Information Technology as an Indispensable Security Tool: Nigeria's Boko Haram Sect in Focus.

Chinda, F. E.[1], Shuaibu, A. N.[1] and Dyikuk, J.[2]

[1]University of Jos, Plateau State, Nigeria.
[2]Centre for the Study for African Culture and Communication (CESACC), Catholic Institute of West Africa (CIWA), Nigeria.

Esxon Publishers

Information Technology as an Indispensable Security Tool: Nigeria's Boko Haram Sect in Focus.

Chinda, F. E.[1], Shuaibu, A. N.[1] and Dyikuk, J.[2]

[1]University of Jos, Nigeria.
[2]Centre for the Study for African Culture and Communication (CESACC), Catholic Institute of West Africa (CIWA), Nigeria.

Abstract

Today the world is contending with the sad phenomenon of global terrorism. What is more frightening is the sophistication of the modus operandi of terrorist groups who cash in on the benefits of Information and Communications Technology (ICT) to cause mayhem to unsuspecting members of the public. This qualitative paper titled, "Information Technology as an Indispensable Security Tool: Nigeria's Boko Haram Sect in Focus" used the Digitalizing Crime Prevention Theories as theoretical frameworks to ascertain the use of ICT as a security tool for quelling the threatening activities of Boko Haram. The study discovered that the sect uses the dynamics of ICT such as posting amateur videos on social media platforms to intimidate the citizenry and threaten the peace of the nation. It recommended establishment and enforcement of cyber-laws and proscription of online hate speeches as possible panacea to the fight against terror. The paper concluded that since terrorist groups often form an alliance with other terrorist organizations around the world as an operational strategy, the United Nations, various governments, Non-Governmental Organizations, security agencies and spirited individuals must embrace online vigilance and also form a global synergy to nip the menace of global insecurity in the bud. In the estimation of the authors, the rudiments of ICT remain an indispensable security tool for bringing Nigeria's number one terrorist organization down to its knees.

Introduction

In the world today, the ability to store information in computers facilitates easy access and sharing of information by various users (Beebe & Rao, 2005). The competitive global information super highway (Dyikuk, 2017) offers people free access to information in such a manner that communication is not only easy but also learning and education. Nowadays, real-time, face-to-face communicating is being replaced by social media communication which seemingly provides unlimited access for individuals to share and exchange banters, photos and even do business with friends or business associates.   In the midst of the uncontrollable glow of information lies the potency of control, dominion and even exploitation. It is not surprising, therefore, that global peace is threatened as various insurgencies are increasing by the day. The more various governments of the world are updating counter insurgency initiatives to climb down on militant groups, the more emboldened these sects appear. From the transatlantic proliferation of small arms to the more threatening explosion of technologically enhanced tactics of terror groups who cause fear and inflict pain leading to death, the global war on terror is far from finished. Therefore, it is no longer an assumption that the advancement of technology and a media-savvy populace provides a leeway for faceless people to not only threaten the peace of societies but also cause harm to unsuspecting members of the public. From the London bombing, to the sporadic shooting in America through the recent bomb blast in Mubi, Adamwa State, Nigeria is story is the same – one of fear, suspicion and consternation.

Terrorists' organizations like the dreaded Boko Haram in North Eastern Nigeria daily take advantage of social media platforms for access to information and also spread their propaganda ideologies. That is not all, the media also provides them with the opportunity of showcasing their weaponry, intimidating security agencies and countering claims of defeat by government armed forces. The utilization of the rudiments of ICT by the insurgencies has opened the eyes of the world to the reality of an apparent synergy between local sects and their splinter groups as well as that between larger militant groups and their mentors abroad. Technology underpins Boko Haram's ability to operate (Barkindo, 2017). This expands our discussion to the probable links between Al Qaeda and Al Shabab in the Islamic Megrip with an erstwhile Kala Kato and currently Boko Haram in Sub-Saharan Countries like Nigeria. Boko Haram also recruits from other extremist but non-violent groups in the region like *Aljana Tabbas, Medinatu al-Keffi* and *Kala Kato* (Barkindo, 2017). This is because, organised crime syndicates (Radlicki, 2015). These and other international terrorist groups have cashed in on the indispensable role of ICT to show solidarity and the big-brother kind of "fellow feeling" for smaller sects – this they do by way of training in countries like Sudan, Somalia, Afghanistan, Pakistan to mention just a few. The unabated killing, destruction of lives and property by Boko Haram is not only a cause of worry for the Federal Republic of Nigeria but also its nieghbours like Niger, Cameroun and Chad but indeed the world over. The destruction carried out by the sect is a humanitarian crisis of monumental proportions. It was the abduction of over 270 Chibok schoolgirls from their dormitory on 14 April 2014 (Adekunle, 2017 & Lichter, 2014) that opened the eyes of the international community to the alarming atrocities of the sect. Many other atrocities like abduction and killing of children, women, expatriates, security agents and politicians further put Boko Haram on the terror index as the deadliest terrorist group (Okoro, 2017).

Aside from targeting government institutions, schools, places of worship, markets and motor-parks, the insurgents sometimes pay surprise visits to villages where they gather the people and preach to them before publicly executing those they feel deserve to die – Top politicians, local chiefs (emirs as they are called) and religious leaders have also not being spared of their venom. Part of their strategy is to attack military installations – often times, if they succeed, they go ahead to raid financial institutions as part of boosting their pecuniary kitty. With these monies, they are able to pay families of suicide bombers, spies, cooks, drivers and other staff. Perhaps the bombing of the United Nation's House by a suicide car bomber in Abuja on August 26, 2011 in which 18 people were reportedly killed (Gardner, 2011) was Nigeria's 9/11 which made the of nations of the world more concerned about the urgent need for synergy in tackling the menace. However, the lack of political will, bribery and corruption continued to slow down the expected global solidarity to expel the insurgents from the West African country (Danjuma cited by Ogbeche, 2016). Barkindo stresses that impunity which has become a norm in Nigeria leads to excessive forms of violent conflict and crimes (2013).

Therefore, this study aims at: Investigating the use of ICT by the Boko Haram sect as ideological and pragmatic tools of engagement; Ascertaining the operational ideology of the sect in a view to finding its causes and possible panacea; Establishing the indispensable role of ICT in the fight against Boko Harm insurgency; accessing the role of education, empowerment and other non-combatant approaches in putting the insurgency in check; Arguing for embracing the essentials of de-radicalization and reorientation of insurgents towards positive use of ICT; and because of the danger insecurity poses to global peace, the study is significant. It is also crucial because militia groups are opportunists who always think ahead of others in terms of strategy and execution. This means that their opportunism opens the window which social media offers like Facebook, Twitter, Instagram, LinkedIn, WhatsApp to mention just a few – which makes the case for using ICT as a legitimate and most urgent security tool. This study makes a case for engaging members of the sect in their comfort zone which namely, digital warfare.

