Unabated Cyber Terrorism and Human Security in Nigeria

David Oladimeji Alao[1], Goodnews Osah[1] & Eteete Michael Adam[2]

[1] Department of Political Science and Public Administration, Babcock University, Ilishan-Remo, Ogun State, Nigeria

[2] School of Law and Security Studies, Babcock University, Ilishan-Remo, Ogun State, Nigeria

Correspondence: Goodnews Osah. E-mail: osahg@babcock.edu.ng

Received: September 27, 2019 Accepted: October 5, 2019 Online Published: October 24, 2019

doi:10.5539/ass.v15n11p105 URL: https://doi.org/10.5539/ass.v15n11p105

Abstract

The development of Information and Communication Technology (ICT) due to Internet connectivity has called to question the preparedness of nations to curb cyber terrorism and the effects on human security. Boko Haram emerged as one of the deadliest terrorist groups globally. The paper investigated the Nigeria's efforts in checkmating cyber terrorism, the implication on human security and the inherent challenges associated. The paper employed descriptive research and qualitative method while secondary sources of data were adopted. The study found that cyber terrorism as employed by Boko Haram was deployed in raising fund, propaganda, coordinating operation, international collaboration, recruitment and training of its members. In addition, the Nigerian government has not given sufficient attention to war against cyber terrorism and this has complicated human security provisioning particularly in the North-East Nigeria. This study concluded that cyber terrorism has come to stay as long as development in ICT cannot exclude the terrorists and the prevalence of fear of attack and the destruction of lives and property facilitated by Internet have devastating effects on human security. This paper recommended the criminalization of terror attacks, adequate equipment of the security agencies and political will to tackle societal ills.

Keywords: information and communication technology, internet, cyber security, security threat, terrorism, human security

1. Introduction

The world is increasingly becoming a global village. This is facilitated by the interconnectedness and interdependence among nations through the internet. The internet is linked with the aid of information and communication technology. By January 2019, the global internet user stood at 4.39 billion (Global Digital Overview, 2019) out of the world's population of 7,519,028,970. This makes the internet one of the fastest growing technologies of our time (Orngu, 2014; Lynch, 2011; Rogers, 2003). It is imperative to appreciate that the global system is deeply relying on cyber technology in all aspects of human life and it has become indispensable (Legris, Ingham, & Collerette, 2003). The cyberspace is open to all. More so, the advent of cyber as a weapon of warfare is rapidly gaining momentum not only in Nigeria but globally. Terrorists now employ it to monitor individuals, governments and security networks as well as to attack institutional or governmental facilities (Ntamu, 2014; Onuoha, 2011; Yar, 2006).

Beyond the traditional and conventional style of terrorist activism, the violent rise of the jihadist group Boko Haram in Nigeria's Northeast region has now dominated policy debates among academics and policymakers not only in Africa but beyond. Boko Haram membership which prefers to be called by the Arabic name *Jama'atu Ahlis Sunna Lidda'awati wal-Jihad*, meaning "People of the Sunnah (the practice and examples of the Prophet Muhammad's life) for Preaching and Jihad Group" is believed to be founded by Mohammed Yusuf in the town of Maiduguri, Northeast Nigeria in 2002. It has since 2015 transformed to become one of the deadliest terrorist groups globally (Global Terrorism Index, 2016). Boko Haram which is a combination of two Hausa words *boko* meaning Western education/civilization and *haram* meaning sin or forbidden. Thus combined means western civilization is forbidden. It is also believed that the membership of over 500,000 people who were generally disgruntled with the situation in Nigeria especially the configuration of the political and economic structure were taxed one Naira daily to sustain their ideology (Adibe, 2013).

The Nigerian government had claimed decimating the Boko Haram sect, but the reality is that warfare of the 21st century has gone from hardware to software. The group has strategized to using not only physical weapons of warfare but unconventional tactics to cramp the government. Beyond throwing bombs, taking hostages and crossing borders they now target critical national infrastructure by attacking the cyber security of Nigeria. Their adoption of cyber technology for technology integrated intelligence through the use of ICT devices such as computer, internet, mobile phone, Close Circuit Television, surveillance camera, social network, biometric surveillance, data mining, satellite imagery, IP devices and other technologically driven weapons is believed to have aided their collaborative efforts with others like Al Shaba of Sudan, ISIS and al Qaeda to unleash terror on citizens not only in northern Nigeria but also to the neighboring Chad, Niger and Cameroon (Adam, Osah, & Alao, 2019; Jacob & Akpan, 2015; Obayuwana, 2011; Osho, Adesuyi, & Shafi'l, 2013). This is what Aladenusi (2015) calls 'cyberharam'.

The integration of technology in the operational plan of Boko Haram has by no means aided their striking power and assisted them in the exchange of information, recruitment, ideological propagations, training and finances through electronic transfers. In addition, it has occasioned traumatic experiences on the part of the citizenry and the general belief that the government has been incapable to curtail them. This explains why Arimatéia da Cruz (2013) noted that apart from using internet to launch cyber-attacks against countries, terrorists possess the capacity to engage in "hacktivism," which is described as strategy of merging hacking and activism. The implication is that the seven dimensions of human security namely economic, food, health, environmental, personal, community and political as established by the United Nations Development Programme (UNDP) in 1994 might be difficult to attain as a result of terrorism by 2030 being the set target of the Sustainable Development Goals (SDGs) if nothing urgent is done to reverse the trend. This informs the study to examine the state of Nigeria's preparedness in coping with cyber terrorism and to determine the effects of cyber terrorism on human insecurity in Nigeria and the challenges of checkmating the menace. The paper adopted a descriptive research design that is qualitative in nature.

