
Alex Ekwueme Federal University, Nigeria

Abstract

The cyberspace-Boko Haram terrorism nexus is on the increase in Nigeria. Yet, only a handful of studies have explored the criminogenic forces and interactions that connect the two phenomena. Five theories were integrated to address the problem. Using theory deconstruction approach, insight into the underlying operational procedures and dynamics of the group and its manipulation of the cyberspace to facilitate terrorism was gained. The choice of cyberspace for promoting Boko Haram activities is not farfetched: We found evidence to justify the fact that terrorists are becoming more invisible and invincible, since they now hide in the cyberspace to recruit and (re)train members, elicit and disseminate information and intelligence, source for and obtain funds, and acquire weapons, logistics and supplies. Since both the offence and the offenders involve syndicates, with regional and global networks, local and international cyber security partnership becomes imperative for Nigeria at this point in history. Such co-operation holds strong promise for evidence-based harm reduction and safer space, which becomes realisable through intelligence-led law enforcement and constant cyber-patrol/surveillance. Proactive, rather than reactive cyber counterintelligence and counterterrorism, is also recommended.

Keywords: Boko Haram Terrorism, Cyberspace, Integrated Theoretical Perspective, Nexus, War.

[1] Lecturer, Department of Criminology and Security Studies, Alex Ekwueme Federal University Ndufu-Alike, PMB 1010, Ebonyi State, Nigeria. Email: icharilife@yahoo.com
[2] Lecturer II, Social Sciences Unit, School of General Studies, University of Nigeria, Enugu Campus, Nigeria. Email: okorie.ajah@unn.edu.ng
[3] Lecturer, Department of Political Science, Alex Ekwueme Federal University, Ndufu-Alike, PMB 1010, Ebonyi State, Nigeria. Email: ceejakchioma@gmail.com
[4] Lecturer, Department of Political Science, Alex Ekwueme Federal University, Ndufu-Alike, PMB 1010, Ebonyi State, Nigeria. Email: groupsonpaul@yahoo.com
[5] Lecturer, Department of Political Science, Alex Ekwueme Federal University, Ndufu-Alike, PMB 1010, Ebonyi State, Nigeria. Email: ocorneloko@gmail.com

Introduction

Cyberspace is a spinoff of 'cybernetics', which originates from the ancient Greek word 'kybernētēs', to mean 'steersman, governor, pilot, or rudder'. Arguably, cybernetics was first used in the scientific community by Wiener (1942), from where Artists (see Ussing, 1968) and Novelist (see Gibson, 1986) adopted the term in their works. Cyberspace "comprises three partially overlapping terrains: (1) The Internet, encompassing all interconnected computers; (2) the World Wide Web (WWW), consisting only of nodes accessible via a URL interface; and (3) a cyber 'archipelago', comprising all other computer systems that exist in theoretical exclusion [i.e. not connected to the internet or the web]" (Kello, 2013, p. 17). Cyberspace is likened to Information and Communication Technology (ICT), comprising the Internet and other sophisticated computer-assisted communications. Although some of the ICTs and/or Internet facilities are tangible and installed in the social-cum-physical space or environment, the vast majority of them are not. Nonetheless, they are mainly utilised or made super-functional in the cyberspace to aid human activities, whether prosocial or antisocial.

Virtual environments, cyberspace is arguably characterised by both intended and unintended establishment goals. The former attempts to explain the original and main aim of creating the cyberspace: To catch up with globalisation trends in runaway society. Examples include improved, flourishing global economy and such other structures of society as the legal system, polity, security, and crime prevention and control efforts. The latter, on the other hand, simply refers to the manipulation of the cyberspace. It explains a situation whereby the original conception of this idea is circumvented, subverted, or perhaps supplanted by individual offenders and terrorist groups to perfect in their criminal enterprise. The 2012 United Nations Office on Drugs and Crime (UNODC) report attests to this assertion. The report reveals that, although the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organisations and to transmit information on, as well as material support for, planned acts of terrorism, all of which require specific technical knowledge for the effective investigation of this offence (UNODC, 2012).

Since the 1990s, the Internet has clearly been of growing societal significance which offers terrorists and extremists the same opportunity and capability that it does for the rest of society: To communicate, collaborate and convince (Behr, Reding, Edwards, & Gribbon, 2013). There is a growing concern in both policy reports and academic literature about the use of cyberspace in committing crimes in Nigeria. Currently, Nigeria ranked first in the list of cyber-dependent and cyber-enabled criminal activities in West Africa (see, for detail, Longe & Chiemeke, 2008; Aransiola & Asindemade, 2011; Quarshie & Martin-Odoom, 2012; Whitty, 2018). According to the 2009 Internet Crime Report, Nigeria ranked third globally in four consecutive years: 2006, 2007, 2008 and 2009 as a country where cybercrime is unbridled (National White Collar Crime Centre and the Federal Bureau of Investigation, 2010 cited in Ndubueze, Igbo, & Okoye, 2013).

