ELECTRONIC SURVEILLANCE AND COUNTER-TERRORISM: PROSPECTS FOR THE NIGERIAN STATE

UJARA, Ese Christabel; IFALOYE, Oluwatosin Ruth; EKONG, Idongesit Daniel
Covenant University, Ota, Nigeria

Abstract

Nigeria's national security has been threatened over the past few years by the menace of terrorism. On a large scale, several efforts have been made by the Nigerian government to combat terrorism (mostly military based strategies), yet the threats persist. Crucial to the quest of combating terrorism in Nigeria is the role of technology. This is especially so because, terrorists also utilize modern technology, both online and offline in seeking funds, engaging operations, recruitment, training and communication. Thus, there is a need to not only evaluate offline activities, but also include the monitoring of online and digital communications in the counter-terrorism process. The general objective of this paper is to highlight important strategies rooted in electronic surveillance that the Nigerian state should adopt in counter-terrorism efforts that can ultimately guarantee national security and engender national development. Using a qualitative approach, this paper relies majorly on secondary data analyzed textually. It is situated within the securitization framework. This paper submits that technology exclusively cannot guarantee security, however, security would be an impossible accomplishment without the influence of technology. A collaboration of technological tools, especially through the use of electronic surveillance poses a potentially effective counter-terrorism strategy, as more and more terrorist operations depend on ICT tools.

Keywords: Terrorism; Counter-terrorism; Electronic Surveillance; Security; Nigeria

INTRODUCTION

Nigeria's national security has been threatened over the past couple of years by the menace of terrorism. The nature of terrorism is engendered by the quest to perpetrate havoc targeted at vulnerable elements of the society in order to influence and assert the desired change the terror organization seeks. These daunting terror attacks have therefore kept individuals in perpetual fear, robbing them of freedom and security (Joshua & Chidozie, 2014). While terrorist attacks have been prevalent in Africa in recent years, other regions of the world equally experience its torture and seek for its total eradication, particularly because of the insecurity, economic decline and retarded national development that comes with it. Indeed, since the wake of this millennium, terrorism has been on a steady rise; it can be characterized as one of the greatest threats to global peace and security stability in the contemporary international society (Okoli & Iortyer, 2014).

While Europe is constantly under threat by the Islamic State's attacks (Uhrmacher & Sheridan, 2016), within Nigeria, terrorism has found expression in Boko Haram group. Using the destructive strategy of suicide bombing, the group has been responsible for the loss of lives of people in their thousands as well as property worth millions of dollars since their emergence in 2009 (Okoro, 2014:103). The government in Nigeria has, at different times, adopted different approaches to combat terrorism from dialogue to military-based strategies. Each of these measures taken have either proved ineffective or counter-productive (Omale, 2013; Majekodunmi, 2015). In this light this study seeks to proffer an alternative measure to counter-terrorism – electronic surveillance. Due to the high costs counter-terrorism requires to function effectively, intelligence gathered via electronic surveillance costs less in terms of manpower and logistics while providing speed (Okauru, 2013). On April 13, 2013, America deployed its security system to track down the Boston Marathon bombers. In less than five minutes the world was made aware of the images of the two men that murdered a soldier on May 22, 2013 using advanced surveillance technology (Oludare, Omolara, Umar & Kemi, 2015). These scenarios were tackled swiftly due to access to relevant technology and ICT tools in tackling crime and terrorist activities. Nigeria needs to take a cue from these types of approaches in handling terrorism and dousing the insecurity challenges within the country in order to ensure national security and engender national development.

Using several sections, this study seeks to submit that terrorism is a threat to national security and as a result, more pre-emptive measures need to be taken in countering terrorism that differ from the existing measures. The study advances electronic surveillance as a more pre-emptive and potentially more successful strategy at countering terrorism in Nigeria when combined with the existing counter-terrorism strategies currently in implementation. Therefore, the paper is structured into the following: an introduction which includes research method, aims and objectives of the study; conceptualization of terrorism, counter-terrorism and electronic surveillance; securitizing terrorism in Nigeria; the link between electronic surveillance and counter-terrorism; and finally, conclusions and prospects for the Nigerian State.