2. Challenge of Cyber Terrorism and Cyber Insecurity

As earlier enunciated, the revolution in the field of information technology and the popularization of usage of internet services has aided the ease of doing business globally and closing communication gaps among individuals and nations. According to Urbas and Choo (2008) the technology driving telecommunications was invented in 1837. They also averred that the first record of criminal usage of such technology was around 1867. This was corroborated by Grabosky & Smith (1998) who recorded cases of illegal interception. Today, the use of laptops, I-pads and computers have become imperative in respect to the operation of all organizations. The cyberspace is open to all users. Thus there is no limitation and barrier as to who goes in and out.

The National Strategy to Secure Cyberspace (2003) says cyberspace is "the nervous system of the nation's infrastructure and it is comprised of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructure work". It is the interconnectivity provided in the cyberspace that allows end users of internet services to operate successfully and this is the facilities that criminal elements exploit to perpetrate their nefarious activities. Criminally minded persons have taken advantage to engage in cybercrimes. Cybercrimes constitute some of the fastest growing crimes globally and it embraces huge number of criminal activities such as financial fraud, computer hacking, downloading of pornographic images from the internet, virus attacks, stalking and creating websites that promote hatred (Erhabor, 2008). In very simple form, cybercrimes are crimes that are mediated by networked technology (Wall, 2007).

Section 18 (1) of the Cybercrimes Act 2015 clearly states that "any person that accesses or causes to be accessed any computer or computer systems or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment". Unfortunately, clients often fall victim of fraudsters or criminals. According to the Carnegie Endowment for International Peace (2019) since 2016, there have been growing concerns about cybersecurity risks to the financial system prompting the G20 finance ministers and central bank governors to warn in March 2017 that "the malicious use of Information and Communication Technologies could . . . undermine security and confidence and endanger financial stability."

Cyber terrorism is a product of cyber technology and an aspect of cybercrime. Cyber terrorism is a conglomeration of cybermetrics and terrorism. The US Federal Bureau of Investigation (FBI) in a 2014 report, stated that cyber terrorism as the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result systems, computer programs and data which in violence against non-combatant targets by sub-national groups and clandestine agents. Terrorists among other criminals can therefore exploit organizations' exposure to perpetrate atrocity. As good as internet development is to mankind; such facilities are often adopted by criminal elements to perpetrate atrocity.

Cyber terrorism thus is seen as the illegal use of computer or computer network to deliberately harm, damage, unduly compel, seriously intimidate, destabilize or coerce a government or international organization to do or refrain from doing a particular thing in furtherance of the terrorist's socio-economic, political or religious agenda. In this vein, Wall (2008) opined that cyber terrorism is:

> Criminal or harmful activities that are informational, global, and networked. They are the product of networked technologies that have transformed the division of criminal labor to provide entirely new opportunities for, and indeed, new forms of crime which typically involves the acquisition or manipulation of information and its value across global networks.

Similarly, Tehrani, Manap, and Taji, (2013) noted that cyber terrorism means unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives. It is also important to perceive cyber terrorism as an international crime as this will have implication on procedure or strategy that can be adopted to checkmate it.

The United Nations Office for Drug and Crime (UNODC) 2012 divides cyber terrorism into six areas, namely; propaganda, financing, training, planning, execution and cyber-attack. Thus, the protection of the cyberspace is necessary. The major objective of cybersecurity therefore includes: protection of system/networks against unauthorized access and data alteration from within; and defense against intrusion from without. Cyber security in effect comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber-attacks. Increased consciousness was reawakened after 9/11 and the vulnerability of the global system.

Security, like many other terms is difficulty to define in a generally acceptable manner and Baldwin, (1997) views it as essentially contested concept. The traditional understanding of security based on realist perspective (Chandele, 2012; Ulman, 1983; Walt, 1991) views it as "*a freedom from any objective military threat to the state survival in an anarchic international system*". The widener school of thought that prominently featured Buzan moved horizontally from purely military conception to political, economic, societal and environmental sectors while vertically to accommodate humanity in general. Hence according to Buzan (1991), *security is pursuit of freedom from threats*. In effect, freedom from Boko Haram and others threats constitute security. Human security therefore assume wider meaning with the UNDP (1994) position and the objective as defined is to safeguard the vital core of all human lives from critical pervasive threats, in a way that is consistent with long-term human fulfillment. It is therefore people centered, all-encompassing consisting of elements such as food, health, political, economic, individual, community and environmental security.

The Nigeria Communication Commission (2017) reported that the Nigeria lost about N127 Billion to cybercrime in 2015 alone. Thus, making Nigeria the 3rd highest globally. It is pertinent to appreciate that most of the cyber-attacks are automated and indiscriminate but exploit the likely vulnerability or exposure of individuals or organizations. The implication for this paper is that the criminality of Boko Haram leading to loss of thousands of live, internally displaced figure rising to 3.3 million and the general traumatic experiences by the citizenry in Nigeria constituted in no small way threat to human security.

3. Theoretical Framework

The paper adopts two theoretical frameworks to underpin the work. These are Technology-Enabled Crime and Risk Society Theory.

3.1 Technology-Enabled Crime

McQuade (2006) is one of the scholars that emphasize the relevance of Technology-Enabled Crime theory with the growth in telecommunication industry. He notes that it encompasses such crimes committed directly against computers and computer systems which are often referred to as high tech crime, computer crimes or cybercrimes. He reasons that the use of Internet or technology helps to facilitate the commission of traditional crimes and it can take the form of fraud, scams, threat and harassment which introduces multidimensional challenges to overcoming old crimes.