Method of Analysis

This paper adopts the qualitative method of reviewing relevant literature on the matter under review by juxtaposing these views in order to arrive at an informed opinion about the use of ICT as an indispensable security tool for tackling Boko Haram. Since getting the insurgents to interview them would have amounted to a security risk, the authors used the qualitative method. This is because the study would be biased if the authors employed the quantitative method of study which would have involved interviewing only the public without getting the opinion of the insurgents.

Deconstruction of Concepts

In this study, information technology is used as short form of Information and Communications Technologies (ICT). These refer to all modern digital platforms used for computation of ideas, generation and dissemination of information, as well as monitoring and processing of information. In this paper, information technology is employed as the infrastructure and components that enable modern computing (Rouse, 2017) and disseminating of information by insurgent groups for intimidation and execution of threats which often leads to destruction of lives and property.

Boko Haram

Boko Haram, is a militant Islamic group which climbs down on education, western civilization and secular authority. It goes by the official Arabic name of *Jama'atu Ahlis Sunna Lidda'awati wal-Jihad* which translates as: "People Committed to the Propagation of the Prophet's Teachings and Jihad" (BBC, 2016). The sect promotes a version of Islam which forbids Muslims from taking part in any socio-political activity that has links with Western Education. The sect is an ISIS-aligned jihadist group based in Nigeria but also operates in Cameroon, Chad and Niger (Counter Extremism Project, 2017, p.1).

Theoretical Framework

This paper adopts *Digitalizing Crime Prevention Theories* as theoretical framework. These theories came out of certain traditions. In the last three decades, there have been two main theoretical traditions in crime prevention studies. These are the victimization perspective and the social control perspective. While the former considers the victim, offender and environment, the latter considers the informal role community and family members play in influencing the moral values of potential insurgents. Both the victimization and social control perspectives are employed as theories of crime prevention which focus on modifying behavior of potential offenders (Lewis & Lewis, 2011). Despite the loftiness of these two theories in the detection and prevention of crime, scholars have criticized them for not taking into cognizance the invaluable role of technology in the modus operandi of insurgents on the one hand and the innocent victims of violent crime on the other. To this end, Lewis and Lewis (2011) proposed an addendum to the extant victimization perspective and the social control perspective of crime prevention. In their work, "Digitalizing crime Prevention theories: How Technology Affects Victim and Offender Behaviors," the scholars attempted to "digitalize" the theories of crime prevention. They argued that since technology influences the lives of both potential offenders and victims, it is important to use the existing principles of victimization perspective and social control perspective to propose the use of technology as an indispensable security tool. While acknowledging the limitation of the victimization and social control perspectives in holistically addressing the use of information technology for checkmating insurgencies, the authors contended that technology has a great influence on how information is gathered, processed and disseminated. They further proposed that technology should be situated within the context its usage understand and predict criminal behavior and averting same (Lewis & Lewis, 2011). Because this study makes a case for information technology as a vital security tool for tackling Nigeria's Boko Haram sect, the authors have employed the *Digitalizing Crime Prevention* Theories as appropriate theoretical framework for this paper.

Boko Haram: Early beginnings and Ideology

Islamic radicalism has increased in Nigeria since the 1960s (Counter Extremism Project, 2017, p.1). From time one, the emergence of sects like the Maitasine was to spell doom for the country. Many people believe that what is today known as Boko Haram is an old version of the Maintatsine movement which was led by the Cameroonian born Muhammadu Marwa. The cruel activities of the sect led to bloody clashes in Northern Nigeria between 1980 and 1984. It would appear that the resilience and guerilla tactics of Maintatsine was pregnant for another sister sect in the future.
When Boko Haram came on board, the sentiments did not change. While it is believed that the Boko Haram insurgency started in 2002, (BBC, 2016) others hold that it began in 2004 (Radlicki, 2015). On its part, the Nigerian army put the year which the insurgency started as 2009. The activities of the group were inimical to national security. This made the government to not only proscribe the sect but take a decisive step putting their activities to a halt. This led to the death of their leader and founder Mohammed Yusuf (Burutai, 2017). Yusuf's death opened a new page in the annals of the militia group as his next in command, Abubakar Shekau released a video in July 2010 claiming to be the next leader of the group (Burutai, 2017). This video emboldened the commanders who vowed to avenge the death of their leader. By 2012, the state of security in the country was a grave yard experience especially in the North East where the security of lives and property deteriorated into a Hobbesian State of nature which created a situation of anarchy, collapse of law and order and survival of the fittest (Dyikuk, 2012). From that time on through 2013, frequent explosions, killings and destruction became the order of the day.The "People Committed to the Propagation of the Prophet's Teachings and Jihad" (BBC, 2016) promotes a brand of Islam which forbids Muslims from partaking in any social or economic activity which relates to Western Education. Aside from Nigeria as it operational base, the sect also operates in Cameroon, Chad and Niger (Counter Extremism Project, 2017, p.1) were they destroy lives and property in an endless guerilla war.

As adherents of proselytism and holy war, they believe that "Western Education is a sin" in the regional Hausa Language. They are committed to the establishment of an Islamic State or Caliphate in Nigeria. They operate in compliance with the strict principles of Sharia Law. Their leader Abubakar Shekau would justify the abduction of women by claiming that, the sect holds that "In Islam, it is allowed to take infidel women as slaves" (Lichter, 2014).
It was therefore not surprising the insurgents abducted over 270 schoolgirls at a Chibok Secondary School on 14 April 2014 (Adekunle, 2017). Since most of the girls who were kidnapped were Christian, they were allegedly forcefully

converted to Islam and sort to trade them with Islamists who were in government's custody (Lichter, 2014). Through the dogged efforts of civil society groups like the Bring Back the Girl's Campaign (Bring Back Our Girls, 2017), some of the schoolgirls were released. Others are still in captivity.