The method this paper adopts is qualitative and analytical in nature. It relies heavily on textually analyzed data collected from secondary sources. The paper highlights historical evidence within the context of other regions of the world with the goal of drawing inferences for Nigeria. This paper aims at investigating the possibilities of electronic surveillance as a veritable tool for engaging counter-terrorism drawing from its use in other parts of the world with prospects for its success in Nigeria. This is against the milieu of the existing counter-terrorism strategies implemented by the federal government of Nigeria targeted at eradicating the menace. The study is significant as it is anticipated that it will suggest new insights into tackling the terrorist campaigns ongoing within the country as well as make additions to the existing body of knowledge on the counter-terrorism discourse. While several studies have been carried out on terrorism and counter-terrorism, few studies have sought to elaborate on the impact that electronic surveillance

can project to the process. Using the concept of securitization as a theoretical framework, the paper seeks to fill the identified existing gap in literature within the Nigerian context.

CONCEPTUAL CLARIFICATIONS

The following concepts will be clarified in the following segments in line with the arguments of the paper: Terrorism; Counter-Terrorism; and Electronic Surveillance

Terrorism

Central to the theme of this paper is the concept of terrorism. Its direct meaning has been largely contested by various schools of thought. Due to its ambiguity, the concept has been construed in several ways (Ibietan, Chidozie & Ujara, 2014:68). Wilkinson (2011:4) avers that, the use of the term terrorism has been equated with political violence by the mass media and politicians. However, the users of terrorism as a weapon, equate the act with freedom fighting, holy wars and revolutions (depending on the cause being fought for).

Instead of defining terrorism, Ajayi (2012:103) opts to describe terrorism by stating that the term 'terror' imprints an image of fear and trepidation with the intention of instilling submission in the victims. The position that posits that terrorist acts are usually unprovoked, random and unpredictable with the most common method of perpetration being bombing. In concluding his description he asserts that the core purpose of terrorism is to draw attention to, as well as gain sympathy for a cause. The perpetrators commonly fall into the category of either one or all of the following: religious fundamentalists, right/left extremists, governments and/or underground organizations. This description of terrorism is one that can be contended with however, being that terrorist acts are far from 'random.' It is in this light that Shuhghart (2005, in Ibietan et al, 2014:69-70) argued that terrorism possesses four distinct characteristics: violence for political effect; usually planned, calculated and systemic; unbound by established rules or codes of conduct for warfare; with the goal of having far reaching psychological consequences beyond the immediate victim/target.

A concise, yet apt definition of terrorism was identified by Enders & Sandler (2005:3) as the "premeditated use or threat to use violence by individuals or subnational groups in order to obtain a political or social objective throught the intimidation of a large audience beyond that of immediate victims." They further express that while terrorist attacks are not random, terrorists make them appear random in order to perpetrate anxiety among members of the public. Wilkinson (2011:4) conceptualises terrorism while making empirical distinctions between terrorism and other means of violence and conflict using the following characteristics:

- It is premeditated and designed to create a climate of extreme fear;
- It is directed at a wider target than the immediate victims;
- It inherently involves attacks on random or symbolic targets, including civilians;
- It is considered by the society in which it occurs as 'extra-normal', that is in the

literal sense that it violates the norms regulating disputes, protest and dissent; and
- It is used primarily, though not exclusively, to influence the political behaviour of governments, communities or specific social groups (Wilkinson, 2011:4).

Terrorism can be expressed as a veritable instance of collective violence. In effect, it is perpetrated by groups who believe in the use of such tactic as a means of advancing a group cause (Okoli & Iortyer, 2014:41). Okoli & Iortyer (2014) typify terrorist organizations into: rebel/militia groups; Islamic insurgents; political movements; government agents; and clandestine organizations.

