# HARNESSING CYBERSPACE INTELLIGENCE AND THE FIGHT AGAINST BOKO HARAM IN NORTH-EASTERN NIGERIA

**Benjamin Tyavkase Gudaku**
Ph.D candidate of Benue State University, Makurdi in the department of Religion and Philosophy. He is studying African Traditional Religion.

**Grace Koko Twaki**
Lecturer, Computer Department, FCT College of Education, Zuba.

**ABSTRACT:** *Intelligence gathering is key to the war against terrorism. However, intelligence in the 21st century cannot make the desired impact without the use of cyber-space and cyber-intelligence. This is because terrorists in their resolve to over-come national boundaries in order to inflict terror on the populace find cyber-space as handy tool to use. Therefore, this paper argues that checkmating and monitoring the cyber-space is not an option but imperative to succeed the battle against terrorism. Evidence abound that Boko haram insurgents in Nigeria have appreciable track record of making use of cyber-space to perpetrate their atrocities. However, this paper discovers to its chagrin there is near lack of monitoring of Nigeria's cyber-space. As a result, the terrorists are having a field-day in its usage. This has negative consequence on the nation's quest to defeat boko haram. The paper therefore, challenges the security hierarchy in Nigeria to as a matter of urgency rise to the occasion.*

**KEYWORDS:** Boko haram, cyber-space, intelligence, cyber-intelligence, terrorism

## INTRODUCTION

Man is the author and victim of progress and change. It can, therefore, be argued that man is both the subject and object of progress in the changing world. The fact is that man has progressed; for instance, from peasantry to mechanized agriculture; from using animals as the only available means of transportation to the use sophisticated automobiles such as aeroplanes. The advent of the internet has made thin the wall of ideological differences and compromised geographical distance. As such what happens anywhere on the globe is instantly almost everywhere.Much more is the fact the gamut of cyber space and its potentials offer many choices that were hitherto not only absent, but simply impossible. For instance, cyber intelligence was not available a couple of decades ago.

The emergence of cyber space has greatly changed intelligence architecture that was in existence. It has necessitated the rigging of the intelligence cycle of identifying Essential Elements of Information (EEI), to collection, analysis and distribution. While different actors were required in the different phases of the intelligence cycle, cyber space has made it possible for an individual to be involved in all the phases of the cycle. For instance with Web, 2:0 culture, where both the producer and consumer of information interact on the internet, it is very easy to have a broad-based opinion on an issue and to identify Essential Elements of Information (EEI); that can be tailored into intelligence. Alvin & Heidi (2006) opine that Web 2.0 expresses the idea of the prosumer (producer+ consumer). Ufuophu-Biri (2013) explains further that Web 2.0 emphasizes activeparticipation, connectivity, collaboration and sharing of knowledge and ideas among users. Simon-Tov &Ofer (2013) also attest that Web 2.0 is a technological infrastructure for sharing and creating content. This is unlike Web, 1:0 culture~~that~~which is unidirectional, and often the product of only the webmaster. The danger of Web, 2:0 cultureis a foe that can pretend to be a friend just to know your view and pre-empt you. The Facebook, Whatsapp,flickr, Digg, blog Wikipedia among others are classical examples.

It is undoubtedly true that the Facebook and its related platforms are indeed the 'wisdom of the crowd via technology'. However, the challenge of using these ICT platforms isknowing when and where to say so little in order to conceal, and when and where to say much for the purpose of revealing, especially Essential Elements of Information (EEI) that are crucial for intelligence gathering. The second throng of the argument is aptly captured by the USA renowned security expert, Woodward (1987), when he observed that "everyone always says more than they are supposed to". This is highly applicable to the use of cyberspace. As a result, it has made cyber space intelligence much easier than it should have been since critical information is always there in the public domain via the tool of cyberspace. To this extent, cyberspace has become one of the most pressing and prominent national security issue; not only in Nigeria but the world at large. What has aggravated this situation is the technification of societies that has increased dependency on the cyberspace on one hand and vulnerability cloud that hovers on society on the other hand.