In effect, Technology-Enabled Crime theory is an amalgam of criminological theories to enhance the societal understanding why crimes associated with computer and telecommunication technologies have become increasingly difficult to prevent, investigate and control (Essays, UK. November 2013). This is based on the understanding that criminal behavior might be very difficult to explain by a single theory and why Patchin and Hinduja (2011) focus on the utility of low self-control theory and strain theory. Grabosky & Smith (1998) listed some of the telecommunication crimes emerging of recent to include: illegal interception of telecommunications, electronic vandalism and terrorism stealing communications services, telecommunications piracy, pornography and other offensive content, telemarketing fraud, electronic funds transfer crime, and electronic money laundering.

In addition, McQuade (1998) observes that to understand and maintain complex crime is usually difficult particularly at onset as there is tendency for challenges associated with periodic competition between the criminals and security agencies for technological edge. This implies that the criminal elements will always attempt to innovate in their criminal tendencies while the security agencies will also attempt to decode and deter new form of crimes. The theory is applicable to this paper as terrorists now adopt information technology in raising fund, mobilize supporters or recruit, plan attack and monitor security agencies as to present the government incapable of handling the situation. This weakens citizenry moral support for government and the resolve of the security agencies striving to curb terrorist criminalities. Hence, while technological development has more advantages than disadvantages, the theory points to the threats posed by emerging forms of cybercrime, transnational crime and terrorist networks that defy traditional methods of criminal justice and security measures for preventing and controlling crimes. It therefore provides insight into understanding the new tools and techniques used by cybercriminals particularly the terrorists in this regards. It also provides insight into huge resources provided for security at the expense of human security provision beyond military hardware technologies. This explains why Cruz (2013) notes that though social, economic and political transformations are taking place with the advancement of the internet in the last two decades, it has led to the “end of geography, as geographic borders separating nations has become nebulous and porous with the advancement of the informational society.

3.2 Risk Society Theory

The Risk Society theory was popularized by Beck (1992:21) and it was associated with a movement from traditional to industrial society and towards a new modern risk society which often is individual, global and self-confrontational. A risk society is viewed as a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself. The theory notes that considering the nature of modern societies, risk has the tendency to multiply with the increasing complexities of societal system of production, consumption, governance and technological control (Jonathan, Nick, & George, 2004). This led Beck (1992) to assert that in modern society, risk is on increase due to technological and scientific discovery more than what technological progress is abating. This was made possible due to the revolution in the field of Internet and the increasing usage of mobile devices that facilitated instant messaging, electronic business transactions, banking and learning among others globally as this has made the world become a global village. This is made easy as millions of people globally are connected to computer and other potable electronic devices at the same time and hawking, fraud, scaring pictures and terrorist activities can simultaneously be perpetrated.

This theory is applicable to this paper as criminals under any guise, insurgents, thieves, kidnappers and terrorist groups equally like innocent and honest users adequately and successfully used the Internet to demonstrate their capabilities, strike fear, and conduct their nefarious operations in recent times. Indeed, the ease of internet usage cannot but help the terrorist to communicate with one another, share experiences, direct operations, recruitment of foot soldiers, raise and transfer funds. The implication therefore is that the wrong use to which internet facilities have been deployed is increasing the risk level in the global system and constitute threat to human security.

4. Interrogating the Linkage between Boko Haram and Cyber Terrorism

Cybercriminals are relentlessly investigating and developing new methods to perpetrate their goals and by implication, cyber terrorists such as Boko Haram are not left in the trade. A pertinent feature in cyber terrorism is their avowed commitment to be a step ahead of other internet users inclusive of governments and security agencies so that it might be difficult to pin down their activities. Makatiani, (2016:8) was right to have observed that the use of E- services is expanding in Nigeria and services offered range from online shopping, filling tax returns, cashless policy introduction and the use of Bank Verification Number (BVN).

Goodman (2008) further noted strategies adopted by terrorists enabled by Internet which included promoting ideologies and ideas, fund raising, transfer of money, propaganda, and recruitment of members. Others include launching of real and imaginary threat or attacks, exchange of communication among fellow terrorists, training and collection of operational information, booking and ordering supplies among others. The implication is that these platforms provided opportunities apart from legal transactions facilitated by Internet but also for cybercriminals and/or cyber terrorist to flourish. This was demonstrated in Jacobson (2009) (U.S.A. v. Babar Ahmad, “Affidavit in Support of Request for Extradition of Babar in 2004) that Babar was alleged to have converted his expertise in ICT, as a British citizen from South London to support the jihadist cause until his arrest in 2004. Another popular case was that of Tsouli and others that were arrested in connection with been in possession of 37,000 credit card numbers on his computer which was believed to have been used to steal about $3.5 million largely for terrorism (Krebs, 2007).

Alao, Atere and Alao (2012) quoting retired Major Chris Moghalu of the United States of America's military that Boko Haram received over $70million between 2006 and 2011 for its insurgent activities in Nigeria. Ezigbo (2014), Stewart and Wroughton (2014) and Ogundipe (2012) noted that the amount was linked to Al-Qaeda to support terrorism and was successfully transferred through inefficient financial and security network through various groups in Saudi Arabia and the UK. According to Sakar (2014) and Hogendoorn (2013), Osama bin Laden was said to have sent $3 million "seed money" to Nigeria to support terrorism.