Deaths, Destructions, Humanitarian Crisis and the Sect's Use of ICT

Based on estimates, Boko Haram insurgency has made 2,114,000 people Internally Displaced Persons (IDPs) as at December of 2016 - 537,815 in separate camps, 158,201 at official camps in Maiduguri; 52,311 orphaned, 54,911 widowed and the death of almost 100,000 persons (Shettima cited by Tukur, 2017). The group has also burnt over 200 schools (Lichter, 2014) in an attempt to defend their Islamic ideology of not only proscribing Western Education which they perceive as corrupt but expunging it. This puts the destruction of the militants as a humanitarian crisis (Osinbajo, cited by Tukur, 2017). Their tactics includes widespread recruitment, abductions, sexual violence, attacks on schools, increased use of children as suicide bombers and inflicting of horror on children Nigeria's north-East (Gamba, 2017). As at October 2016, Boko Haram activities resulted in more than 20,000 deaths and 5.5 million displacements in the Lake Chad basin (Barkindo, 2016). In 2014, the Global Terrorism Index disclosed that Boko Haram killed more people numbering 6,644 in terror attacks than any other group (Alfred, 2015). Commenting on its devastating and corrupting influence, a consultant on countering violent extremism, Zenn notes that the hostage taking of wealthy individuals and weapons smuggling in Nigeria and Cameroon risks creating a multi-million dollar "terrorism economy" in the South Sahel which fuel corruption and also raises tensions between neighbouring countries as well as Muslims and Christians in the region (2014). Even though the Civilian Joint Task Force, mercenaries, local hunters and vigilantes are involved in fighting Boko Haram, the insurgents have not been expelled (Barkindo, 2016). Kukah argues that exclusive policies which sought to privilege a tiny, unproductive and selfish elite whose gargantuan greed only fed it led to the Boko Haram crisis (cited in Nwafor, 2017). He contends that a hypocritical elite who believe that it can claim the benefit of democracy but only use it to consolidate power, laid the foundation of Boko Haram. The cleric and social critic also blames the northern elite for not living up to their dubious creed of being Muslims by preaching Sharia Law for only the poor and encourage education while own people are held in the bondage of ignorance (Kukah, cited by Buari, 2016).

Boko Haram insurgents are knowledgeable in the use of cyber operations. In fact, they use the media to their advantage (Al-Harthi, 2014). The terrorists use computer generated intelligence to execute their atrocities (Burutai, 2017). As a propaganda tool, the insurgents are skilled in posting amateur videos on social media. The video Abubakar Shekau released in July 2010 in which he claimed to be the next leader of the group (Burutai, 2017) was the first in the series of videos the group would make public. Experts believe that the video containing the gory account of how security agents publicly executed the Boko Haram leader, Yusuf Mohammed by Mike Hanna of Al Jazeera was not only blood chilling but may also have set the tone for the viciousness of post Yusuf Boko Haram (Kukah, 2016). The said video and others in which the police publicly paraded and killed suspected members of the sect arbitrarily without trail were viral on social media. This further infuriated members of the group. Apparently, their commanders garner morale for more violent attacks on military and financial installations, churches markets, parks and other crowded places where people meet. This may have set the tone for a change of tactics for the sect – from raids of houses and few abductions, to full scale recording of war on communities, more abductions, burning of houses and killing of security agents by the militia group. The militants use sermons, leaflets and videos to rail against education of girls (Lichter, 2014). These sermons are often preached to either their hostages or in villages where they lay siege and hold everyone to ransom. After preaching such sermons, they sometimes flock offenders or execute erring locals. The leaflets are thrown in the air in villages where they have a stronghold hold – the Islamists believe that locals would read them and act accordingly. Their ICT team often records the messages and activities for dissemination to the public.

Boko Haram's Global Links

Boko Haram has international links. Internationally, the jihadist sect, Boko Haram is also known as the most famous manifestation of Salafism in Nigeria. Being a global movement, Salafism has its stronghold in Saudi Arabia. Unlike mainstream Salafism, extreme Salafism subscribes to purist, scholarly or quitism to exhibit deadly forms of Jihad or Holy war aimed at proscribing Western Education and Christianity. It is in this regard that Boko Haram and Al-Qaeda are Salafi-jihadis (Campbell, 2017). In the same vein, Wahhabism which was founded by Mohammed Ibn Abd al-Wahhap (1903-92) is seen as the reactionary branch of Islam from Saudi Arabia which was transformed by Ibn Taymiyyah into a violent form of Islam is said to be the main inspiration of Boko Haram as well as the global source of terrorism as seen in table 1(Telegraph Reporters, 2017).

In March 2015, the Nigerian jihadist group publicly pledged it allegiance to Islamic State (Gartenstein-Ross & Zenn, 2016). Since then, it is believed that the sect recruits Jihadists from neighboring Cameroon and Niger to help it wage jihad in Nigeria. Besides that, some Boko Haram members have left the country as foreign fighters to the Middle East or South Asia (Counter Extremism Project, 2017, pp.1-2). It also believed that Boko Haram's reintegration into al-Qaeda's network may give the sect an immediate boost by linking it with other growing insurgencies (Gartenstein-Ross & Zenn, 2016). Zenn maintains that the sect is something more than a domestic Nigerian movement (2012). This shows that the sect shares many things in common with other international terrorist organisations. According to Radlicki (2015), ISIS, Al-Shabab and Boko Haram have many things in common such as:

Use of Fear as Strategy and Killing

Common feature among these sects is the clear recurring instilling of fear in people. They impart fear in people which allow for easy intimidation and domination. Like ISIS, their Iraqi counterparts, Boko Haram have killed and are killing people with reckless abandon (Dyikuk, 2014).

Creation of a Sense of Mystery

Aside from creating fear wherever they operate, they also create a sense of mystery which makes them appear almost God-like. The mystery of the sect is that within few years, it has become one of the most recognized terrorist entities in the world (Draitser, 2015).

Ideology of Religious Extremism

All the groups employ the use of religious extremism as a justification for their actions. Their use of religious extremism is tied to the Wahhabism idiosyncrasy although this is being argued (Thurston, 2011).

Mafia Mystic

Because of their syndicated strategy, the three groups appear more like a mafia gang than a quire religious group. These militant sects are like a new mafia operating in shadows (Al-Harthi, 2014).

Gunning for Money

Often times, they make money through black markets or other self-declared appropriations like breaking of financial institutions or killing of rich people. These sects raid banks to boost their financial base (Banjo, 2015).

Use of Organized Crime Strategy

Since it has been establish that they operate as a mafia group, the three militia groups engage in organized crime as a backbone for their operations. They are intelligent, watchful, tactful, and opportunistic and organized which is why their attacks often take people unawares. This is why they not only carry out acts of violence but also transnational organized crime (United Nations, 2017).

Use of Money for Allurement

All the sects usually provide salaries to impoverished local communities to lure people into their jihadist organizations. Because there are limited sustainable alternatives for those who are recruited, once in, followers are not allowed to leave (Radlicki, 2015).

Employing Propaganda

The insurgents exploit the traditional and social media propaganda, intimidation and instilling fear in the minds of people. The advancement in technology provides them with the leeway to make noise on television and the internet where they either broadcast their messages or post amateur videos (Yusha, 2011 & Adekunle, 2017).