The problem has led to a plethora of research being conducted on different areas of cybercrime, cyber fraud, and cyber victimisation to curb the menace (see, for example, Longe & Chiemeke, 2008; Adeniran, 2008, 2011; Aransiola & Asindemade, 2011; Tade & Aliyu, 2011; Ojedokun & Eraye, 2012; Ndubueze *et al.*, 2013), as well as cyberterrorism

(see Ibrahim & Muktar, 2017; Manu, 2017). Specifically, there is increasing scholarly attention on the causes, consequences, trends, patterns, prevalence, modus operandi, and prevention and control of conventional or physical terrorism—different from cyberterrorism (Hinshaw, 2014; Hill, 2014; Akanji, 2015; Bamidele, 2016; Anaedozie, 2016; Ordu, 2017; Nnam, Arua, & Otu, 2018). Despite these concerted efforts, the problem persists, with no end in sight. Worse still, only a handful of scientific research effort has (see Karacasulu, 2006; Ajayi, 2012; Look & Kindzeka, 2014; Shola, 2015) specifically examined, in a systematic manner, the nexus between cyberspace and terrorism in Nigeria. Although establishing the cyberspace-terrorism connection has received growing policy and academic attention in the Western world, the problem is seriously under researched in African, especially in Nigeria where the crime is a recurring decimal.

The term 'cyberterrorism' was coined in the 1980s by Barry Collin who described this dynamic terrorism as transcendence from the physical to the virtual realm and the intersection, the convergence of these worlds (Lewis, n.d.; Tafoya, 2011) facilitates the occurrence of the two offending behaviours. According to the Centre for Strategic and International Studies (CSIS), cyberterrorism is the use of computer network tools to shut down critical national infrastructure (such as transportation, energy, and government operations) or to coerce or intimidate a government or civilian population (Lewis, n.d.). It is the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure date or information (Tafoya, 2011). Cyberterrorism is a violence, which is commonly politically motivated, committed against population through the use of or facilitated by computer technology (National Crime Prevention Council, 2011).

Pushing back the frontiers of knowledge on the subject of discussion is of strategic importance in understanding and explaining where, how and why the choice of computers and the Internet as staging point for terrorism. Identifying the missing link and filling-in the gap in knowledge holds strong promise for developing concrete intelligence and strong investigative tools for launching successful and sustained e-counterterrorism. Therefore, the intrinsic interest of this study is to explore the criminogenic activities that take place in the cyberspace, upon which the traditional terrorists/terrorism, particularly members of Boko Haram, acquire the requisite skills and resources with which they use in carrying out and sustaining their terror campaigns.

The Interplay between Cyberspace and Boko Haram Terrorism in Nigeria

The rapid advancement in modern science and technology, coupled with the near-recent evolution of social media networking, has permanently left the door of cyberspace ajar and unmanned. The situation has been exacerbated by such vulnerabilities obviously peculiar to the Internet and computer system as hyper-speed in data retrieval, processing and transfer. Others include convenience, temporality of information, anonymity among users, and lack or total absence of clearly delineated cyber borders. Users, both criminals and non-criminals, currently use it with little or no restriction. Behr *et al.* (2013, p. 3) posited that "the so-called information revolution, with the unexpected rise of the internet since the 1990s, has clearly been of growing societal significance. The internet offers terrorists and extremists the same opportunity and capability that it does for the rest

of society: To communicate, collaborate and convince. There are already significant quantities of radical materials available online, and this volume is growing daily".

There is high level criminogenic infiltration in the cyberspace, which has led to contamination and abuse by most users. It is now a springboard for patterning and reshaping the modus operandi of many traditional crime perpetrators and criminal groups. Offenders now carry out research on the types of crime to indulge in, methods of attack and operation, and how to evade arrest, trial and conviction. Alemika (2017, p. ix), in his foreword to the first and only comprehensive text on cybercrime and cyber criminology in Nigeria (as at the time of this research) titled *Cyber Criminology and Technology-Assisted Crime Control: A Reader*, posited that the cyberspace "has facilitated the ease with which serious crimes such as terrorism, transnational economic and financial crimes as well as political and economic espionages are perpetrated within and across countries".

The use of computer for easy, timely and successful perpetration of different types of terrorism is a growing trend among terrorist groups, including Boko Haram terrorist group. This operational shift in modus operandi has made the offenders more invisible and invincible, as they now hide in the cyberspace to recruit and (re)train members, elicit and disseminate information and intelligence, source for and obtain funds, and acquire weapons, logistics and supplies. In support of this view, the United Nations Office on Drugs and Crime (UNODC) reported that information and communication technology is one of the strategic factors driving the increasing use of the Internet by terrorist organisations and their supporters for a wide range of purposes. And they are: Recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes (UNODC, 2012). At this juncture, it is necessary that these variables are briefly discussed under subheadings to further keep the study in perspective.

Recruitment and Training

Boko Haram sect was founded by Mohammed Yusuf in 2002. Mohammed was earlier a member of a more conservative Moslem group called Izala Society (Mohd, 2017). From the same source, he promoted radical Islam within Izala and later broke out of the group with loyalists in 2002 to form Boko Haram. The first ever recruitment and spread of Yakubu's ideologies was in Izala Society and these were done in face-to-face conversations. With the spread of Internet across Nigeria, social media outlets such as Facebook and Twitter found their ways through the pockets of millennial. Yakubu and his group also adapted their membership recruitment modalities to reach new members through the Internet. As recent as in 2018, the Nigerian Military discovered a recruitment link on one Barde's Facebook account that is used by Boko Haram to find and add members to their group. Below is the graphic narration of the military in this regard:

> …through the suspect's (i.e. Barde) mobile phone, we (Nigerian Military) found several videos soliciting finance for the group. We also found some other videos where Barde was seen preaching Jihad and the ideology of the group. Most of Barde's pictures were that of Abu-Mosad Albarnawi and other Boko Haram fighter posing with Anti-Air craft guns, rockets and Boko Haram flag (Chika, 2018)

Most of the social media strategies for spreading terrorism involve the use of private messages, closed groups, sugar-coated Islamic stories, anonymous hate videos, and other strategies that may not be outright conspicuous. Social media facilitates communication, incitement and inducement. It appears to be the fastest medium through which information is transmitted and certain logistics provided for the purpose of terrorism.