Counter-terrorism

The concept of counter-terrorism is one that is easily misconstrued. Okoli & Iortyer (2014:48) express that, counter-terrorism "…presupposes combating terrorism through preventive and mitigative measures. This emphasizes the use of strategic intelligence, pragmatic policies and proactive strategies to counter the terrorists' designs in an attempt to forestall and/or mitigate terror." Pratt's (2010) definition of counter-terrorism is similar to Okoli & Iortyer (2014) where he conceptualizes that counter-terrorism measures involve actions/strategies targeted at the prevention of terrorism escalation, control of damage from terrorist attacks that occur, with the ultimate goal of eradicating terrorism within a given context. He also emphasizes that counter-terrorism measures are exclusively undertaken by government action.

Counter-terrorism also differs from counter-insurgency, and in some instances both concepts have been used interchangeably despite their different connotations. Pratt (2010) shares in this perception as he differentiates between counter-terrorism and counter-insurgency. In conceptualizing counter-insurgency, he argues that terrorism is usually a strategy engaged by insurgent groups, yet, they are not the same. He argues that counter-terrorism measures usually fit into the broader context of counter-insurgency which can be seen as a category of responses to political violence carried out by minority groups, both terror-based and otherwise.

Hughes (2011:14-15) expressed that counter-insurgency "involves the coordinated response of a state's government and its external supporters to integrate political, socioeconomic, legal, police, and military measures to frustrate and ultimately defeat an insurgency. Within the framework of counter-insurgency lies counter-terrorism which "…includes defensive measures to minimize the ability of a terrorist/insurgent group to inflict violence against the civilian population…" (Hughes, 2011:15) He also acknowledges that counter-terrorism may also incorporate offensive measures directed at undermining terrorist groups and neutralizing their membership base. As such, it can be deduced that his position on counter-terrorism takes a defence-offense standpoint.

The rationale for engaging counter-terrorist measures according to McCulloch & Pickering (2009:630) is the prevention of harm by "pre-empting threats." The need to pre-empt terrorist

threats exists as a result of the casualities that follow terrorist attacks. If the response to terrorism remains reactive, the damages accrued may take a longer period than is required to pre-empt the threat in the first place. It is in the same vein that this paper argues that counter-terrorism as an approach to combating terrorism should be assessed and advanced from a pre-emptive standpoint in order to enagage effective control of the terror situations that occur. Thus, counter-terrorism consists largely of the pre-emptive measures taken to inhibit terror attacks from occuring, as well as control the effects of terror attacks that have already occurred through the use of tactical intelligence and rational policies in the control of terror-related threats.

Electronic Surveillance

This concept, like many others does not possess a universal meaning. It has been defined in various ways by governments, organizations, and individuals. Despite this, similarities exist among these definitions. The Ajazeera Investigative Unit (AIU) (2017) defined electronic surveillance as the process of monitoring and collecting "digital footprints left behind by people" through a variety of methods such as: CCTV monitoring, text message monitoring, sifting through internet browsing history and social media networks, secretly activating webcams or microphones to spy on people as the case may be. The AIU asserts that this kind of surveillance is mostly carried out by government departments and intelligence agencies for several purposes which may include criminal investigation or intelligence gathering.

The United Nations (2009) defines surveillance as the process of monitoring or collecting information about a person or group of persons through the use of technology. While the definition given by the United Nations (2009) is not targeted at electronic surveillance, the authors find the definition admissible because it includes the use of technology as a key variable. Banks (2016:514) conceptualizes electronic surveillance as the "interception of communication between two or more parties that can give insight into what is said, planned and anticipated by adversaries". The purpose of surveillance generally is usually for constructive monitoring that can enable the parties carrying out the surveillance either prevent an action or react to an action or set of actions. Similarly, Lyon (2003) describes surveillance as the trace and tracking of mundane activities for a plethora of purposes which is targeted at planning, prediction and prevention by classifying and assessing profile and risks. While he does not include the use of electronic or technology in his definition, he adds that, abstract data (inclusive of video, biometric, genetic as well as computerized administrative files) are manipulated in surveillance to produce profiles and risk categories in a liquid, networked system.