Hostage Taking:

All the terror groups are involved in hostages taking to cause fear, press home their demands or make a statement. They sometimes use the hostages for swap, as spies or suicide bombers, sex slaves or shields when they are overran by members of the armed forces (Gross & Meisels, 2017).

Extant Laws on Cyber Crime

In 2014, Nigerians lamented about the absence of ICT law in country. At the time under review, government appeared to be more comfortable with ICT policy than actual ICT laws. It should be noted that while the former is merely and administrative guide, the latter is a binding document that can be enforced (Uwaje, 2014). Because of these agitations, a scanty Cyber Crimes Act which only passed first reading was signed into law in 2015. The Act was aimed at containing the growing spate of internet offences by seeking to arrest and prosecute anyone guilty of committing cyber-crimes and other allied offences. The law was poised to making the internet a safer place. Despite the lofty expectations, the Cyber Crimes Act did not meet the desired results because of its loopholes such as danger of confusion with the use of specific definitions and other structural deficiencies (Adaramola, 2015). It would also be recalled that the said Cyber Crimes Act did not follow the normal procedure of passing through second reading. Aside from the fact that the general public was not briefed about the bill and experts were also not consulted, the cybercrime bill, the country was left without a solid law on cybercrime (Buhari cited by Busari, 2017). Perhaps it is reason why the Nigeria's Senate Committee on ICT and Cybercrime recently stated that the law on cybercrime in Nigeria was moribund and needed review to meet international and acceptable standards. In the past, various attempts have been made in the country to legislate on cyber security. These are: The Computer Security and Infrastructure Bill of 2005, Electronic Provisions Bill of 2008, Cyber-Security Bill of 2011, Criminal Code Amendment for Offenses Relating to Computer Misuse and Cybercrimes of 2011and Electronic Transfer of Funds Crime Bill of 2001 (Adelabu cited in Tribune Online, 2017). In 2015, Nigeria's Governor of Central Bank, Godwin Emefiele made a case for the establishment and enforcement of cyber laws in the country. While delivering a keynote address at a stakeholder's workshop on Cybercrime organised by Nigeria Electronic Fraud Forum (NeFF) to mark the second anniversary of the enactment of Cybercrime Prohibition and Prevention Act 2015 in Abuja, the CBN

helmsman disclosed that since there are challenges in terms of exposures and vulnerabilities, "firm legal frameworks must be put in place, supported with sound and effective law enforcement and enhanced technical and institutional capabilities to effectively protect these networks and secure the systems and infrastructure from all forms of cybercrimes" (Tribune Online, 2017).

According to Uwaje, (2014) the benefits of having a solid cyber law in place are: If critical steps are taken, technology and other such processes would always remain safe, secure and fundamental. The security of lives and property of the citizenry as well as that of government's databases including national information system would be easily achieved. In a world of e-governance, cyber laws would make government's computerization and automation easy. It would give Nigeria the chance of debuting its own cyber technique since the country is an integral part of the Global Electronic Cyber web. It would help government and other ICT related stakeholders to acquire complete and effective understanding as well as implications of cyber gladiators such as insurgents like Boko Haram. It would enable the country build a National Cyber Security Force and also incorporate Cyber Security and Cyber Crime Emergency response Team for all forms of cyber-attacks. While concrete cyber laws are still in the incubating stage, skills to ward off being potential victims of hackers and terrorists remain crucial. Perhaps that is why *IT News Africa* came up with 8 tips on how to avoid cyber-crime. These include: Constantly updating passwords and login details, securing ones computer, being social media savvy; securing mobile devices, protecting one's data, being careful of what one does while suing public Wi-Fi Hotspots, protecting one's identity and avoiding being scammed (Linington, 2014). While these safety tips are essentials moral safeguards for the citizenry, they are even more important for gullible young stars that are easily recruited online into terrorist groups like Boko Haram.

The Army's Use of Technology as an Indispensable Security Tool

Technology is no doubt as an indispensable security tool in tackling the Boko Harma menace. To buttress this claim, in the year 2013 precisely on May 23, the Nigerian government shut down mobile communications in the North-Eastern states of Adamawa, Borno and Yobe. According to military authorities, the aim of the shutdown was to the limit Boko Haram's communication capabilities, restrict their ability to regroup and reinforce and also limit their ability to detonate improvised explosive devices - Notwithstanding its socio-economic effects, the action forced the members of the sect out of Maiduguri and its environs to the treacherous Sambisa forest where the army is still winning the war on terror (Burutai, 2017). Since the insurgents are ICT savvy, the government, security agencies and the general public now use the same medium to provide access to critical, real-time information and also crucial and timely location of the insurgents so as to proactively stop before they cause harm to unsuspecting members of the public. It as to enhance security that the government in 2011 mandated the NCC to register all mobile phones in the country to ensure the security of the state and the citizenry and enable the service providers have predictable profiles of all users in their networks (Burutai, 2017). The army authorities claimed that it was information plus the intelligence gathering courtesy of the Nigerian Security Services that key Boko Haram commanders like Sani Mohammed, Kabiru Sokoto and Shuaib Mohammed Bama amongst others, were captured (Burutai, 2017). The armed forces are also taking advantage of the Open-Source Intelligence (OSINT) which is being used to gather available information on specific targets. In their theatre operations, the Nigerian Army is employing the use of other several modern techniques to arrest terrorists and economic saboteurs of the fight against terror (Burutai, 2017).

It is also believed that through the army's Media Campaign Centre, the operation LAFIYA DOLE provides real-time and accurate information on military operations in the North East and also coordinating military-media activities. To this end, the radio station which broadcasts in English, Hausa and Kanuri and other major languages is aimed at sensitizing the citizenry on the dangers of the Boko Haram ideology, reorient the locals on the need for peaceful coexistence preached by both Christianity and Islam and on the need to renounce violence (Burutai, 2017). The army is said to be actively using various social media platforms to reach out to the world and counter the Boko Haram propaganda machinery. It idea is to defeat physically as well as on social media. The soldiers also take advantage of Psychological Operations (Psy Ops) to influence perception by broadcasting information targeted at influencing the emotions, motives and objective reasoning of large audiences – The psychological warfare is wagged through the use of leaflets, jingles, clips, posters to mention a few (Burutai, 2017). This shows that ICT or Information Systems (IS) security technologies play an important role in protecting information from unauthorized disclosure, modification or use (Beebe and Rao, 2005).