Berkowitz (2007) notes that while technological development and exponential growth of the World -Wide- Web has enhanced the possibility of breaking opponent's systems and reaching the data, it has even increase the chances of grand cyber-attack that has remain part of the bigger strategy on how to win a war or beat the opponent at war. The implication is that leaving the cyberspace without blocking the possibility of what Berkowitz warns is doing so at one's own peril. This accounts for why some countries have some form of cyberspace regulation.As a matter of fact, it has become abundantly clear that cyberspace intelligence is a new trend that has replaced the antediluvian idea of spying. It suffices, therefore, to say that the craftiness and control of information or networks has become the base ground for modern warfare.

Peace will continue to elude the world (Nigeria inclusive) if cyberspace is negatively used to plan and coordinate attacks or other nefarious acts, for that matter. Hence, one sure way of achieving peace in the modern world is by not allowing unhindered and free range of the cyberspace without spying for potential danger that can be detected and averted via cyber intelligence. Another dimension is that security personnel, especially those engaged in fighting any war or insurgency as in the case of Boko Haram in North-east Nigeria should be mindful of engagement with the cyberspace with a view to avoid revealing Essential Elements of Information (EEI) that terrorist can use for intelligence.

## Statement of the problem

The threat to life and property posed by *Boko Haram*, especially in north-east Nigeria is very worrisome. Undoubtedly, it has become a nightmare, not only to Nigerians and the Nigerian government or the West African sub-region but indeed the entire world. The alarming killings of lives and destruction of property in addition to other heinous crimes by Boko Haram undermine the constitutional responsibility of the Nigerian government to ensure safety of citizens. It is therefore, no surprise that in 2009, Nigeria was listed among the 15 most vulnerable nations in the world (*Sunday Nation*, 2009; Ocholi, 2009). Since the emergence of Boko Haram, the federal government of Nigeria has put in place measures of combating the Boko Haram menace. One of such measures is the formation of Joint Task Force (JTF) with members drawn from all the armed forces and the Nigerian Police Force (NPF). However, it is regrettable to observe that until now (2015) the fight against Boko Haram by the federal government troops is not yet successful. This is in spite of the fact that the federal government's troops are backed by the Mutli- National Joint Task Force, which comprises of troops from Nigeria's neighbouring countries of Cameroon, Chad and Niger.

As a matter of fact, Boko Haram operates with unwavering dexterity in its persistent attacks and presence despite efforts to curb its manoeuvre that typifies the guerrilla warfare style. Until recently, Boko Haram attack strategy was far from technology. However, since its association with Al-qaeda, Boko Haram has demonstrated a vastly changed approach to executing its attacks. It has shown significant use of cyber space and its opportunity of Information and Communication Technology (ICT) to coordinate attacks. This is not strange anyway; particularly that cyber space has been part of the terrorists' warfare tool kit since 1998. What is rather strange is the inability of Nigeria's security architecture to use same cyberspace to counteract Boko Haram terrorist attacks. This would have brought out the dual use of cyber space as a tool for and against terrorist acts. This failure is too strategic to be overlooked.

This, therefore, demands for more than cursory appraisal but thorough investigation. Of truth, so much research works have interrogated the failure of the Nigerian state to effectively combat Boko Haram. However, the use of cyber space, especially ICT-generated intelligence to halt or thwart the activities of Boko Haram has received very little attention. In order to provide for this dearth, this study shall undertake an examination of how Boko Haram has taken advantage of ICT to recruit, raise funds and coordinate attacks.

## Objectives of study

This study will seek to find out whether the Nigerian government has done enough to block the cyberspace, which Boko Haram is using in perpetrating their crimes and planning as well as executing attacks. The study shall specifically:

- Determine the extent Boko Haram has used cyber space, especially ICT in their on-going fight against the Nigeria state in North-East Region.
- Identify commonest ICT Platform(s) that Nigerian security agents engaged in combating Boko Haram use in exchanging information among themselves and non-military persons.
- Identify measures adopted by the Nigerian security agents to block the cyberspace are adequate to counter Boko Haram's use of the cyberspace.
- Find out if there are factors militating against strategies adopted by the Nigerian security agents to block the cyberspace especially in the area of Essential Elements of Information (EEI).
- Determine whether there are better strategies that could be adopted in blocking the cyberspace to prevent Boko Haram from using it to wage war against the Nigeria State in North-East Region