In the 21st century, the theaters of conflict, attacks as well as terrorism are shifting. The cyberspace is increasingly becoming a new avenue for such operations. As a result, in the process of intelligence gathering and surveillance, engaging the cyberspace is not an option (Podesta, 2015). The explosive growth of technological capabilities and the individuals with the ability to manipulate these capabilities to probe, prepare and perpetrate an attack or criminal act against a

geographically dispersed region from thousands of miles away, undermines traditional surveillance strategies (Liscouski, 2014). As a result, the authors recommend that the definition of electronic surveillance should be expanded to capture cyber activity. Electronic surveillance can therefore be conceptualized as the tracking and monitoring of behaviour and activities both offline and online by means of electronic, digital, audio-visual and online equipment for the purpose of planning, prediction, and prevention (as well as reaction, as the case may be).

SECURITIZING TERRORISM IN NIGERIA

Securitization theory seeks to provide answers to the following issues: what constitutes a security problem; what distinguishes security challenges from non-security challenges; the realization of threat images and; the debate on whether security and politics are compatible or mutually exclusive (Balzacq, 2011a). The core argument of the theory explains that, once a securitizing actor states that a particular referent object's existence is threatened, the securitizing actor can claim a right to engaging extraordinary measures to ensure the survival of the referent object (Taureck, 2006). In defining security therefore, the theory describes security as a 'speech act' that creates "a certain kind of social situation whereby issues are moved into a special category or politics where emergency rules apply – a 'securitization" (Corry, 2010:5).

There has been an identified process of securitization in order to avoid the possibility of confusion between security and non-security issues. It therefore consists of three chronological steps (with the end result being securitization) – identification of existential threat to a referent object (which may be a state or not); prescription of an action plan in response to the identified threat; and the movement of the issue into the realm of emergency-politics that sets aside the usual rules governing decision-making in a given society (Corry, 2010). It can be deduced from the prenominal arguments that, security is viewed through the lens of constructivist philosophy, such that, no issue is originally a hazard, and that security issues are subject to what key actors make of it.

In order to check the securitizing actor's (usually political elite) liberties in identifying what becomes a security threat, the theory proposes the importance of an audience (which may be the electorate) that is given the prerogative to decide on whether to accept or decline a given agenda. Thus, securitization cannot be imposed; and the purpose of gaining the permission of the audience is to justify the application of extraordinary measures as the case may be (Balzacq, 2011b; Šulovic, 2010). It has been argued that the success or failure of securitizing moves depend largely on the audience's receptiveness to the different arguments on what constitutes security threats, thus giving them the audience the (sometimes unnecessary) power to determine whether measures can be applied against these threats or not (Balzacq, 2011b:7).

One of the underlining values that presage the sovereignty or credibility of any government is its ability to secure/protect its boundary and citizens. Nigeria, has been under the seige of terrorist

attacks for a lengthy period. Drawing from the stance of securitzation theory in relation to the state of Nigeria, the presence and activities of the clandestine Boko Haram terrorist group has possed eminent threat to the country and the outcry from the people of Nigeria has become deafening. Boko Haram which translates to anti-western education, as a case in point, has some religion similarities with the Taliban and has been said to have emerged in the early 1990's as a fundametalist form of Islam. Its core base is centered in Maiduguri, the capital of Borno State in the north-eastern part of the country but has long spread its operational centers to various parts of the country (Walker, 2014). Countless attacks from Boko haram have been recorded and its first known attack can be traced back to the 2003 multiple police station attacks in Yobe and Niger states. Terrorist activities and uprising began to spread rapidly in 2009. According to CNN reports, there have been numerous kidnaps and raids by the terrorist group, some cases being the July 17-20, 2014 raid of Damboa town which killed 66 residents and displaced 15,000, holding villages for days and the tactic of abducting of females (CNN, 2017).

The Multinational Joint Military Task Force had been put up to curb the Islamic insurgency, while former President Goodluck Jonathan declared a 'state of emergency' in the north-eastern Nigeria following provoking attacks such as the assault on military barracks, detonating a bomb at a bus station in Kano, kidnap of a French family and the abduction of over 200 secondary school girls in Chibok, Borno State. Since the declaration of the 'state of emergency' in Adamawa, Yobe and Borno states, the civilian causalities and death toll has long tripled from 741 in 2009 to 2,265 in 2011 according to data gathered by the University of Sussex (Walker, 2014).