Technology as an Indispensable Security Tool in Tackling the Menace

There are some many ways in which ICT-based technologies can assist security agencies in achieving more efficiency and effectiveness in their operations. Under this, we shall consider both ICT and non ICT-based technologies for tackling the Boko Haram insurgency:

ICT-based Technologies for Tackling the Insurgency

Surveillance and Intelligence Gathering:

Surveillance is a deliberate system of keeping a close watch on the behaviors or activities of persons, groups, organizations and institutions suspected of doing something illegal or capable of causing a breach of security by government's security agencies. This is done electronically with *closed circuit television* cameras or interception of electronically transmitted information (such as Internet traffic or phone calls) or by means of low-technology methods such as human intelligence agents and postal interception. Other means include: surveillance cameras, social network

analysis, biometric surveillance, data mining and profiling, corporate surveillance, satellite imagery, radio-frequency identification and geo-location devices to mount surveillance on suspected targets. Intelligence gathering helps security agencies to keep tabs on the activities of suspected groups, organizations or persons likely to breach the peace. Today, such ICT tools as the internet, mobile telephony system, social media networks and the media have become veritable platforms for intelligence gathering efforts of our security agencies, so long as they observe the ethics of using these technologies for intelligence gathering purposes.

Intercepting Communication and Purposeful Coordination

Intercepting communication between terrors and terror groups and enhancing intelligence sharing and other collaborative measures between security agencies is now possible through ICT tools. There are now electronic devices and gadgets with in-built unique identification numbers that makes them electronically traceable regardless of location. So it is no longer impossible to track communication devices or gadgets used by criminal gangs or groups. Security agencies can minimize duplication of efforts, guard against the mishandling of information as well as enhance information sharing among them for a better management of our national security through ICT. This involves pulling the nation's data into a coordinated and centralized database as a proactive means of combating insecurity.

Tracking of Finances

ICT is a vital tool for tracking, tracing and investigating suspected financial transactions funneled to criminal activities. With the recent introduction of cash-less society, transactions could be done on electronic platforms where suspicious cash movements can be identified and questioned. This goes a long way in curbing the financing of activities that constitute a threat to national security because no terrorist group or gang can operate without funding.

Creation of Central Intelligence or Central Intelligence Unit

The creation of a Central Intelligence Unit (CIU) or Counter Terrorism Unit (CTU) within arm forces and security agencies with a robust, dynamic, vibrant and updated central database for a country helps in the fight against terrorism. The centralized database could contain every person's data and details for proper identification.

Developing Identification Initiatives

In advanced countries of the world, birth and death registration, in addition to unifying various identification initiatives, plays significant roles in national security, especially when combined with DNA, facial recognition and finger printing technologies which operate on platforms provided by ICT. That is why it is easier in those climes to easily track down criminals. This initiative includes developing electronic identification cards. Conversion of the National Identification Card (NIC) into an electronic form as well as making all the identification (work ID, school ID, drivers' license, SIM card registration, National ID etc.) into a single digital electronic form and uploading same on a central data base (Oludare, Omolara, Umar & Kemi, 2015).

Provision of Adequate ICT tools

It crucial to provide adequate ICT which can be used in tackling crime and insurgency. The channel of communications using ICT tools are computer, internet, mobile phone, close circuit television (CCTV), surveillance cameras, social network analysis, biometry surveillance, data mining, satellite imagery and IP devices such as the satellite (Oludare, Omolara, Umar & Kemi, 2015).

Public Enlightenment/Sensitization and advocacy

Recently, a church in Nigeria unveiled its e-portal system that computerized membership registration and other ancillary services. Managers of this e-portal send regular precautionary SMS alerts that assist members to be at alert and take precautionary measures. On security enlightenment issues, using ICT-driven solutions, therefore, can play significant roles in tackling insecurity in the country (Seventh Framework Programme, 2015).

Non ICT-based Techniques for Tackling the Insurgency

Involvement of public and MDA's:

All ministries, departments and agencies of Government must be involved in the fight against crime and terror in Nigeria – these are: The Federal Ministry of Defense, Interior and Foreign Affairs, Communications, Information, Science and Technology. Departments involved in this are: Immigration, Custom, Federal Airport Authority, Shippers Council, Nigeria Port Authority and Agencies like the Economic and Financial Crimes Commission (EFCC) to mention are few.

Synergizing with Organizations, Community and Religious Leaders:

Telecommunication industries, banks, mining companies, oil companies, industries and construction companies and ship companies etc., should be vigorously involve in the fight against crime and terror in Nigeria (James & Saraso, 2016). Forming a synergy and collaboration with community leaders such as: Emirs and settlement leaders at various levels and religious leaders like pastors, reverends, bishop, evangelist and Imams is essential. This should be a major component in the fight against crime and terror in Nigeria.

Chinda et al. (2018).

Training/Seminars and Conferences:
Public awareness training and security personnel training on security issue should continue on daily basis.

Journalists
The media has a role to play which is why journalists must be been to engage in the fight against crime and insurgency in country.

Adequate legislation, Prosecution and Judgment:
The government of Nigeria should enact laws that can punish criminals and check insurgency attacks as well as criminal activities. Government should setup task force on crime and security. This will help in the fight against crime and terrorist activities.

Adequate Funding
The Government at all levels - Federal, State and Local must be ready to release money funds for security especially as it relates to fighting the insurgency. State governors must be sincere in handling security funds.

Controlling Immigrant and Boarder Collaboration:
The government of Nigeria should build an institution that can redeploy illegal immigrants and stop illegal entry of people into the country. This can be more effective by partnering with neighboring or boarder countries such as Cameroun, Chad, Niger, Benin and Ivory Coast as a way of building a united and formidable force to fight the insurgents. Implementing the introduction of an advanced electronic system for border monitoring and securing entries used by terrorists to infiltrate the Sahara is key (Osun Defender, 2012).

International Collaboration
The Nigerian government should seek assistance from the Economic Community of West African States (ECWAS), African Union (AU), United Nations (UN) and Developed Countries to fight the Boko Haram insurgency. This paper proposes the creation of Integrated Ballistics Information Systems (IBIS), Traffic Ticketing System (TTIS), Crime and Information Management System (CIMS) and the use of Geographic Information Systems plus introduction of Automated Finger Printing Information Systems (AFIS) as ways forward.