Financing and Funding

The report of the United Nations, submitted by an Analytical Support and Sanctions Monitoring Team, listed extortion, charitable donations, smuggling, remittances and kidnapping as top means through which Boko Haram gets funded (Abdulkareem, 2018). Funding is about the most fuelling yardstick in terrorism; however, it is surprising that most terror groups, such as Boko Haram, acquire so much of these funds with less difficulty. Some of the key routes to this wealth are discussed below:

Extortion: Extortion in this context involves the use of threat of force to make people with financial and nonfinancial resources to relinquish resources to Boko Haram. This occurs in different scenario, both on the Internet and the physical world. A good sample is the use of threat of attack to communities and leaders in Northern Nigeria to make them surrender their financial or nonfinancial resources to the Boko Haram terrorist group. Once this is achieved, the group converts the nonfinancial resources to financial resources and makes it impossible for the entire resources in their possession to be traced. In most cases, these transactions are conducted publicly by less conspicuous allies or members of Boko Haram using social media, online banking, and other Internet-backed financial platforms.

Charitable Donations: This involves the free contribution of financial and nonfinancial resources to Boko Haram. The contributors are not necessarily active members of Boko Haram; they could be villagers in local communities, politicians, religious leaders, foreign or local government agencies, other terrorist organisations, or companies. This is freewill contribution to the radical Islamic course and comes without any mandatory demand from Boko Haram to the contributors. These contributors are sympathisers of Boko Haram who secretly believe in their ideologies or willingly give their supports for certain benefits from the actions of the group. With the existence of the Internet, people or groups easily send their contributions to the accounts or platforms that give the terrorists access to these contributions.

The BBC News of 8 January 2012 reported where President Goodluck Jonathan corroborates the fact sponsors of Boko Haram terrorism were "in the executive arm of the [Nigerian] government; some of them are in the parliament/legislative arm of the government, while some are even in the judiciary arm. Some are also in the [Nigeria] armed forces, the police and other security agencies" (BBC News, 2012). Guitta and Simcox (2014, p. 19) revealed that, "…unfortunately, even with the best intelligence possible, Boko Haram would still thrive due to its supporters' seeming penetration of the Nigerian political and security apparatus". The pertinent question then is: Where (location) and how (online transactions) do these stakeholders donate their resources in

support of Boko Haramism? Of course, the cyberspace is safer for such complicity and unlawful sponsorship compared to the physical space.

Smuggling: The Boko Haram terrorist group resides at the river basin area, bordering Chad, Niger, Nigeria, and Cameroon. With access to these countries and control of their borders, the group easily move illegal goods and services from one country to another and make money from sales of contraband goods and receive kickbacks or financial inducement from services rendered to smugglers. Smuggling in this context does not only entail unlawful importation of goods, but also trafficking of human beings. Drug traffickers also use the cyberspace to fund Boko Haram activities. Lending credence to this, Braun (2008), Rana and Moditsi (2017) reiterated that terrorist organisations worldwide, including Boko Haram, have become heavily involved in the drug trade, so there are hybrid organisations emerging. The hybrid organisations are morphed into one part terrorist organisation and one part global drug trafficking cartel.

The United Nations Office on Drugs and Crime [UNODC] (UNODC, 2017) reported in its Part 5 World Drug Report of 2017 that Boko Haram has reportedly helped drug traffickers to smuggle heroin and cocaine across West Africa. A working example is the trial of 10 alleged Boko Haram members in Chad, where it was established in the court of appeals that a considerable quantity of psychotropic substances had been recovered and that Boko Haram members were regularly involved in the trafficking in and consumption of those substances (see also Nnam *et al.*, 2018).

Remittances and Kidnapping: Boko Haram has also been involved in kidnapping for ransom. Among the kidnapping incidents, the Chibok girls kidnapping saga is not only an unforgettable trauma in the minds of many Nigerians but also a major source of funds for the group. It has nearly sapped the country economically in a bid to rescue the victims. On the 15 April 2014, 276 female students of Government Secondary School, Chibok in Borno State of Nigeria were kidnapped. On extremely cases, the group either sells the kidnapped victims or takes huge ransoms from the government, affected communities, families, or individuals. Some of the victims have allegedly been released after series of ransom had been paid, while others have been radicalised, brainwashed, manipulated and conscripted into the group (for similar argument, see Bloom & Matfess, 2013; Pearson, 2014; Iyekekpolo, 2016; Ordu, 2017; Nnam *et al.*, 2018). These remittances are often made through Internet banking and are added to the Boko Haram's funding sources and strengths.

Propaganda

At inception, Boko Haram as a socio-religious movement had no established goal or perhaps its goals were not clearly defined. The group members simply reclused, withdrew themselves from the rest of community members to camp in remote forest, desert and precarious mountainous terrain. It is interesting to note that Boko Haram, at this point in history, was not violent; rather, the group became unimaginably violent and extreme in their practices and ideologies in 2014. Originally, according to Ordu (2017), Mohammed Yusuf (the founder of Boko Haram Islamic Sect) did not advocate violence, but his

followers had violent encounter with the State security agents. As a result, a full-blown conflict exploded between Yusuf's followers and the Federal Government of Nigeria. Mohammed Yusuf was captured and killed by the police in 2009, together with about "800 of his followers" (Meligard, 2015, p. 1). Those who survived the tragedy dispersed into the villages, reinforced and, having received external/foreign aid, these terrorists have been launching incessant offensive attacks on Nigerians till date (Ordu, 2017).