The Save Humanity Advocacy Centre (SHAC) (2018) noted that Nigerians must be aware that one major component of terror is information flow. Terrorists like ISIS, Boko Haram, Al Shabab and their collaborators create dreadful images to instill fear followed by hate which travels like wild fire. This same was corroborated by Jacobson (2009) and Krebs (2007) among others. Terrorists now make use of internet to propagate their agenda, recruit new members and attack their targets. This explained why Shekau, the Boko Haram leader featuring on internet with a view of proving their capacity to strike and cause psychological trauma on citizenry by presenting government as incapable to protect them and casted doubt on the capability of the security agencies. It is widely believed that Boko Haram is using email to raise fund and other video tools for its online propaganda as observed by Fanusie and Entz (May 2017) and Forster-Bowser and Sander (2012).

Also, the same sources above noted that in December 2015, the Shite Muslim brotherhood sympathizers hacked the official websites of the Lagos State Government and the Court of Appeal in which the group in a massage posted described government in Nigeria as terrorists. The Terrorists have developed and used encrypted data in order to plan, communicate and execute their activities which is largely believed that the law enforcement agencies often find difficult to decode (Oluwafemi, Adesuyi and Abdulhamid, 2013). This is achieved through the use of ICT tools inclusive of disposable cellular phones, internet cafes and embedded information in digital pictures and graphics for propaganda. For instance, among numerous propaganda was the one reported in Vanguard (2016) in which Shekau was boasting in a video of his might to fight Nigeria as well as the whole World. This could not but have led the Chief of Army Staff, Lt.-Gen. Tukur Buratai to advice security personnel on counter terrorism operations in the North-East not to be deterred by the propaganda machinery of Boko Haram that was capable of misinformation.

5. Evaluation of Nigerian Government War on Cyber Terrorism

A great landmark in telecommunication industry took place in 1992 with the law deregulating the sector while the GSM revolution that started in 2000 provided an unrestricted opportunity for inclusive arrangement for the citizenry in Nigeria to enjoy mobile communication services. Oluwafemi, Adesuyi, and Abdulhamid, (2013). The Nigeria Communication Commission NCC (2018) noted that active mobile lines in Nigeria rose to 144 million as at December 2017. The implication of the huge cell phone users is that more than 70 per cent of the population are connected to digital communication, though some individuals use up to two or move line while the criminal elements also have unrestricted access. One of the practical steps taken by the Nigerian government to checkmate cybercrime was the directive by the National Communication Commission in May 2010 in respect of registration of "Subscriber Identity Module" (SIM) cards of mobile phone users. The goal partly was to monitor and track different form of crimes that could be enabled by Internet. The fact that majority of those who had their phones stolen or lost may decide not to do SIM sap or welcome back allowed for inaccurate statistics of mobile phone users since there is no restriction on the number of lines an individual could acquire even from the same service provider. Also, the prevalence of local sellers of SIM card already registered may be an impediment to such a lofty program achieving the set goals. This could have led Daily Trust (2010) to describe the policy as dead on arrival. It could be the scenario that led the NCC to impose a fine of $5.2 billion on MTN for failing to disconnect 5.1 million unregistered SIM cards before the end of August and September 2015 deadlines (Tshabalala, 2015).

As part of government control, the Terrorism Prevention Bill in May 2011 was signed into law by President Goodluck Jonathan on June 3, 2011. In addition, the Cybercrimes Act was passed into law in 2015. An evaluation of the achievement of the laws glaring showed that more action needed to be done to ensure cybersecurity. The persistent of attacks on soft targets in Nigeria is a demonstration that the enactment of laws without political will, citizenry and international cooperation is not enough to curb Cyber terrorism. This explains why the huge fund spent on installation of CCTV cameras failed to secure the June 16 and August 26, 2011 terrorist attack of the Police Headquarters and United Nations Building in Abuja as well as attacks on other security establishments. It is noteworthy that in 2014, the Jonathan administration launched a National Action Plan against Cybercrime and internet service providers, domain name registration body, telecommunications service providers and internet exchange were regarded as agencies essential to achieve the goal. It also provided for centralization of control to ensure prompt and effective response to cybercrime (National Security Policy, 2014). As a follow up in 2017 with a view to strengthening the position of the government in checkmating cyber terrorism and terrorism, the Nigerian government launched the Nation Action Plan in November 2017. The intent was to prevent violent extremism (PVE) and focused on strengthening Nigerian Institutions to PVE; strengthening the rule of law and human rights, building community capacity engagement and resilience as well as integrating strategic communication to PVE (Office of the national Security Adviser: Counterterrorism Center, 2017).

It is too early to determine the success of these action plan tough Trump administration has given a green light for the purchase of military aircraft for the fighting of the terrorist. However, it is on public domain that the security agencies particularly the Special Anti-robbery Squad (SARS) have converted the war against cybercrime to an instrument of enriching themselves by irrational check and arrest of youth with phones or laptop alleging them of cybercrime and forcing them to withdraw money from their ATM for settlement Ogundipe (2018) and Oludimu (2018).

The FATF (2013) also noted that as a result of vigilance in the banking system in Nigeria, the effort of an International NGO/Charity organization in the Middle East effort to open an account in Nigeria was frustrating and a Suspicious Transaction Report (STR) was made to the Nigeria Financial Intelligence Unit (NFIU). As part of the measure by the Federal Government to curb ease of financial transaction by criminal elements including the terrorist, the Central Bank of Nigeria took proactive steps to block the accounts and transactions linked to Boko Haram members and their likely sponsors as noted by Ajakaye, 2014; Komolafe, 2013 and Nwaoha, 2013. Contrary to the above position, The Cable (August 31, 2014) and Varghese (August 31, 2014) reported that an independent Australian hostage negotiator between Nigerian government and Boko haram observed that an official in the Central Bank of Nigeria actually processed financial transactions on behalf of Boko Haram, which permitted the group to hide the sources of its funding and avoid scrutiny when purchasing equipment.