Limitations of the Use of ICT in Fighting the Insurgency
While this study has argued favorably for the use of ICT as an indispensable security tool for ending the Boko Haram insurgency in Nigeria, it is important to acknowledge certain limitations which stand in the way of achieving success in this regard. First, there is the challenge of deficit in infrastructure. In rural Africa, especially Sub-Saharan countries such as Nigeria, the problems of either lack of or poor internet services militates against the effective use of information technology as a security tool. The paper also established that the lack of concrete cyber-crime legislation is another challenges to making head way in use of ICT as a security tool. The paper faulted the extant Cyber Crimes Act which was signed into law in 2015 after passing first reading. It noted that the Act was scanty and moribund stressing that it needed reviewed. The authors also pinpointed its loopholes such as danger of confusion with the use of specific definitions and other structural deficiencies (Adaramola, 2015), the inability to brief the Nigerian populace about the bill and lack of involving experts in its formation which lives the country without a concrete law on cybercrime (Buhari cited by Busari, 2017). Monitoring or tracking potential terrorists online also remains a great challenge because regarding the use of the internet, one could be dealing with anonymous or faceless groups. Those with sinister plans often clandestinely engage the use of the basis of ICT or social with either pseudo names or credentials of those who have died. As a result, it presents a limitation on how information technology can be accessed to reduce crime in society given the fact that in Nigeria, data generation and presentation is still in its remote stage.
Lack of cooperation by network service providers equally puts a big clog in the wheel of progress regarding the effective use of information technology for safeguarding society from terrorists. Although in the year 2011 the Nigerian government mandated the NCC to register all mobile phones in the country to ensure the security of the state, its citizenry and enable the service providers have predictable profiles of all users in their networks (Burutai, 2017), the mandate is a far cry as there are still many people who use unregistered sim-cards.

Conclusion and Recommendations
Although the world today continues to contend with the sad phenomenon of global terrorism, this paper has demonstrated that its frightening impact in terms of the sophistication of the modus operandi of terrorist groups who cash in on the benefits of ICT to cause mayhem to unsuspecting members of the public can be curbed through the effective use of the essentials of information technology as an indispensable security tool. The *Digitalizing Crime Prevention Theory* used as theoretical framework also supports the use of ICT to quell the threatening activities of Boko Haram. It is up to the Nigerian government and security agencies to seek for valuable insights into how the sect can be countered by engaging in intensive analysis of its use of information technology, technological capacity and how it channels messages both at home and abroad (Barkindo, 2017). The propaganda that is typical of the sect can be turned around if all stakeholders encourage media literacy, online vigilance and efficient engagement with social media platforms as means of spreading the gospel of peaceful coexistence amongst people and dissuading the recruitment of the young into terrorist organizations. Accordingly,

if those who intimidate the citizenry and threaten the peace of the nation are brought to justice, it would serve as a deterrent to potential terrorists. The establishment and enforcement of cyber-laws as well as proscription of online hate speeches is a right step in the right direction. The Nigerian government needs to first address the issues of corruption, impunity and strengthen accountability institutions if it must curb the menace (Barkindo, 2013). Since terrorist groups often form an alliance with other terrorist organizations around the world as an operational strategy, the United Nations, various governments, Non-Governmental Organizations, security agencies and spirited individuals must embrace online vigilance and also form a global synergy to nip the menace of global insecurity in the bud. It is the estimation of the authors that the rudiments of ICT are possible panaceas to the fight against terror and remain an indispensable security tool for bringing Nigeria's number one terrorist sect down to its knees.

Based on the findings of this study, the following recommendations were made from the study;

Establishment and Enforcement of Cyber-Laws
To put the overt or covert online activities of Boko Haram in check, it is important to establish online laws otherwise known as cyber-laws (Emefiele, cited in Tribune Online, 2017) which criminalizes any threats in form of amateur videos posted by members of the sect on the internet. If the laws are made by the national assembly, the executive and judicial arm of government must take up the responsibility of enforcing them so as to deter young people who are constantly being recruited online into militia groups. Government must make concerted efforts at not only enforcing the Cyber Crime Act with its elements of Prohibition, Prevention and Prosecution (Alakali, Faga, & Mbursa, p.175) but also review it to meet international best practices. In order for government to address the issues of cyber security, it has to declare cyber security as a national emergency which deserves political will and budgetary resources to implement it headlong; provision of a legal framework for cyber-crime and security; the establishment of national cyber-crime and cyber security training centre; establishment of national emergency response framework on cyber-crime and cyber security; establishment of cyber police and forensic commission to mention a few (Uwaje, 2014).

Proscription of Hate Speeches
The authors recommend a purposeful enforcement of the crime of hate speech by law enforcement agencies in Nigeria (Alakali, Faga, & Mbursa, p.175). As part of cyber-laws, government must make efforts at proscribing online hate speeches. Because the ripple effects of broadcasting hate speech are disastrous, the relevant government agencies should enforce the proscription of hate speeches. This would serve as a deterrent to those who spread the gospel of division and intimidation or target certain groups of people in the society for elimination.

Synergy in Fighting against Terror
Insurgencies are not fought and won alone. Key players like the Nigerian Communications Commission (Adaramola, 2015), National Security Adviser, the Office of the Accountant General of the Federation must collaborate with other stakeholders to effectively tackle cyber-crime and cyber security (Udotai, cited by Adaramola, 2015). This why synergy among bodies like the United Nations, various governments, Non-Governmental Organizations, security agencies and spirited individuals is crucial to tackling global insecurity. Organizations have to guard against illegal or unethical activities which are perpetrated through electronic or other means (Beebe & Rao, 2005). This requires must embracing online vigilance and forming a global synergy to nip the menace of global insecurity in the bud. Network Service providers like MTN, GLO, Etisalat must collaborate with security agencies by providing necessary information about people who post incriminating or intimidating remarks online.

Education and being ICT Savvy
Since militia groups are using the fundamentals of ICT for destructive purposes, it is absolutely necessary that the people are ICT or media savvy. This demands education and creation of awareness aimed at letting people know to secure their online private details such as Facebook, Twitter, Email etc, be sensitive in posting materials on the internet (Linington, 2014) and also detect "fake friends" who pose as imposters to threaten the peace of nation. Network Service Provides should be able to provide security lines or number which the public can use to report eccentric-people who pose threats to society. It is safe to conclude that Boko Haram will be defeated not only with guns and weapons but also through education and policies which centre on the development of the human person (Kukah, 2017).

Information Gathering and Intelligence
The most modern crucial way of tackling insurgences is through information gathering and intelligence (Burutai, 2017). As a country, Nigeria must be ready learn the current approaches of counterinsurgencies such data analysis, use of civilians for gathering information and covert collations from bigger democracies. This includes cell mating which enables security officers to disguise and blend with civilians so as to gather relevant information (Kukah, 2016).

Curbing Radicalization

Since illiteracy has being fingered as one of the causes of the insurrection, all stakeholders must make concerted efforts at de-radicalizing young who are often pruned to being used by selfish politicians and religious leaders are thugs. Youth radicalization can be curbed through education for all especially children, youth and women, screening of teachers who teach religious studies, and reorganization of the Almajiri System of children which exposes children to roaming the streets in search of meal-handouts. Often times, these kids end up becoming vulnerable targets for recruitment into groups like Boko Haram. It would be appropriate to either issues licenses religious preachers or censure their preaching. This would help in curbing radicalization.