## Significance of study

Siman-Tov & Ofer (2013) posit that "turning information into intelligence is a science in and of itself". While it is arguable, and rightly so, that intelligence can be used as a tool for peace or against peace, this study encourages the Nigerian government to make use of cyber generated intelligence models to curtail attacks of Boko Haram, and as a step towards defeating Boko Haram to peace to once again return to the troubled region of north-east. The centrepiece of the argument in this study is that ICT poses new sets of strategic vulnerabilities. For it is not only the Ak-47 gun that it indispensible for the terrorist to wreck havoc, but the laptop, smart phone, tablet among others. Therefore, the study calls on the Nigeria government to rise up to this challenge, if it must guarantee security of lives and property of the citizens in fulfilment of its constitutional mandate.

## Theoretical Framework

The theoretical framework for this study is Asymmetric Warfare. This is the war between intimidators whose relative military power differs, or whose strategy or tactics differ significantly. Asymmetric warfare can describe a conflict in which the resources of two belligerents differ in essence and in the struggle, interact and attempt to exploit each other's characteristic weaknesses. Such struggles often involve strategies and tactics of unconventional warfare, the weaker combatants attempting to use strategy to offset deficiencies in quantity or quality (Tomes, 2004). Such strategies may not necessarily be militarized (Stepanova, 2008). Asymmetrical warfare is also used to denote a military tactic or mode of operation that exploits the opponent's weaknesses and vulnerabilities and emphasizes differences in forces, technologies, weapons and rules of engagement (Long, 2010). War, according to Carl Von Clausewitz, is the continuation of politics by other means. He further asserted that asymmetrical warfare refers to armed conflicts to achieve political objectives, and as the name implies, involves an unbalanced distribution of power (Clausewitz, 1976). Unlike most conventional warfare, it is usually initiated by the weaker side.

Although all armed political conflicts have much in common, their strategic objectives can differ widely. The primary strategic objective of asymmetrical warfare is psychological, and less military. It is to intimidate the adversary psychologically by directly or indirectly inflicting fear and terror in order to achieve its political agenda. In more graphic terms, it is, the collective use and threat of violence that is directed at one set of targets—the victims—to compel compliance or allegiance from another set of targets (targets of demands) or to impress a wider audience that is not directly involved in a specific conflict (the mass media, the general public, world opinion, other governments, etc. (Crelinsten, 1989).The use of asymmetric warfare as the theoretical framework in this study is based on the modus operandi of the Boko Haram terrorist in using both the unconventional military method of executing the war and the use of technology in propagating and recruiting sympathizers for their nefarious activities.

Asymmetrical combatants generally use covert terrorist and unconventional guerrilla warfare tactics and seek to avoid direct military encounters with the adversaries' vastly superior armed forces. This is in sharp contrast to conventional military warfare strategies that involve direct military-on-military confrontations with the strategic objective being to erode the enemy forces' will to fight, and thereby to produce decisive military victories that can force the defeated side to accept the victors' terms. The second but vital strategic objective in asymmetrical warfare is to win the hearts and minds of potential sympathizers and supporters, thereby gaining financial and logistic support, safe haven, and the ability to recruit new combatants. No asymmetrical organization or movement can long survive much less achieve its political objectives without a significant outside support system. This informed the use of the theory of asymmetric warfare for this study. It is important to agree with Arregun-Tift (2001) that if power implies victory war, then weak actors should almost never win against stronger opponents, especially when the gap in the relative power is very large. Yet history suggest otherwise: weak actors sometimes win. This is what Boko Haram seems to be demonstrating.

## METHODOLOGY

The study will adopt a survey design. Moreover, primary and secondary sources will be used for this study. The use of primary sources will require the instruments of structured and unstructured questionnaires while the use of existing literature on the subject matter will constitute secondary sources. Qualitative, quantitative and interpretative methods will be used in analysing the data collected. Qualitative method will guide the researcher to arrive at themes, motives and trends in the security landscape of Nigeria. Since it will be of great importance to know what percentage of security personnel involved in the fight against Boko Haram make use of what platform available on cyberspace, quantitative methodology will play a role in determining this and other related percentages incidental to the study. Collection of data without interpretation, will amount to a job half done. Therefore, the interpretative method shall be a useful tool for comprehensively analysing the data for it to be understood; which is the final end of the study. Descriptive Statistics will be used making use of mean and standard deviation for the analysis.