In view of the need for external collaborations to curb cyber terrorism, the Nigerian government approached the US State Department in 2012 for the training of about 200 security personnel and a Nigerian army battalion. The arrangement was aborted on account of alleged human right posture of the Federal government due to their perception that Nigerian government violated US Leahy Amendment 2012 (Amnesty International Report, 2013). It is therefore glaring that the efforts of the Federal Government in checkmating cyber terrorism is on-going but the battle is far from being won. It should be appreciated that terrorism is not a regular warfare that could easily be won and the terrorists cannot be stopped from embracing and using modern technological invention. This implies that more positive actions are expected from the Federal Government to curb cyber terrorism.

6. Cyber Terrorism and Human Security Challenges in Nigeria

The UNDP (1994) came up with contemporary understanding of what constitutes human security. These are economic, food, health, environmental, personal, community, and political security. Cyber terrorism is perceived as terrorism perpetrated of facilitated through the use of ICT, therefore, the effect of cyber terrorism on human security could by psychological, real or both. Odiogor (2011) in his report in the Vanguard Newspaper noted that "the financial system of any country is vulnerable to financial terrorism from within and outside. It is therefore, important to treat this as a vital component of national security." One likely effect is the distortion in financial plan and spending as Greifeld (July, 2011) noted that his organization a stock exchange firm spent about 1 billion yearly of security of information as his firm was constantly under hackers and cyber terrorists attack. It needs be understood that form of cyber terrorism include cases of stolen Automated Teller Machine (ATM) or credit cards or numbers, the use of online facilities to steal fund or through scam mails.

In addition, there is no doubt that a nation noted for cyber terrorism with little demonstrated concerted effort to checkmate might find it difficult to be investment friendly nation. This might have led Adesegun and Ayenakin (2015) to conclude that a state of insecurity under any guise has the tendency to constitute a negative effect with respect to inflow of foreign direct investment. This position agrees with Aro (2013) that "Boko Haram insurgency has not only led to closure or abandonment of people's business activities within the affected region but also led to immigration of people from affected region while Afolabi (2015) noted that terrorist nuisance in Nigeria has created palpable fear for foreign investors in Nigeria due to insecurity and anarchy. This agrees with Oriakhi and Osemwengie (2012) and Mckenna (2005) that the increase in government expenditure due to rising insecurity especially in less developed countries like Nigeria may likely result in the sales of foreign reserves and espionage, as a consequence, inflation in those countries will rise. Hence, Andyopadhyay, Sandler and Younas. (2011) and Keefer and Loayza (2008) opined that the economic effects of terrorism led to declining foreign direct investment (FDI), production loses, cost of maintaining security, hamper economic growth and negatively affect tourism among many others.

The CEIC (2018) reported that the total value of FDI as at December 2012 was $3,084 million which coincided with the period when Boko Haram adopted violence as an instrument for the propagation of their activities. As at 2015 that marked the period that Boko Haram was classified as a leading terrorist group globally, the FDI dropped to $501.8 million. As at December 2017, the period believed to have marked success in war against terrorism, the FDI nearly doubled the record for 2015 and stood at $ 959.5 million while it further experienced a decline to $808.6 million as at March 2018 the period coincided with renewed violence by Boko Haram and herdsmen. The implication is that terrorism as demonstrated in the case of Boko Haram has negative effect in a nation's economic security which is an aspect of human security.

The HRP (2018) revealed that 4.5 million children required urgent humanitarian assistance. Though the total number of Internally displaced persons declined from 3,3 million in 2014 to 1.76 million in the North East in as noted by IOM DTM Round XXIII (June 2018), humanitarian needs were far from been met. The loss of lives, injury sustained displacement and psychological trauma on account terrorism had in no small ways affected the community, environmental and political security of the people in the Nigeria. It is important to further note that the effect of cyber terrorism in this regard expanded the scope of the threat and psychological trauma beyond the North East but to cover the whole Nigeria and beyond. Therefore, terrorism under any guise has negative effect on the health of the nation.

7. Conclusion and Recommendations

The study concluded that cyber terrorism like cybercrime has come to stay as long as development in ICT cannot exclude the group and it will continue to aid the operation of the terrorist particularly at psychological level such as in propaganda, fund transfer, training and collaboration with other international groups. In effect, the threat of cyber-terrorism cannot but increase in intensity as long as there are educated and knowledgeable youth occupying positions of authority in terrorist organizations. The degree of success in curbing cyber terrorism is largely a function of the extent of international cooperation and the ease at which Nigeria government can be a step ahead of the terrorists. The study also concluded that the prevalence of fear of attack and real destruction of lives and property aided and facilitated by Internet have devastating effects on human security. This is in terms of lives lost, family dislocation, poor health service delivery, school closure, stoppage of farming activities and other means of likelihood.

Thus, if Nigeria must claim decimating the Boko Haram insurgents, and remain the giant of Africa, this paper recommends that the Federal Government must demonstrate sincere commitment with huge investment in not only in military (hardware) warfare but to cyber terrorism. This can take the form of establishing effective institutional mechanisms for managing cyber security; fund and implement the measures designed in line with international best practices. Consequently, the National Security Adviser (NSA) should respond swiftly whenever suspicions are made of cyber-attacks. The Nigeria Police and other security agencies should be retrained and equipped to be meet with the menace of cybercrime.