Their strongest belief is that Western traditions, including education, religion and values, should be abolished or proscribed and replaced with strict Islamic laws, as well as nationwide Islamic governance be instituted in Nigeria. At the heart of members of Boko Haram extremists is the desperation to change the country from a secular State to Islamic theocratic country. These requests are the main rationale behind their killings, and they constantly use bombings, threats, and unexpected incursions to disrupt government operations. All this is made known to the public through cyberspace propaganda,

In their efforts to win more members and sympathisers, the group has devised means of winning the interest of people through online platforms. Many people are brainwashed, manipulated and influenced to join or support Boko Haram cause as a call from Allah (God). These messages are usually spread through social media and digital platforms. Social media is a key tool used by Boko Haram to publicise its propaganda and ideologies. Such propaganda includes milestones, requests, claims, ideals, and the like. On the 15 April 2014, as earlier stated, the group used social media outlets to claim and publicise its adoption of 276 schoolgirls in a school in Northern Nigeria. Little wonder therefore, that Rand Corporation advises that every Nigerian counterterrorism effort should include a nationwide visibility stand that addresses the incursion of Boko Haram on social media (Rand, 2019).

Gathering and Dissemination of Information

Across the world, terror groups thrive on clandestine networks of informants, funders, and intelligence. These networks serve as key channels for information gathering and dissemination. The same scenario applies to Boko Haram, as there have been stories of Boko Haram moles in the Nigerian Military and in other key intelligence agencies. For instance, Olojo (2013), Whitehead (2014), The Guardian (2014), Hill (2014), Bamidele (2016), Nnam *et al.* (2018), Nnam *et al.* (2020) acknowledged that co-ordinated efforts and measures put in place to control terrorism in Nigeria have been sabotaged and frustrated by some civilians in the host communities, politicians and security personnel, who provide corresponding assistance to the terrorists both in the cyber space and the physical space. Another evidence reveals that virtual environments are the main sources of information for the Boko Haram members, and "…there is corruption and sabotage within the military, hindering the fight against this terrorist group" (Ogbonna & Jimenez, 2017, p. 18 cited in Nnam *et al.*, 2018, p. 39).

Radicalisation

Radicalisation is an act of accepting and/or spreading irrational and unguarded radical ideologies that are capable of predisposing recipients to commit acts of terror or which are more likely to expose potential recipients to recruitment by terrorist organisations. Extreme Islamism has been the core preaching and doctrine of members of Boko Haram.

The emphasis is on impacting fanaticism, bigotry and religious intolerance on people. The group employs stringent and strange hazing in training and desocialising convinced or abducted individuals. The aim is to supplant both their social and moral conscience and also severe their psychology in a manner that they become extremely callous, violent and destructive.

The group plants and nurtures high level of hatred in local and international audiences using the social media. The spread of fake news on social media is a common way Boko Haram implants hatred and its ideologies in targeting members (Kate, 2018). Radicalised victims may not directly participate 'in the physical space', but are incline to clandestinely support the terror group either for pecuniary motives or out of religious fundamentalism. And the cyberspace serves as a safer, faster, hidden and suitable location for actualizing this goal.

Cyberspace-Terrorism Nexus: An Integrated Theoretical Perspective

Establishing a link between cyberspace and Boko Haram terrorism is so complex that no single theory can adequately account for it and, as a result, an integration of relevant theories is required to elucidate the core of the problem. Adopting space transition as a central theory, we set out to build a robust theoretical framework by integrating routine activities, social learning, rational choice and crime pattern theories. It has been advocated in the scientific community, particularly in the world of criminology that crime scholars and researchers should always strive to employ integrated model approach or engage in theory deconstruction in analysing the sequential chain of events, especially when a crime is an outcome of several different causes. The goal is to present an interaction of probabilities from different theoretical perspectives that could explain why some people commit crimes (Lanier & Henry, 2004).

Since criminologists have started viewing the emergence of cyberspace as a new locus of criminal activity, a new theory is needed to explain why cybercrimes like cyberterrorism occurs. For this reason, Karuppannan Jaishankar, the doyen of cyber criminology, propounded space transition theory in 2007 to provide a general explanation of the new, emerging crime trend (Jaishankar, 2008). For clarity and broad-based understanding of the growing trends in cybercrimes, cyber-enabled, or technology-assisted crimes and criminality, this theorist came up with seven central tenets of space transition theory:

1. Persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position;
2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime;
3. Criminal behaviour of offenders in cyberspace is likely to be imported to physical space which, in physical space, may be exported to cyberspace as well;
4. Intermittent ventures of offenders in the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape;

5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space. (b) Associates of physical space are likely to unite to commit crime in cyberspace;
6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society; and
7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes (Jaishankar, 2007, p. 7).