## REVIEW OF RELATED LITERATURE

Cyber warfare is experiencing a boom in Nigeria because of Boko Haram's affiliation with Al-qaeda. Baken (2013) observes that al-qaeda has used internet as a vital communication vehicle since 1996, suggesting that Boko Haram incorporation of cyber into its arsenal is almost inevitable due to its affiliation with Al-qaeda and other terrorist groups. Oluwafemi (2013) is right on point to have raised alarm that terrorist groups are taking advantage of ICT potentials to recruit, propagate their propaganda, train its members, communicate and conspire and even raise money. Baken (2013) corroborates in a warning style that perpetrators of cyber warfare can use the demographic of Nigeria and the Sahel to train, recruit and execute attacks

It is likely that this is what has led to Boko Haram's tactical advancement. This would seem to suggest that Nigeria and its neighbouring Sahel region are ripe for exploitation as cyber warfare hub. Providing an example to this, Baken (2013) points out that in August 2012, Boko Haram reportedly hacked the personnel records database of Nigeria's secret service. The individual who successfully compromised the covert -personnel data indicated the breach was executed in the name of Boko Haram and as a response to Nigeria's handling of interactions with the group. This is too serious a threat to national security to be ignored.

There is no one satisfying and all-encompassing definition of the term cyberspace. If anything at all, the existing definitions are contradictory. For instance, Joint Publication (2006) defines cyberspace as the notional environment in which digitized information is communicated over computer network. As if in concurrence with the idea of notional environment, University of New Orleans (2006) says that cyberspace is the non-physical space where interactions take place between computer networks. Essentially tied to the understanding of cyberspace is the use of computer network(s). Little wonder, Klingova clarifies that the prefix 'cyber' originates from the word cybernetics and it literally means "through the use of computer" (Klingova, 2013, P. 9).
It is therefore understandable why Princeton University (2006) defines cyberspace as a computer network consisting of world network that use the TCP/IP network protocols to facilitate data transmission and exchange. On his part, Cavelty (2012) observes that cyberspace encompasses the fusion of all communication networks, databases and sources of information into a vast, tangled and diverse blanket of electronic exchange [it is a network ecosystem], which is virtual and immaterial bioelectronics environment that is literally universal. The explanation of Cavelty

clarifies the misconception of comparing cyberspace to World Wide Web. It is much more than opening the internet explorer, but includes all that is associated with Information and Communication technology. What is means is that Klingova (2013) was right on point to have stated that cyberspace refers to activities that the use of computers and other electronic devices and thus make a distinction between the electronic and physical world.

The fact is that there has been an upward surge in the use of the cyberspace in Nigeria via the Global System for Mobile communications (GSM) network providers, as an average Nigerian uses a mobile phone, while internet penetration is growing steadily on a daily bases (Osho et al, 2013). Further to that is the fact that Nigeria has the largest mobile market on the African continent with over 90 percent of individuals and corporate organizations relying completely on the mobile industry for their day-to-day transactions (Nwanga et al, 2015). And according to the statistics from the Nigerian telecommunication regulator, National Communication Commission NCC (2014), the teledensity in Nigeria is at 94.4 percent as at August, 2014 and active lines at 133 million subscribers out of 167 million connected GSM lines in a country of about 160 million populations.

This shows a rapid growth in the country's connectivity. This has in turn led to the abuse of the cyberspace, because according to Internet Crime Report (2012), Nigeria ranks among the worst countries in the abuse of ICT. It is used to carry out unlawful acts by criminals, terrorists and other undesired agents of the society. The present day technology and social advances through the internet especially the social media has made it possible for terrorist to create and heighten public anxiety and also show the global world the level of destruction that could be carried out by them as usually demonstrated by Boko Haram.

It is a known fact that Boko Haram attack civilian populations with the objective to kill as many people as possible and to create chaos, destruction and psychological fear on their victims and often showcase these atrocities using the cyberspace. One wonders why the Nigerian government has failed to evaluate and analyse terrorist communication using transaction-based models to foil attacks. (Allanach et al., 2004) hint that transaction-based model is not solely relying on the content of the information gathered, but more on the significant links between data which are people, places and objects that appear to be suspicious.