Again, the Nigeria government should embark on capacity building beyond what the local efforts could achieve. At the local level, there should be better partnership between public and private sectors efforts in fighting cyber terrorism as the effects are not directed only to a particular sector. Also, since the attack has no specific boundary, global partnership through training, sharing of information, creating legal regime and other technological assistance in the fight is indispensable.

The government must not use the excuse of terrorism to justify poor provisioning of basic human needs. Since poverty and unemployment are attribute of human insecurity a sincere commitment towards infrastructural development will help to grow the economy as to boast production and ensure employment generation. The government should also ensure that adequate financial allocations are made for security and infrastructural development of all parts of Nigeria, in addition to investing in research for local capacity building to detect, deter and effectively respond to threats emanating from internet sources.

References

Adam, E. M., Osah, G., & Alao, D. O. (2019). From Civilization to the Dark ages: Addressing violation of Human Rights in Northeast Nigeria. *European Journal of Social Sciences, 58*(3), 211-222.

Adesegun, O., & Ayenakin, O. O. (2015). Insecurity and Foreign Direct Investment in Nigeria. *International Journal of Sustainable Development & World Policy, 4*(4), 56-68. https://doi.org/10.18488/journal.26/2015.4.4/26.4.56.68

Adibe, J. (2013). *What do we really know about Boko Haram?* In Ioannis Mantzikos, Boko Haram: Anatomy of a Crisis. E-International Relations.

Afolabi, A. (2015). The Insurgence and Socio-political Economy in Nigeria. *International Journal of Development and Economic Sustainability, 3*(5), 61-74.

Alao, D. O., & Osah, G. (2018). A Mid-Term Analysis of President Muhammadu Buhari's Change Agenda on Sustainable Peace and Development in Nigeria. *Lead City Journal of the Social Sciences, 3*(1), 1-13.

Agbakwuru, J., & Ugbor, E. (2018). *SARS: Osinbajo orders probe of abuses as IG rejigs squad.* Vangaurd News Paper. Retrieved from https://www.vanguardngr.com/2018/08/sars-osinbajo-orders-probe-of-abuses-ig-rejigs-squad/

Ajakaye, R. (2014). *Nigeria central bank denies funding Boko Haram.* Anadolu Agency (Turkey), October 22, 2014. Retrieved from http://aa.com.tr/en/world/nigeria-central-bank-denies-funding-bokoharam/108663

Ajani, J. (2014). *Funding of Terror Network: 'Boko Haram got over N11bn to kill and maim'.* May 4, The Vanguard. Retrieved from https://www.vanguardngr.com/2014/05/funding-terror-network-boko-haram-got-n11bn-kill-maim/

Aladenusi, T. (2015). *Cyberharam: Can Nigeria prepare for the next generation of terrorists? Nigeria Cyber Alert.* Retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/cyberharamcan-nigeria-prepare-for-the-next-generation-of-terrorists.html

Andyopadhyay, S., Sandler, T., & Younas, J. (2011). Foreign direct investment, Aid, and terrorism: An analysis of developing countries. Federal Reserve Bank of St. Louis. *Working Papers, 12*(3), 321-435. https://doi.org/10.20955/wp.2011.004

Alao, D. O., & Nwogwugwu, N. (2015). Does Cyclical Explanation Provide Insight to Protracted Conflicts in Africa. *Arabian Journal of Business and Management Review. Nigerian, 3*(11). https://doi.org/10.12816/0017686

Alao, D. O., Atere, C. O., & Alao, O. (2012). Boko-Haram Insurgence in Nigeria: The Challenges and Lessons. *Oman Journal of Business and Management Review, 2*(2). https://doi.org/10.12816/0002250

Alao, D. O., & Osah, G. (2018). A Mid-Term Analysis of President Muhammadu Buhari's Change Agenda on Sustainable Peace and Development in Nigeria. *Lead City Journal of the Social Sciences, 3*(1), 1-13.

Arimatéia da Cruz, J. (2013). Terrorism, War, and Cyber (In)Security. *Small War Journal.* Retrieved from http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity

Aro, O. I. (2013). Boko Haram Insurgency in Nigeria: Its Implication and Way Forward toward Avoidance of Future Insurgency. *International Journal of Scientific and Research Publication, 3*(11), 1-8.

Bantekas, L. (2007). *International Criminal Law* (3rd ed., p. 265). Routledge-Cavendish Publication.

Beck, U. (1992). *Risk Society: Towards a New Modernity.* London: Sage.

Carnegie Endowment for International Peace. (2019). *Timeline of Cyber Incidents Involving Financial Institutions.* Retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Caulderwood, K. (2014, May). Fake Charities, Drug Cartels, Ransom and Extortion: Where Islamist Group Boko Haram Gets Its Cash. *International Business Times.*

CEIC. (2018). *Nigeria Foreign Direct Investment 2008-2018.* Central Bank of Nigeria. Retrieved from https://www.ceicdata.com/en/indicator/nigeria/foreign-direct-investment

Cunningham, W. G. Jr. (2003). Terrorism Definitions and Typologies. In *Terrorism: Concepts, Causes, and Conflict Resolution.* Retrieved from http://terrorism.about.com/od/causes/a/causes_terror.htm

Cunningham, W. G. Jr., Friedman, A., Hauss, C., Hersey, M., Moore, R. S., Sandole, J. D., & Sheehan, S. (2003). *Terrorism: Concept, Courses and Conflict Resolution.* Advanced Systems and Concepts Office Defense Threat Reduction Agency and Working Group on War, Violence and Terrorism. Virginia: Defense Threat Reduction Agency. January.