Counterinsurgency Initiatives

Key among counterinsurgency initiatives is engaging insurgents headlong while caring for those affected by the insurrection. This can be accessed through intelligence gathering, rehabilitation of Boko Haram victims through counseling and psycho spiritual support, supporting victims to rebuild their lives and home, creating civilian groups like the CJTF who would monitor, report or even arrest suspicious people in the community, monitoring the insurgents source of funding, blocking their access to good food supply and water as well as putting in place other holistic approaches to the war on terror.

References

Adaramola, Z. (2015). Nigeria's cybercrime law and it's 'loopholes.' www.dailytrust.com.ng/news/it-world/nigeria-s-cybercrime-law-and-its-loopeholes/110593.html. Accessed November 16, 2017.

Adekunle, A. (2017). FG raises alarm over Boko Haram new media propaganda strategy. www.vanguardngr.com/2017/01/fg-raises-alarm-over-boko-haram-new-media-propaganda-strategy/. Accessed November 21, 2017.

Adekunle, A. (2017). The abducted Chibok schoolgirls: A timeline. www.vanguardngr.com/2017/05/abducted-chibok-schoolgirls-timeline/.Accessed November 21, 2017.

Adelabu, B. (2017). Why Nigeria needs effective cybercrime law. In Tribune Online. www.tribuneonlineng.com/nigeria-needs-effective-cyber-law-%2E2%2580%2595emefiele/. Accessed November 16, 2017.

Alakali, T.T; Faga, H.P & Mbursa, J. Audience perception of hate speech and foul language in the social media in Nigeria: Implications for morality and law. Academicus - International Scientific Journal. No Date of Publication. www.academicus.edu.al. Accessed November 1, 2017.

Alfred, C. (2015). Boko Harm actually kills more people in terror attacks than ISIS. www.huffingtonpost.com/entry/boko-haram-isis-_us_564cd890e4b00b7997f8c15d. Accessed November 22, 2017.

Al-Harthi, M. F. (2014). Boko Haram and ISIS are two sides of the same coin. www.english.alarabiya.net/en/views/news/middle-east/2014/05/18/Boko-Haram-and-ISIS-are-two-sides-of-the-same-coin.html. Accessed November 22, 2017.

Banjo, T. (2015). How we robbed banks to raise money for Boko Haram – Suspect. www.nigerianmonitor.com/how-we-robbed-banks-to-riase-money-for-boko-haram-suspect/. Accessed November 22, 2017.

Barkindo, A. (2013). Impunity and Boko Haram in North-Eastern Nigeria. www.peaceinsight.org. Accessed November 22, 2017.

Barkindo, A. (2016). How Boko Haram exploits history and memory. www. www.africaresearchinstitute.org/newsite/publications/boko-haram-exploits-history-memory/. Accessed November 22, 2017.

Barkindo, A. (2017). Tackling Boko Haram: Some policy ideas for Nigeria. www.africaresearchinstitute.org/newsite/blog/tackling-boko-haram-policy-ideas-nigeria/. Accessed November 22, 2017.

Beebe, N. L & Rao, S. (2005). Proceedings of the 2015 SoftWars Conference. Lag Vegas.www.mafiadoc.com/using-situation-crime-prevention-theory-citeseerx_59a7f18d1723dd08400c54d0.html. Accessed November 15, 2017.

Bring Back Our Girls, (2017). Bring Back Our Girls. www.bringbackourgirls.org. Accessed November 22, 2017.

British Broadcasting Corporation, (2016). Who are Nigeria's Boko Haram Islamist group? www.bbc.com/news/world-africa-13809501. Accessed November 15, 2017.

Buari, J. (2016). Northern elites should stop pretending, they're behind Boko Haram. www.naija.ng/651706-northern-elites-stop-pretending-theyre-behind-boko-haram.html. Accessed November 22, 2017.

Burutai, T.Y (2017). Counter-insurgency and role of the Nigerian Army in creating conducive environment for Nigeria's economic development. Lecture presented at the Guild of Corporate Online Publishers' First Annual Conference which held at the Renaissance Hotle, Ikeja, Lagos. www.thecitizen.com/counter-insurgency-and-role-of-nigerian-army-in-creating-conducive-environment-for-nigerias-economic-development/.Accessed November 15, 2017.

Busari, K. (2017). Nigeria's cybercrime Act needs review – Senate Committee.www.premiumtimesng.com/news/more-news/247851-nigerias-cybercrime-act-needs-review-senate-committee.html. Accessed November 16, 2017.

Campbell, J. (2017). Salafism in Northern Nigeria beyond Boko Haram. www.cfr.org/blog/salafism-northern-nigeria-beyond-boko-haram. Accessed November 22, 2017.

Counter Extremism Project, (2017). Nigeria: Extremism and counter-extremism. www.counterextremism.com . Accessed November 16, 2017.

Draitser, E. (2015). Unraveling the mystery of Boko Haram. www.counterpunch.org/2015/01/27/unraveling-the-mystery-of-boko-haram/. Accessed November 22, 2017.

Dyikuk, J. J. (2012). In between the bomb and the bullet. www.saharareporters.com/2012/02/26/between-bomb-and-bullet-justine-john-dyikuk. Accessed November 22, 2017.

Dyikuk, J. J. (2014). Gwoza: A Caliphate soaked in blood. www.naija247news.com/2014/09/05/gwoza-a-caliphate-soaked-in-blood-by-justine-john-dyikuk/. Accessed November 22, 2017.

Dyikuk, J.J (2017). Promoting professionalism among Nigerian social studies educators in a global information-highway. International Journal of Novel Research in Education and Learning Vol. 4, Issue 3, pp: (15-21), May – June 2017. www.noveltyjournals.com. Accessed November 16, 2017.

Emefiele, G. (2017). Why Nigeria needs effective cybercrime law. In Tribune Online. www.tribuneonlineng.com/nigeria-needs-effective-cyber-law-%2E2%2580%2595emefiele/. Accessed November 16, 2017.

Gamba, V. (2017). Nigeria: UN report details 'grave violations' against children by Boko Haram. www.un.org/apps/news/story.asp?NewsID=56683#.WhWt19ko_qA. Accessed November 22, 2017.

Gardner, F. (2011). Abuja attack: Car blast hits Nigeria UN building. www.bbc.com/news/av/world-africa-14686780/abuja-attack-car-bomb-hits-nigeria-un-building. Accessed November 21, 2017.

Gartenstein-Ross, D. & Zenn, J. (2016). Boko Haram's doomed marriage to the Islamic State. www.warontherocks.com/2016/08/boko-harams-doomed-marriage-to-the- islamic-state/. Accessed November 22, 2017.