The theory of space transition attempts to account for the rapidly increasing rate of cybercrimes proper and criminal activities sustained through the aid of computers and the Internet. This is made possible through globalisation, which has been associated with such technologies as computerisation, miniaturisation, digitalisation, satellite communication, fibre optic and the Internet (Stibli, 2010). A case in point is the obvious social transitions, processes that occur in the cyberspace, wherein terrorists acquire criminogenic knowledge about crime of terror to improve upon and prolong their violent extremism with ease and success. And this is facilitated by the highlighted innovations in ICT and other transition space-based technologies, where several different terrorist groups experience interchange of ideas, intelligence, skills, and logistics. According to the Federal Bureau of Investigation (FBI), the co-ordinated attacks by various terrorist organisations across the globe is linked to high-technology that encourages the proliferation of ICT which is now used by terrorists for destruction of lives and property and to cause public panic (FBI, 1999 cited in Manu, 2017). The cyber is a suitable space for crime-switch, shifting from the intended purposes—for advancement in information and communication technology—to the use of same for unintended objectives, such as to facilitate and co-ordinate terrorist activities.

The basic assumptions of space transition theory, particularly the number one, three and seven principles clearly address the issue of terrorism sponsorship in Nigeria using the cyber space. For instance, the first principle states that "persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position" (Jaishankar, 2007, p. 7). From this particular assumption, as also implicated in assumptions three and seven, that terrorists and their sponsors exist and operate in both physical and virtual environments is, though theoretically tested, a fact to reckon with in the Boko Haram terrorism history. This finds support from existing conspiracy theories about terrorism, which indicate that some politicians, community and religious leaders, and military and paramilitary personnel aid and abet terrorism (for detail, see BBC News, 2012; Guitta & Simcox, 2014; Ogbonna & Jimenez, 2017; Nnam *et al.*, 2018; Itua, 2018; Gudaku, 2019; Nnam, Ogwuoke, Njemanze, & Akwara, 2020). Commonsensically, sponsoring terrorism by these individuals is more convenience and safer in the cyberspace due to their status and position in society. It is no wonder that telecommunication networks and Internet facilities have been intentionally disconnected by the Federal Government of Nigeria (FGN) in the Northern parts of the country where crime of terror is intense.

The reason for the utilisation of cyberspace instead of physical environment as a suitable avenue for supporting Boko Haram activities is not farfetched: Virtually all the spaces in the cyber is transitional, which makes the convergence of participants, deliberations, and

interchange of resources—whether material or human—easier, faster, safer and anonymous. Others, however, may restrained from committing act of terror 'in the physical space' by geographical inhibitions, proximity and 'their status and position' in society. These are predictions of space transition theory, so the adoption of this theory is not only justified but also has provided further validations on its utility, strengths and empirical relevance to both mainstream criminology and the new subdiscipline, cyber criminology. It brings to light the overwhelming strengths of space transition theory and its compatibility with other theories whose underlying principles we integrated to provide a holistic and practical explanation of cyberspace-Boko Haram terrorism connections in Nigeria.

On that score, ideas contained in assumptions two, four, five and six vividly captured the postulations of routine activities, rational choice and social learning theories. For instance, principles two (i.e. "Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime") and four (i.e. "Intermittent ventures of offenders in the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape") are particularly tied to the beliefs of routine activities theory advanced by Lawrence Cohen and Marcus Felson in 1979. These theorists explained that structural changes which occur in routine activity patterns influence crime rates by affecting the convergence in time and space of three interactive factors or elements of direct-contact predatory crimes, such as armed robbery, kidnapping, and terrorism. Example of these elements are the availability of suitable targets, the absence of capable guardians/guardianship, and the presence of motivated offenders. While the absence of any of these factors tends to prevent crime from occurring, the presence of one or more of them may precipitate crime (Cohen & Felson, 1979). The cyberspace and its borders are naturally porous, characterised by insecurity. Routine activities conducted online activities are not adequately protected (lack of capable guardians) due to the transient, anonymous and clandestine nature of cyberspace. Here, computers and Internet devices as well as their owners, users, or operators, who are mainly human beings, are suitable targets of several different forms of terror within and/or outside the virtual environments.

The terrorists and their sponsors remain the motivated offenders, who frequently surf the net for digital information, intelligence, enlistment, sponsorship and communication, which are impermanent by nature and subject to alteration, defacement, manipulation, or deletion within a twinkle of an eye. To improve upon or perfect in their chosen career, terrorists take advantage of the complexities and unsecured nature of the Internet connectivity and other ITC devices to surreptitiously research crime of terror and thereafter translate the knowledge so acquired into use—the perpetration of terrorism in the physical space. These activities are often well co-ordinated, learnt, rehearsed and rationalised, first in virtual environments such as the computers and mobile phone channels connected to the Internet, and later, perfected in the real world. This is where space transition and routine activities theories intersect with rational choice and social learning theories to further identify and address the phenomenon under investigation. Ajayi (2012) and Shola (2015) attested that there are ties (which are borne out of rational choice and learning behaviour) between terrorist groups which facilitate activities between

Boko Haram in Nigeria and Al-Qaeda in the Maghreb (Libya, Algeria, Tunisia, and Morocco), Hezbolla in Lebanon, Al-Shabab in Somalia, and the Islamic State of Iraq and Syria.

Learning the art and science of terrorism in the cyberspace is a rational choice, and rational choice theory is particularly anchored in two principles: Offence-specific crime and offender-specific crime. The former explains that offenders react selectively to the characteristics of particular offence, while the latter maintains that criminals (including terrorists) are not simply automatons who, for one reason or another, engage in random acts of antisocial behaviour (Phillips & Votey, 1987). Therefore, terrorism is a learnt and premeditated violent organised crime. The act is not initiated or committed on the spur of the moment, but rather requires serious, calculated and meticulous thoughts before decision is made, conclusion reached and action taken, suggesting that terrorism is not all-comers affairs. Indeed, thought-out plans are made and rational decision taken prior to recruitment of members, attacking targets, and exploring why, where and how to obtain and spread information and other assistance. From our theoretical orientation, terrorists pass through intensive criminogenic learning processes and military hazing and training, which are usually made available and accessible on the Internet.