Daily Trust. (2010). *Nigeria: Sim Card Registration - a Policy Dead On Arrival? All Africa.* Retrieved from https://allafrica.com/stories/201005050339.html

Denning, D. E. (2001). Cyberwarriors: Activists and Terroritsts Turn to Cyberspace. *Harvard International Review, 23*(2), 70-75.

Digital 2019: Global Digital Overview. Retrieved from https://datareportal.com/reports/digital-2019-global digital-overview

Erhabor, I. M. (2008). *Cybercrime and the Youths* (PGDE Thesis, p. 37). Department of Education, Ambrose Alli University, Ekpoma, Nigeria.

Essays, U. K. (November 2013). *Applying Criminological Theories to Cyber Crime.* Retrieved From https://www.ukessays.com/essays/criminology/explaining-cybercrime-using.php? vref= 1

Eye Witness News. (2017). *Unicef: Boko Haram child bombings in Nigeria quadrupled in 2017.* Retrieved from https://ewn.co.za/2017/08/23/unicef-boko-haram-child-bombings-in-nigeria-quadrupled-in-2017

FATF. (2013). *FATF Report on Terrorist Financing in West Africa.* FATF & GIABA: Paris, France.

Fanusie, Y. J., & Entz, A. (May 2017). *Boko Haram Financial Assessment Center on Sanction and Illicit Finance.* Retrieved from http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-boko-haram-financial-assessment/

Forster-Bowser, E., & Sander, A. (2012). *Security Threats in the Sahel and Beyond: AQIM.* Boko Haram and al Shabaab, Civilian-Military Fusion Center, Norfolk VA, United States.

Global Forum for Cyber Expertise (GFCE). (2016). The Budapest Convention on Cybercrime: A framework for capacity building. *Global Cyber Expertise Magazine.* Retrieved from https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime

Grabosky, P. N., & Smith, R. G. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities.* New Brunswick, NJ: Transaction Publishers.

Haruna, A. (2019, January 20). *How Boko Haram attack destroyed Nigerian community, Rann.* Premium Times. Retrieved from https://www.premiumtimesng.com/regional/nnorth-east/306674-how-boko-haram-attack-destroyed-nigerian-community-rann.html

Hoffman, B. (1998). *Inside Terrorism.* New York: Columbia University Press.

Jacob, J. U., & Akpan, I. (2015). Silencing Boko Haram: Mobile Phone blackout and counterinsurgency in Nigeria's Northeast region stability. *International Journal of Security and Development, 4*(1), 1-17. https://doi.org/10.5334/sta.ey

Jacobson, M. (2009). Terrorist Financing on the Internet. *Combating Terrorism Center Sentinel, 2*(6).

Jonathan, J., Nick, & George, G. (2004). *Perceptions of Risk in Cyberspace.* Cyber trust and Crime Prevention Project. Retrieved from http://scholar.google.co.uk/scholar_url?url=http%3A%2F%2F

Kareem, Y. (2018, June 25). Nigeria has become the poverty capital of the world. *Quartz Africa.* Retrieved from https://qz.com/africa/1313380/nigerias-has-the-highest-rate-of-extreme-poverty-globally/.

Kasznár, A. (2018). *The Challenges of the Cyber-terrorism.* Hadmérnök (XIII) I1. Retrieved from http://www.hadmernok.hu/182_28_kasznar.pdf

Kegley, C. W. Jr. (Ed.). (1990). *International Terrorism: Characteristics, Causes, Controls.* New York: St. Martin's Press.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology: Acritical review of the technology acceptable model. *Information and Management, 40,* 191-204. https://doi.org/10.1016/S0378-7206(01)00143-4

Lewis, J. A. (2002). *Assessing the Risks of Cyberterrorism, Cyber War, and Other Cyber Threat.* Center for Strategic and International Studies. Retrieved from https://www.csisorg/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

Mckenna, J. (2005). *Implications of transnational terrorism on international trade.* Retrieved from https://econ.duke.edu/uploads/assets/dje/2006/McKenna.pdf

NCC. (2018). Active mobile lines in Nigeria hit 144 million in December. *The Premium Times.* Retrieved from https://www.premiumtimesng.com/news/more-news/257906-active-mobile-lines-nigeria-hit-144-million-de cember-ncc.html

Ntamu, G. U. (2014). Boko Haram: A treat to National Security. *European Scientific Journal, 10*(17).

Obayuwana, O. (2011, October 3). *The Terror Cells up There, threatening Nigeria.* The Guardian (Lagos).

Stephanie, T. Solansky University of Houston-Victoria solanskys@uhv.edu. See all articles by this author Search Google Scholar for this author.Odiogor, H. (2011, November 21). Cyberterrorism and Nigeria's Economy. *Vanguard Newspaper.* Retrieved from https://www.vanguardngr.com/2011/11/cyber-terrorism-and-nigeria%E2%80%99s-economy/

Office of the National Security Adviser: Counterterrorism Center. (2017). *Nigerian Government Presents Policy Framework and National Action Plan for Preventing and Countering Violent Extremism to Members of the Public.* Retrieved from http://ctc.gov.ng/nigerian-government-presents-policy-framework-and-national-action-plan-for-preventing-and-countering-violent-extremism-to-members-of-the-public/

Oludimu, T. (2018). *How the SARS menace is affecting workers in the Nigerian tech community.* FXTM. Retrieved from https://www.forextime.com/register/open-account?myfxtm=open-Account

Oluwafemi, O., & Adesuyi, F. A. (2013). Combating Terrorism with Cybersecurity: The Nigerian Perspective. *World Journal of Computer Application and Technology, 1*(4), 103-109.