How to trace the dynamic evolution, communication and movement of terrorist groups across different jurisdiction in Nigeria and how to analyze and predict terrorists activities, associations, and threats becomes an urgent and challenging issue (Chen, et al., 2004). Many terror-related groups use the web as a convenient, anonymous communication infrastructure. This infrastructure enables an exchange of information and propagation of ideas to active and potential terrorists. The Boko Haram as a terrorist group is not left out in employing cyber systems to perpetrate and perpetuate their messages. It will not be too suggestive to opine that given this trend, cyber-attacks may come up among the list of possible avenues through which this group will vent their anger on a global scale (Ajike & Longe, 2014). However, the concern is hoe the Nigerian security apparatus can spy on cyberspace to provide access to critical, real-time information, and crucial and timely location of the insurgents proactively and stop them before they unleash terror on unsuspecting citizens.

An example to drive home this point is when the Nigerian government seized control of the more than 150 million mobile telephone lines in the country; and directed of Nigerian Communication

Commission (NCC) in 2011 to register all mobile telephone lines in the country in order to 'enhance the security of the state' and to enable operators to have 'predictable profile about the users in their networks' according to NCC. SIM registration started on 28 March 2011 and ended officially in January 2012 after which all unregistered SIMs were deactivated. With this information, the intelligence gathering capability of the Nigerian security services was remarkably enhanced, and a number of key Boko Haram commanders were captured, including Sani Mohammed, Kabir Sokoto and Shuaib Mohammed Bama who was arrested in the home of a popular politician (Vanguard Newspaper 2012).

A similar example is that on 23 May, 2013, when the military shut down mobile communications which was limited to GSM in the three north-eastern states of Adamawa, Borno and Yobe. According to the military, the objective of the shutdown was to limit Boko Haram's communications capabilities, restrict their ability to regroup and re-enforce and also limit their ability to detonate improvised explosive devises. During the blackout, State security forces developed new ways of communicating. The Nigerian police, for example, deployed an alternative mobile communication system using Code Division Multiple Access (CDMA) on Global Open Trunking Architecture (GOTA) from the Chinese manufacturer ZTE (Jacob &Apkan, 2015). Since it was only GSM lines that were blocked, it was possible for the police to use CDMA with ease. The GOTA phones were distributed to police officers in North-Eastern Nigeria just before the mobile phone shutdown. This enabled the police, along with other state security units, to circumvent the shutdown. Although this action had its adverse effect on social, economic and security situation in those areas, the success of the action is that it made it possible for members of the sect to be driven from Maiduguri and its environs to the vast and treacherous Sambisa Forest.

The justification for Nigeria to take the issue of cyber intelligence as a top priority lies in the fact that the nation is fighting insurgency; and the insurgents are using cyber intelligence to wreak havoc on the nation and her citizens. This implies therefore that for Nigeria to win the war of insurgency, she must harness her resourcefulness in terms of cyber intelligence. Furthermore, the effects of cybercrimes on Nigeria include reducing the competitive edge, waste of production time and damage to the image of the country. Meanwhile, With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated. Some of the ways of combating such crimes include taking reasonable steps to protect ones property by ensuring that firms protect their IT infrastructure like Networks and computer systems. It is also important that government should ensure that cybercrime laws are formulated and strictly adhered to and individuals should observe simple rules by ensuring antivirus protection on their computer systems.

## CONCLUSION

Thus far, this paper has discussed the need to improve cyber-intelligence as deliberate means of counter terrorism in Nigeria. While the importance of this cannot be over-emphasized, the need to also caution security personnel involved in the fight against terrorism from divulging Essential Elements of information (EEI) is a task that needs urgent attention of the authorities concerned. This is because the terrorists prey for such sensitive information to enable strategize and to remain step(s) ahead of the security. It is only when they do so that they can strike largely successfully. War against terrorism cannot be fought and won without high-level technology. To this extent, the paper discovers that the Nigerian state is ill equipped and prepared.

## Recommendations

From the foregoing, this paper recommends that:

- Cyber-intelligence should be an integral part of training for security personnel in Nigeria.
- Cyber-space needs to block just as the physical space if the war against boko haram is to successful won and in no distant time.
- Security personnel in Nigeria need training and retraining in handling information that can easily be processed into security intelligence.
- Proper registration of all users of mobile networks in the country. Any service provider that fails to comply should be penalized according extant laws.