The basic assumptions of crime pattern theory are in strong support of the preceding viewpoint. Crime pattern theory, which is a systematic combination of rational choice and routine activities theories, focus on the manner in which victims, locations and offenders influence the distribution of crime events over time and space (Brantingham & Brantingham, 1993; Ikoh, 2011; Nnam, 2015; Nnam, Okogwu, & Adinde, 2018). Applying the tenets of crime pattern theory to the study of symbiotic relationships between cyberspace and Boko Haram, we argued that terrorists are rational offenders who carry out their routine activities (terrorism) after learning the requisite skills and neutralisation techniques in such places, locations as cyberspace. In this location, many 'suitable targets' (avalanche of unprotected and *easy-to-hack* information readily available and easily accessible, and unsuspecting computer users) are typically found with no capable guardians to stop 'motivated offenders' who always navigate the cyberspace looking for targets. They are most likely to succeed when their identified targets 'lack capable guardianship' (weak national cybersecurity network, porous cyber borders, and ineffective cyber patrol). Among the terrorists' sources of sending and receiving resources, both material and human, the cyberspace is or provides a suitable opportunity for achieving those terroristic goals.

On the whole, there is dearth of theories that specifically and directly underpin cybercrimes, particularly cyberterrorism, in the criminology literature. At present, only one theory (space transition theory by Jaishankar, 2007, 2008) exists in this regard, suggesting a dire need for additional theories to support future critical enquiries into the subject matter. Thus, integrating space transition, rational choice, social learning, routine activities and crime pattern theories is both a practical way of expanding the narrow horizons on theoretical knowledge about cyber criminology and a means of setting the pace for theory building and theory deconstruction for thorough understanding of the nuances of cyberterrorism and other cybercrimes. Again, incorporating these conventional criminological/victimological/sociological theories into cyber criminology is an attempt to bridge the gap in both empirical and theoretical knowledge in the new subfield. Their

relevance, utility and application is both interdisciplinary and multidisciplinary in nature, and can be adopted to predict and explain the same or related phenomenon in such disciplines as Sociology, Mass Communication, Political Science, Psychology, Library and Information Science, Computer Science, Law, Criminal Justice Administration, and indeed, Criminology and Security Studies where Cyber Criminology is domesticated.

Conclusion and Policy Implications

The nexus between cyberspace and terrorism in Nigeria has been critically examined and explored, with both theoretical and empirical evidence showing a significant relationship between the two variables. Indeed, the subarea of cyber criminology generally, and cybercrime in particular, is critically under researched in Nigeria. Although the problem has received adequate scholarly attention in the Western world, as evidenced by a large volume of literature on the topic, it has received comparatively far less attention in Nigeria and thereby making the war on terrorism an effort in futility while the terrorists are having a field day in their daily atrocious operations. Ndubueze (2017, p. xiv), a leading advocate of cyber criminology in Nigeria, has this to say:

> Since the establishment of cyber criminology in 2007 by an Indian Criminologist, Professor Karuppannan Jaishankar, the new subdiscipline seems to have been suppressed by the mainstream criminology and the various research efforts that relate to it are largely Western. Although Nigerian cyberspace is increasingly vulnerable to deviance, crime and terror, it is noted that not so many advances have been achieved by criminologists in Nigeria in form of understanding the dynamics of these critical developments. There seems to be a shortage of dedicated cyber criminologists and a dearth of cyber criminology textbooks (and other instructional materials) in Nigeria, even if for reference purposes.

The cyberspace has complex characteristics that make detection and apprehension of cyberterrorists very difficult, especially through traditional law enforcement measures. As implicated in the integrated theoretical framework, both materials and human beings in virtual environments are naturally vulnerable (suitable targets with little or no capable guardianship) to deviance, crime and terror. Showing their compatibility and relevance to the study, for instance, all the five theories we integrated emphasised that learning the intricacies of terrorism and their applications is bidirectional. Firstly, the crime of terrorism is either imported or exported from unguarded and threat-prone location, which could be physical or cyber environment, aimed at reducing input and enhancing output. Secondly, and more importantly, learning and acquiring the paraphernalia of terrorism is more common in virtual environments, since the risk of failure and arrest is very insignificant while the chances of success and escape are highly significant in the latter when compared to the former.

The cyberspace-terrorism nexus is a transnational problem that requires multilateral synergy among international criminal justice systems for effective prevention and control. Consequently, understanding 'what goes on' in virtual environments through intelligence-led law enforcement and constant cyber-surveillance is a strong lead to understanding 'what works'. This suggests that a concerted effort is needed to push back the frontiers of

knowledge on the crime for practical solution and consolidate African (cyber) criminology. Indeed, the strength of this article lies in its attempt to provide additional insights into the study of Boko Haram terrorism by revealing the 'how' and 'why' of cyberspace as a teaching, learning and research centre for terrorists. Gaining insight into this operational shift stands to orient a practical crime-prevention-control approach that will provoke radical and pragmatic counterterrorism policy and action.

Further research, particularly data-based studies, is needed on the subject matter to further empirically test claims, constructs and theories about the use of cyberspace by members of the Boko Haram group for the purpose of perfecting in their terroristic operations. Many of the policy documents and academic literature in this area is of Western background. Hence, the current study has implications for policy development and to understand the strategic importance of cyber criminology as a discipline with much potentials to effectively combat terrorism within and outside the virtual environments.