Boko Haram militants utilize explosive devices to target security forces, offices, markets, parks and worship centers. Having established that the activities of Boko Haram terrorist group pose eminent threat to the Nigeria's security and peace, the state government as the securitizing actor has through the use of military intelligence deployed dexterity in the combat of terrorism. There is growing international pressure on the Nigerian government over the activities of Boko Haram (Obi, 2017), the increasing spread of same into other countries and its likelihood to spill into more countries; especially after the abduction of the Chibok girls. The military efforts have been helpful in tackling the conventional attacks against the military but there is still a long way to go in returning peace and stability in the north-eastern states of the country. Alternative and supportive means should therefore be explored and deployed towards the tackling of terrorism in the country. Human Rights Watch and Amnesty International have both criticized the Nigerian military for their tactics. Amnesty stated that a number of people (about 600) were killed by the military after an attack on Maiduguri's Giwa barracks in March 2017 (Walker, 2014). The trade of lethal weapons to Nigeria is outlawed by UK law because of such concerns. Inferring from the securitization theory, the audience here being the Nigerian citizens (many internally displaced) and the international audience, are seemingly in agreement on the security threat posed by terrorism in the country and also in agreement that the measures and actions taken so far to combat

this identified threat has been grossly insufficient. As a result, there is need to adopt other measures in conjunction with existing ones.

THE LINK BETWEEN ELECTRONIC SURVEILLANCE AND COUNTER-TERRORISM

Surveillance is a key segment of intelligence operations adapted towards securing delicate offices or fighting terrorism or insurgency. Since the time human beings considered fringes and edges, either for the purpose of watching over his property or to protect the borders of his people, surveillance has been utilized as a part of some frame (Winkler, Ebnöther & Hansson, 2005). It is principally expected to secure the individual, his property or business and the state. Swift advances in science today guarantees that innovation contributes extensively to a more effective Surveillance (Flammini, Setola & Franceschetti, 2013). The domain of intelligence gathering has progressed significantly since the times of yore when Surveillance included singularly conveying scouts to investigate the route ahead or an enemy's location. New inventive strategies have been dynamically accessible. Prognostic approach otherwise known as pre-emptive intelligence and innovation started to be deployed for present day surveillance (Marrin, 2012). The need to secure air and sea boondocks notwithstanding territorial borders and sensitive offices has improved the significance of Surveillance. However, in Nigeria, this part of the intelligence gathering process is highly underutilized. Despite the fact that surveillance systems have been a consistent component of human social orders all through history yet they are continuously playing a more centralized role while switching to a more innovative character (Lyon, 2001). Such patterns are especially reflected in the policing and preventing actions in contemporary society. As Lyon (2003) notes, technological reactions to terrorist attacks or threats are progressively turning into the main port of call.

In the present day, when fast advances in communications and transport structures require brisk reactions, innovation plays a considerably more key part in surveillance. The rise of international terrorism has emphasized the requirement for 'passive', 'archival' and real-time dynamic surveillance. Passive surveillance incorporates all types of observation expected to routinely screen ordinary human action in sensitive or secured zones while Archival surveillance includes inbuilt recognition characteristics in electronic surveillance innovation that recognizes specific people and in addition, their being in a particular place at a particular time and stores this information. 'Real-time' or 'active' surveillance is the observing of an occasion or movement as it happens or unfurls. The data particularly should be immediately accessible to the authorities for suitable action. In every one of these areas, the role of technology is rising (Ranade, 2010).