## REFERENCES

### Books

Alvin, T. & Heidi, F. (2006).*Revolutionary Wealth.* New York: Doubleay.

Baken, D.N. (2013). Nigeria's Vulnerability to Cyber Warfare. In Mantzikos, I. (Eds.).*Boko Haram- Anatomy of a Crisis.* Bristow: E-International Relations

Berkowitz, B. (2013). *The New Face of War: How War Will be Fought in the 21st Century*. New York: The Free Press.

Cavelty, D.M. (2012). Cyber Security.In Collins, A. (Eds.).*Contemporary Security Studies*. New York: Oxford University Press.

Stepanova, E. (2008 ). Terrorism in asymmetrical conflict: SIPRI Report 23 (PDF). Oxford: Oxford University Press

Tomes, R. (2004).Relearning Counterinsurgency Warfare" (PDF).Parameters (US Army War College).

Woodward, B. (1987). *Veil: The Secret of Wars of the CIA 1981-1987.* London: Simon and Schuster.

### Journal Articles

Ajike, C. & Longe, O.B. (2014).'The Boko Haram insurgency in Nigeria: A security officers perspective on the American angle'. *Computing, Information Systems, Development Informatics & Allied Research Journal*, 6 (2), 30-35.

Ajike, C. A. (2015). A Trend analysis of Boko Haram Insurgent and Computer Generated Intelligence in Counter-insurgency in North East Nigeria. *Computing, Information Systems, Development Informatics & Allied Research Journal*, 6 (2), 29-36.

Arregun-Tift, I. (2001). How the Weak Win Wars. *International Security*, 26 (1), 93-128.

Clausewitz, (1976).Section 24, in the Princeton University Press translation.

Oluwafemi, O., Falaye, A.A. &Shafi'I, M.A. (2013). Combating Terrorism with Cyber Security: The Nigerian perspective. *World Journal of Computer Application Technology*, 1(14), 103-109.

Siman-Tov, D. & Ofer, G. (2013). Intelligence 2.0: A new approach to the production of intelligence. *Military and Strategic Affairs*, 5 (3), 15-26.

Ufuophu-Birri, E. (2013). Perception and usage pattern of social media by students of higher institutions of learning in Delta state, Nigeria. *Journal of Communication and Media Research*, 5 (1), 15-26.

### Internet Sources

Allanach, J., Singh, H.S., Willeett, S.P. & Pattipati, K. (2004). Detecting and Tracking Boko Haram.*Journal of Asian Culture and History.*Retrieved from http://www.ccsenut.org on 16th August, 2015.

Crelinsten, R. D. (1989). "Terrorism, Counterterrorism and Democracy: The Assessment of National Security Threats," in Terrorism and Political Violence Data Analytics to Nigerian mobile Phone Industries". Paper accepted for publication in the proceeding of the 2015 Intl' Conference on Industrial Engineering and Operations Management (IEOM)https://www.law.cornell.edu/uscode/text/10/441

Joint Publication, (2000).Joint Tactics, Techniques and Procedures of Joint Intelligence Preparation for the Battle Space.Retrieved from http://www.dict.mil/doctrine/jel/new-pubs-jb6_0.pdf accessed 16th August, 2015.

Osho, O., Adesuyi, F.A. &Shafi'I, M.A. (2013).Combating terrorism with cyber security: The Nigerian perspective.World Journal of Computer. Retrieved from http://www.hrpub.org on 16th August, 2015.

University of New Orleans, (2006).Online distant learning glossary.Retrieved from http://alt.uno.edu/glossary.html on 17th August, 2015.

University of Princeton, (2006).wordNet search. Retrieved from http://wordnet.princeton.edu/perl/webwin on 17th August, 2015.

**Unpublished work**

Nwanga, M. E., Onwuka, En. Aibinu, A.M. & Ubadike, O.C. (2015). Impact of Big Data Analytics to Nigerian Mobile Phone Industries". Paper accepted for publication in the proceeding of the 2015 International conference on Industrial Engineering and Operations Management (IEOM), March, 2015.