Gross, M. L & Meisels, T. (2017). Soft war: the ethics of unarmed conflict. England: Cambridge University Press.

James, A & Saraso, L. D. (2016). The role of information and communication technology (ICT) and early warning system in school security based system in North Eastern Nigeria. Vol. 6. No. 10. [55-59].

Kukah, M. (2014). After the insurgency: Some thoughts on reconciliation in Nigeria. Lecture at University of Nigeria, Nsukka. www.fr.scribd.com/document/215616916/After-the-Insurgency-Some-Thoughts-on-Reconciliation-in-Nigeria-By-Bishop-Matthew-Hassan-Kukah-Bishop-of-Sokoto-Nigeria. Accessed November 22, 2017.

Kukah, M. (2017). Boko Haram'll be defeated not with guns, weapons – Bishop Kukah. www.vanguardngr.com/2017/06/boko-haramll-defeated-not-guns-weapons-bishop-kukah/. Accessed November 22, 2017.

Lewis, S. & Lewis, D. A. (2011). Digitalizing crime prevention theories: How technology affects victim and offender behaviour. International Journal of Criminology and Social Theory. Vol.4. No. 2. [756-769].

Lichter, I (2014). Boko Haram's ideology key to violence. www.m.huffpost.com/us/entry/5324138. Accessed November 21, 2017.

Linington, D. (2014). Top 8 tips to prevent cybercrime. www.itnewsafrica.com/2014/06/top-8-tips-to-prevent-cybercrime/. Accessed November 16, 2017.

Nwafor, P. (2017). Exclusionist policies led to civil war, Boko Haram crisis – Bishop Kukah. www.vanguardngr.com/2017/05/exclusionist-policies-led-civil-war-boko-haram-crisis-bishop-kukah/. Accessed November 22, 2017.

Ogbeche, D. (2016). Bad leadership, lack of political will responsible for Boko Haram in Nigeria – TY Danjuma. www.dailypost.ng/2016/bad-leadership-lack-of-political-will-responsible-for-boko-haram-in-nigeria-ty-danjuma/. Accessed November 21, 2017.

Okoro, C. (2017). Nigeria: Global index rates Boko Haram deadliest terrorist group. www.allafrica.com/stories/201701050587.html. Accessed November 21, 2017.

Oludare, A.A; Omalara, O. E; Umar, A. M & Kemi, D. V. (2015). The use of ICT tools in tackling insecurity and terrorism problem in Nigeria. Vol. 5, [21-40].

Osun Defender, (2012). Boko Haram: Nigeria plans electronic border monitoring. www.osundefender.com/boko-haram-nigeria-plans-electronic-border-monitoring/. Accessed November 2017.

Radlicki, M. (2015). Back to basics: What ISIS, Al-Shabab and Boko Haram have in common and how they preach water and drink wine. www.m.mgafrica.com/article/2015-06-08-back-to-basics-what-isis-al-shabaab-and-boko-haram-have-in-common.Accessed November 15, 2017.

Rouse, M. (2017). ICT: Information and communications technology, or technologies. www.search.techtarget.com/definition/ICT-Information-and-communications-technology-or-technologies. Accessed November 21, 2017.

Seventh Framework Programme. (2015). Updated scenarios, requirements and KPIs for 5G mobile and wireless system with recommendations for future investigations. www.metis2020.com/wp-content/uploads/deliverables/METIS_D1.5_v1.pdf. Accessed November 22, 2017.

Telegraph Reporters. (2017). What is Wahhabism? The reactionary branch of Islam from Saudi Arabia said to be 'the main source of global terrorism.' www.telegraph.co.uk/news/2016/03/29/what-is-wahhabism-the-reactionary-branch-of-islam-said-to-be-the/. Accessed November 22, 2017.

Thurston, A. (2011). Is Nigeria's Boko Haram a Wahhabi group? www.csmonitor.com/World/Africa/Africa-Monitor/2011/0609/Is-nigeria-s-Boko-Haram-a-Wahhabi-group. Accessed November 22, 2017.

Tukur, S. (2017). Shocking Revelation: 100,000 killed, two million displaced by Boko Haram insurgency, Borno Governor says. www.premiumtimesng.com/news/headlines/223399-shocking-revelation-100000-killed-two-million-displaced-boko-haram-insurgency-borno-governor-says.html. Accessed November 21, 2017.

United Nations. (2017). Insurgency, terrorism and organised crime in a warming climate – New Adelphi report. www.knowledge.unccd.int/publications/insurgency-terrorism-and-organised-crime-warming-climate-new-adelphi-report. Accessed November 22, 2017.

Uwaje, C. (2014). Thread: The need for ICT law and cyber security in Nigeria. www.nigerianelitesforum.com/ng/computers-and-ict/55645-the-need-for-ict-law-and-cyber-security-in-nigeria.html. Accessed November 16, 2017.

Yusha, M. J. (2011). The Boko Haram conflict and the endless propaganda. www.premuimtimes.com/opinion/5219-the_boko_haram_conflict_and_the_endless_propaganda.html. Accessed November 22, 2017.

Zenn, J. (2012). Northern Nigeria's Boko Haram: The prize in al-Qaeda's Africa strategy. USA: The Jamestown Foundation.

Zenn, J. (2014). Leadership analysis of Boko Haram and Ansaru in Nigeria. www.ctc.usma.edu/posts/leadership-analysis-of-boko-haram-and-ansaru-in-nigeria. Accessed November 22, 2017.

Tables

Table1: Juxtaposition and Comparative Analyses of ISIS, Al-Shabab and Boko Haram

	ISIS	Al-Shabab	Boko Haram
1.	**Designation:** The Islamic State of Iraq and al-Sham (ISIS)	**Designation:** Party of the Youth	**Designation:** Western Education Forbidden
2.	**Formation:** 1999	**Formation:** 2006	**Formation:** 2004
3.	**Areas of operation:** Syria, Irag, Libya, Lebanon, Nigeria and Afghanistan	**Areas of operation:** Southern Somalia and Yemen	**Areas of operation:** Nigeria, Cameroon, Niger and Chad
4.	**Strength:** 52,600 – 257,900	**Strength:** 7,000-9,000	**Strength:** 7,000 – 10,000
5.	**Partner:** Al-Qaeda (2004)	**Partner:** Al-Qaeda	**Partner:** ISIS
6.	**Leader:** Abu Bark al – Baghdadi	**Leader:** Ahmad Umar	**Leader:** Abubakar Shekau
7.	**Ideology:** Whahabism, Salafism and Jihadism	**Ideology:** Salafi Jihadism	**Ideology:** Wahhabism and Jihadism (Radlicki, 2015).

Table: Designed by Authors

Chinda et al. (2018).