Osho, O., Adesuyi, F. A., & Shafil, M. A. (2013). Combating Terrorism with Cyber Security: The Nigerian Perspective. *World Journal of Computer.*

Onuoha, F. C. (2011). Boko Haram's tactical evolution. *African Defence Forum, 4*(4).

Orngu, C. S. (2014). *Globalization, Imperialism and the dialectics of Economic diplomacy in Africa.* Makurdi: Gwatex Publishers.

Oriakhi, D., & Osemwengie, P. (2012). Impact of national security on foreign direct investment in Nigeria: An empirical analysis. *Journal of Economics and Sustainable Development, 3*(13), 10-43.

Orija, B. (2014). Revealed! How Middle Eastern Backers Fund Boko Haram. *Nigerian Communication Week.* Retrieved from http://www.nigeriacommunicationsweek.com.ng/other-business/revealed-how-middle-eastern-backers-fund-boko-haram#sthash.0tpDnSkK.dpuf

Pillar, P. R. (2001). *Terrorism and U.S. Foreign Policy.* Washington, D.C.: Brookings Institution Press.

Relief Web. (2018). *UNICEF Nigeria Humanitarian Situation Report, January - June 2018.* Retrieved from https://reliefweb.int/report/nigeria/unicef-nigeria-humanitarian-situation-report-january-june-2018

Rogers, E. M. (2003). *Diffusion of Innovations.* New York: Free Press.

Sakar, O. U. (2015). *Our Flag is Changing Colour; Oh! Mother Africa.* Retrieved from https://www.linkedin.com/pulse/our-flag-changing-colour-oh-mother-africa-uchechukwu-obiajulu-sakar

Suleymasn, S. (2008). *Cyber Terrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task, in Responses to Cyber Terrorism* (1st ed., pp. 74-75). Centre of Excellence Defense against Terrorism.

Statista. (2018). *Nigeria: Youth unemployment rate from 2007 to 2017.* Retrieved from https://www.statista.com/statistics/812300/youth-unemployment-rate-in-nigeria/

Tehrani, P. M. (2017, April). The Challenges Faced by International Organisations in Curbing Cyberterrorism. *Cyberterrorism The Legal and Enforcement Issues,* 79-133. https://doi.org/10.1142/9781786342133_0002

Tyendezwa, T. G. G. (n. d.). *Legislation on Cybercrime in Nigeria: Imperatives and Challenges.* Retrieved from https://www.ncc.gov.ng/documents/233-legislation-on-cybercrime-in-nigeria-imperatives-and-challenges/file

Tehrani, P. M., Manap, N. A., & Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review, 29*(3), 207-215. https://doi.org/10.1016/j.clsr.2013.03.011

The Cable. (2014, August 31). *EXCLUSIVE: Boko Haram 'funded through CBN'.* Retrieved from https://www.thecable.ng/exclusiveboko-haram-funded-through-cbn/2

The Save Humanity Advocacy Centre, SHAC. (2018, July 15). *Boko Haram: Cyber-terrorists out to frustraterelocation of IDPs back home.* Vanguard. Retrieved from https://www.vanguardngr.com/2018/07/boko-haram-cyber-terrorists-out-to-frustrate-relocation-of-idps-back-home-shac/

Thibiebi, L. (2018, September 3). *An evaluation of Nigeria's food import bill.* Ships and Ports. Retrieved from http://shipsandports.com.ng/evaluation-nigerias-food-import-bill/

Tshabalala, S. (2015, October 26). *Nigeria is fining MTN $1,000 per illegal sim card even though customers generate just $5 a month.* Quartz Africa. Retrieved from https://qz.com/533041/africas-largest-mobile-network-is-being-fined-5-2-billion-for-flouting-nigerias-sim-card-rules/

Umeagbalasi, E., & Ijeoma, J. (2014). *Spending for mass murder: How Nigerian Government squandered $23billion (N3.6 trillion) on failed security in four years (2011-2014).* News Express. Retrieved from http://www.new.expressngr.com/news/detail.php?news=5866

Urbas, G., & Choo, K. R. (2008). *Resource materials on technology-enabled crime.* Australian Institute of Criminology, No. 28.

Vanguard. (2018, December 25). Be wary of Boko Haram propaganda, Buratai admonishes troops. Retrieved from https://www.vanguardngr.com/2018/12/be-wary-of-boko-haram-propaganda-buratai-admonishes-troops/

Vanguard. (2016). *I'll fight Nigeria, whole world, Boko Haram's Shekau boasts in new video.* Retrieved from https://www.vanguardngr.com/2016/08/ill-fight-nigeria-whole-world-boko-harams-shekau-boasts-new-video/

Varghese, J. (2014, August 31). Australian Negotiator Claims Central Bank of Nigeria Is Funding Boko Haram. *International Business Times.* Retrieved from http://www.ibtimes.co.inaustralian-negotiator-claimscentral-bank-nigeria-funding-boko-haram-607992

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden.

Wall, D. S. (2008). *Cybercrime*. Malden, MA: Polity Press.

Weimann, G. (2004). *Cyber terrorism How Real is the Threat?* United States Institute of Peace, Special Report 119. Retrieved from https://www.usip.org/sites/default/files/sr119.pdf

Yar, M. (2006). *Cybercrime and Society.* Thousand Oaks, CA: SAGE Publications Ltd.

Copyrights