Quick advances in science today guarantees that innovation contributes significantly to a more successful surveillance and assumes a more predictive role. It can transfer advance intelligence on unfriendly actions when it starts to approach the targeted audience. While human intelligence is essential and imperative, innovative improvements are also today a critical piece of surveillance. Observing of web, landline and mobile communications of suspected terrorists provides key

advance information on plans and recent developments (Casey, 2011). This monitoring is a piece of the surveillance as well. There are two main elements that drive surveillance: to diminish the danger of attacks from occurring and to decrease the effect of any attack on such occasions (Mottram, 2006). It is important to note that surveillance does not singularly claim or guarantee is made to dispose of the hazard and effect of terrorism. Despite the fact that this might be one corollary of creating counter terrorism procedures inside contemporary states.

A key component is procuring however much data and intelligence as could be expected, through open and disguised means (Richards & Pherson, 2010). Pre-occurrence surveillance mindfulness and routinely utilizing anti and counter-terror methods will significantly improve the probability of early location and in this manner auspicious cautioning of an arranged assault or activity against an individual, site, home, transport framework among others. Recognizing that pre-episode observation purchases time to survey danger levels and security courses of action and enables counter measures to be started to either wipe out or diminish the hazard to a lesser level (Wright & Kreissl, 2014). More information will put the intelligence and law enforcement agencies into a position to recognize potential suspects before they can launch an attack. Watching out for hundreds or even a huge number of people, distinguished as potential suspects, will forestall future terrorist assaults. Gathering data about violent extremists' gatherings will create intelligence about future terrorist assault (Kreissl, Norris, Krlic, Groves & Amicelle, 2014).

There is need for the establishment and checking of CCTV as a method for discouraging, raising cautions, and aiding post event investigation (Silke, 2010). For sure, this arrangement of surveillance advancements can be referred to as a vital element of concrete, target-solidifying, situational counter terrorist measures. Open street electronic surveillance (especially CCTV cameras) is progressively depended on and referred to as a key apparatus in handling both crimes and terrorist attacks in the general public. The objective for CCTV can be separated into four work streams: to prevent, hunt, protect and, plan. Each with a different purpose, the objective of avoid is to address the radicalisation of people; hunt is to find punishable people; the motivation behind protect is to enhance border security and decrease the vulnerability of national framework and plan is intended to guarantee that the results of a terrorist attack can be overseen (Graham, Brooks & Heery, 1996).

There have been cases of success in countering terrorism using electronic surveillance. Some of which include: the September 2009 planned attack by Osam Maher Husein Smadi a 19-year-old Jordanian who was caught trying to plant a bomb in a Dallas skyscraper. Initially recognized through FBI's observation of radical Islamist chat rooms, Smadi was detained and charged after FBI agents who were undercover acted like terrorists and gave Smadi a counterfeit bomb, which he later endeavoured to explode. Smadi was pronounced guilty and sentenced to 24 years in jail (Bensman, Meserve, Callebs & Frieden, 2009). Additionally, in February 2011 Khalid Ali-M Aldawsari, a Saudi national who was schooling in Lubbock, Texas, was caught by the FBI after

they noticed that he put in an order for a harmful chemical called phenol. Both the chemical merchant and the shipping agency were noticeably suspicious of the order, which could be utilized to produce an Improvised Explosive Device (IED), and notified the FBI and nearby police. Surveillance of Aldawsari's email provided a rundown of prospective targets including dams, atomic power plants, military base, and the Dallas home of former President George W. Bush among others. Since then he has been charged with an attempt to utilize a weapon of mass destruction (Shane, 2011). Moreover, in December 2010 Awais Younis, who is likewise known by the Sundullah "Sunny" Ghalzai, was caught by the FBI after a law enforcement official found a number of threats he had made against the Washington, D.C., metropolitan domain through the social media platform Facebook. He was indicted of conveying threats through interstate communication (Mickolus, 2014).

With the expansion in the dimension of the threats, innovation has found a bigger role for itself. Innovation in electronic surveillance limits the 'human' part in this manner, enhances the successful time-on-target, and reduces human elements like partiality, exhaustion, and the likes. It guarantees practically prompt and exact communication of issues by means of pictures or, data equally providing an extra wellspring of constant intelligence to the security forces, and catches irrefutable information and pictures for assessment.