Since both the offence and the offenders involve syndicates, with regional and global networks, local and international cybersecurity partnership becomes imperative for Nigeria at this point in history. Such co-operation holds strong promise for evidence-based harm reduction and safer space through constant cyber patrol, monitoring and law enforcement. Research suggests that law enforcement agencies responsible for investigating terrorism, including cyber terror, must remain vigilant. This includes ensuring adequate funding for staffing, equipment, and training. But, beyond that, local law enforcement officers must encourage citizens to be alert and to report suspicious behaviour (Tafoya, 2011). Proactive, rather than reactive cyber counterintelligence, is also recommended. This also has policy implication for the European Union (EU) online deradicalisation approach. The idea is aimed at preventing access to terrorists in an attempt to disrupt recruitment efforts on the Internet, cyberspace. Adopting this strategy will go a long way in bringing the problem under effective prevention and control.

References

Abdulkareem, H. (2018, July 30). How Boko Haram is funded – UN. *This Day,* p 51.

Adeniran, A. I. (2008). The internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368-381.

Adeniran, A. (2011). Café culture and heresy of yahooboyism in Nigeria. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behaviour* (pp. 3-12). Boca Raton, FL, USA: CRC Press.

Ajayi, A. I. (2012). Boko Haram and terrorism in Nigeria: Exploratory and explanatory note. *Global Advanced Research Journal of History, Political Science and International Relations, 1*(5), 103-107.

Akanji, O. O. (2015). Security crisis in Nigeria: Boko Haram insurgency and prospects of peace. *Conflict Studies Quarterly Special Issue, 7*, 58-73.

Alemika, E. E. O. (2017). Foreword. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. ix-x). Zaria: Ahmadu Bello University Press.

Anaedozie, F. (2016). Has the emergence of female suicide bombers in Nigeria depicted the exploitation of feminine vulnerability? A critical appraisal of Boko Haram's female

suicide bombers in Nigeria. *International Journal of Innovative Research & Development, 5*(3), 217-227.

Aransiola, J., & Asindemade, S. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759-63.

Bamidele, O. (2016). Combating terrorism: Socioeconomic issues, Boko Haram, and insecurity in the north-east region of Nigeria. *Military and Strategic Affairs, 8*(1), 109-131.

BBC News. (2012, January 8). Nigeria's Goodluck Jonathan: Officials back Boko Haram. Retrieved from https://www.bbc.com/news/world-africa-16462891.

Behr, I. V., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*. Santa Monica, CA: RAND Corporation.

Bloom, M., & Horgan, J. (2015, 17 February). The rise of the child terrorist: The young faces at the frontline. *International Chronicles*, p. 17.

Braun, M. (2008). *Drug trafficking and Middle Eastern terrorist groups: A growing nexus?* Washington DC: The Washington Institute for Near East Policy.

Brantingham, P. L., & Brantingham, P. J. (1993). *Environment, routine, and situation: Towards a pattern theory of crime*. New York: Crime Prevention Studies.

Chika, E. (2018). Army discovers sect's recruitment portal on Facebook, Instagram, others. *Pulse News.* Retrieved from https://www.pulse.ng/news/local/boko-haram-army-discovers-sects-recruitment-portal-on-facebook-instagram-others/dffy78j. Accessed 20 February 2019.

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

Gibson, W. (1986). *Neuromancer*. Bloomfield, MI: Phantasia Press Edition.

Gudaku, B. T. (2019). Boko Haram: The birth, geography and hypotheses responsible for the sustenance of the conflict in Nigeria. *International Journal of History and Philosophical Research, 7*(1), 12-24.

Guitta, O., & Simcox, R. (2014). *Terrorism in Nigeria: The threat from Boko Haram and Ansaru*. London: The Henry Jackson Society.

Hill, J. N. C. (2014). Boko Haram, the Chibok abductions and Nigeria's counterterrorism strategy. *Combating Terrorism Centre Sentinel, 7*(7), 15-17.

Hinshaw, D. (2014). World news: Boko Haram insurgents kidnapped more girls in Nigeria. The *Wall Street Journal, 9*(6), 1-16.

Ibrahim, B., & Muktar, J. I. (2017). Emerging cyber-terrorism threats. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 415-428). Zaria: Ahmadu Bello University Press.

Ikoh, M. U. (2011). Crime victimisation, safety and policing in Nigeria. In E. E. O. Alemika, & I. C. Chukwuma (Eds.), *Criminal victimisation in Nigeria: Pattern and trend* (pp. 41-100). Lagos: Malthouse Press.

Itua, F. (2018 April 18). Insecurity: Senators demand sack of service chiefs. *Daily Sun,* p. 6.

Iyekekpolo, W. O. (2016). Boko Haram: Understanding the context. *Third World Quarterly, 37*(12), 2211-2228.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology, 1*(2), 7-9.

Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro, (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Karacasulu, N. (2006). Security and globalisation in the context of international terrorism. *Ulusalarasi Hukuk ve Politico Cilt, 2*(5), 1-17.

Kate, C. (2018). Combating the problem of online radicalisation in Africa. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2018/11/combatting-the-problem-of-online-radicalization-in-africa/.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security, 38*(2), 7-40.

Lanier, M., & Henry, S. (2004). *Essential criminology* (2nd ed.). Boulder: Westview Publishers.

Lewis, L. (n.d.). *Assessing the risks of cyber terrorism, cyber war and other cyber threats.* Retrieved from http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

Longe, O. B., & Chiemeke, S. C. (2008). Cybercrime and criminality in Nigeria – What roles are Internet access points playing? *European Journal of Social Sciences, 6*(4), 132-139.

Look, A. & Kindzeka, M. E. (2014). *Are Nigeria's neighbours safe havens for Boko Haram?* VOA News. Retrieved from www.voanews.com/content/are-nigerias-neighbours-safe-havens-for-boko-haram/1878522.html.

Manu, Y. A. (2017). Globalisation, cyber-terrorism and Nigeria's national security. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 395-411). Zaria: Ahmadu Bello University Press.

Meligard, E. (2015). *What is Boko Haram*? Retrieved from http://geopolitics/commentaries/backgrounder/what-bo.

Mohd, B. Y. (2017). *Terrorism in Nigeria: History of Boko Haram attacks in Northeastern Nigeria and their collaboration with the world terrorist called "ISIL".* Retrieved from https://www.globalethicsnetwork.org/profiles/blogs/terrorism-in-nigeria-history-of-boko-haram-attacks-in.

National Crime Prevention Council. (2011). *Cybercrimes.* Retrieved from www.ncpc.otg.

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cybercrime victimisation among Internet active Nigerians: An analysis of socio-demographic correlates. *International Journal of Criminal Justice Sciences, 8*(2), 225-234.

Ndubueze, P. N. (2017). Preface. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. xiv-xv). Zaria: Ahmadu Bello University Press.

Nnam, M. U. (2015). *The sociological analysis of kidnapping in Abia and Ebonyi states of Nigeria* (MSc Dissertation). Department of Psychology and Sociological Studies, Ebonyi State University, Abakaliki, Nigeria.

Nnam, M. U., Okogwu, F. I., & Adinde, K. U. (2018). Towards crime prevention and control in the library system: Old and new perspectives. *International Journal of Criminal Justice Sciences, 13*(1), 137-145.

Nnam, M. U., Arua, M. C., & Otu, M. S. (2018). The use of women and children in suicide bombing by the Boko Haram terrorist group in Nigeria. *Aggression and Violent Behaviour, 42*, 35-42.

Nnam, M. U., Ugwuoke, C. O., Njemanze, V. C., & Akwara, F. A. (2020). Boko Haram terrorism and human security in Nigeria: Matters Arising. *Journal of Aggression, Maltreatment and Trauma*, *28*(10), 1-23. DOI: 10.1080/10926771.2019.1710637.

Olojo, A. (2013). *Nigeria's trouble north: Interrogating the drivers of public support for Boko Haram.* ICCT Research Paper, October 2013, 6.

Ogbonna, C. C., & Jiménez, J. A. R. (2017). The inordinate activities of Boko Haram: A critical review of facts and challenges. *Universidade De Santiago De Compostela, 16*(2), 9-24.

Ordu, G. E. O. (2017). Trends and patterns of Boko Haram terrorist and militants' aggression in Nigeria. *Aggression and Violent Behaviour, 37*, 35-41.

Pearson, E. (2014). Boko Haram and Nigeria's female bombers. *Nigerian Security, 35*(5), 19-21.

Philips, L., & Votey, H. (1987). The influence of police intervention and alternative income sources on the dynamic process of choosing crime as a career. *Journal of Quantitative Criminology, 3*, 25-274.

Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computer Science and Engineering, 2*(6), 98-100.

Rana, R., & Moditsi, K. (2017). *The linkage between illicit drug trafficking and terrorist groups*. Retrieved from http://www.ib-2017-first-drugs-and-terrorism.pdf.

Rand Corporation. (2019). *Social media in Africa presents double-edged sword for security and development*. Santa Monica, California: The Author.

Shola, (2015). Globalisation of terrorism: A case of Boko Haram in Nigeria. *International Journal of Politics and Good Governance, 6*(1), 1-22.

Siegel, L. J. (2008). *Criminology* (3rd ed.). Belmont, California: Thomas Higher Education.

Stibli, E. (2010). Terrorism in the context of globalisation. *AARMS, 9*(1), 1-7.

Tade O., & Aliyu, I. (2011). Social organisation of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860-875.

Tafoya, W. L. (2011). Cyber terror. *FBI Law Enforcement Bulletin* (FBI.gov), November. Retrieved from https://leb.fbi.gov/articles/featured-articles/cyber-terror.

The Guardian. (2015, 22 February). *Girl as young as seven kills herself and five others in Nigeria suicide bombing*. Retrieved from http://www.Theguardian.

United Nations Office on Drugs and Crime. (2012). *The use of the internet for terrorist purposes*. Vienna: The Author.

United Nations Office on Drugs and Crime. (2017). *The drug problem and organised crime, illicit financial flows, corruption and terrorism* (Part 5). Vienna: The Author.

Ussing, S. (1968). *Cyberspace, collages, dry transfers and photolithography*. Retrieved from https://www.pinterest.co.uk/pin/308074430744549409/.

Wiener, N. (1948). *Cybernetics: Or control and communication in the animal and the machine*. Paris: MIT Press.

Whitehead, E. (2014). *Corruption in the military, police and among politicians thwarts Nigeria's fight against Boko Haram*. Good governance Africa, No. 42. Retrieved from http://gga.org/stories/editions/aif-26-dirty-dealings/dodgy-defenders.

Whitty, M. T. (2018). 419 – It's just a Game: Pathways to cyber fraud criminality emanating from West Africa. *International Journal of Cyber Criminology, 12*(1), 97-114.