CONCLUSION AND PROSPECTS FOR THE NIGERIAN STATE

The intricate and technical form of communication that Boko Haram insurgent group engage in has been proven complex its efficacy irrefutable. The intermittent release of electronic information from the sect like video releases from the famous sect leader Abubakar Skekau reinforce the fact that the organization relies heavily on electronic devices for communication and information. Electronic surveillance provides a worthy and technical alternative for the monitoring of information flow within the terrorist network. It has been alleged that, through malicious spyware and information theft, the terrorist network has earned the brand of "always being step ahead of the Nigerian military'' and this ought not to be so. Geographical location can be fairly tracked, inappropriate phone interactions can be easily investigated as an integral part of investigation and combat, through electronic surveillance.

While references can be made to several incidences where electronic surveillance has been instrumental to counter-terrorism, the strategy has not been fully utilized full scale by the Nigerian government. Engaging the use of surveillance cameras, wiretapping, bugging and other surveillance technique to monitor the activities of 'suspected' terrorists can assist in forestalling terrorist attacks. This paper does not argue however that, electronic surveillance is an exclusive counter-terrorism measure, it posits that electronic surveillance as a tool of intelligence gathering will serve as valid instruments for combating the terrorism menace plaguing the country. Suffice to say that, though the military has been strategic and instrumental in the fight against terrorism in Nigeria, electronic surveillance can aid their activities. It also has the potential to discover any

discrepancies within the intelligence agencies as well as the military that may have given cause to sabotage the war on terrorism efforts. The loss of lives of civilians during military invasions and combat of terrorism would be greatly minimized when electronic surveillance becomes an integral part of Nigeria's counter-terrorism strategy.

In stating that surveillance of what goes on offline is crucial, it is also expedient for Nigeria to adopt a pro-active stance to surveillance by monitoring the online space. In this regard, it is fundamental to tilt towards this approach to intelligence gathering as technology is evolving and most communications are leaving the offline to the cyber space. The Nigerian government in battling terrorism must adapt to this trend and employ tactical online surveillance as well as offline surveillance. Technology exclusively cannot guarantee security however, security would be an impossible accomplishment without the influence of technology. Technology, specifically through the use of electronic surveillance poses a potentially potent counter-terrorism strategy (in combination with other existing measures), as more and more terrorist operations are becoming dependent on ICT tools. As a result, once the securitized threat of terrorism has been smothered in Nigeria, the current fear that permeates both the domestic society and international society towards Nigeria will be doused and thus engender a positive international image as well as national development.

REFERENCES

Ajayi, A. (2012, July). 'Boko Haram' and Terrorism in Nigeria: Exploratory and Explanatory Notes. *Global Advanced Research Journal of History, Political Science and International Relations, 1*(5), 103-107.

Aljazeera Investigative Unit. (2017, April 10). *Spy Merchants: What is Electronic Surveillance?* Retrieved from Aljazeera: http://www.aljazeera.com/indepth/features/2017/04/spy-merchants-electronic-surveillance-170409100231959.html#One

Balzacq, T. (2011a). Preface. In T. Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve* (pp. xiii-xiv). London and New York: Routledge.

Balzacq, T. (2011b). A Theory of Securitization: Origins, Core Assumptions and Variants. In T. Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve* (pp. 1-30). London and New York: Routledge.

Banks, W. (2016). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Law Journal, 66*, 513-525.

Bensman, T., Meserve, J., Callebs, S. & Frieden, T. (2017). *Jordanian accused in Dallas bomb plot goes to court - CNN.com. Edition.cnn.com*. Retrieved 10 May 2017, from "http://edition.cnn.com/2009/CRIME/09/25/texas.terror.arrest/index.html" http://edition.cnn.com/2009/CRIME/09/25/texas.terror.arrest/index.html

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

CNN. (2017, May 9). *Boko Haram Fast Facts*. Retrieved from CNN Library: http://edition.cnn.com/2014/06/09/world/boko-haram-fast-facts/

Corry, O. (2010). *Securitization and 'Riskization': Two Grammars of Security*. Working Paper, 7th Pan-European International Relations Conference, Standing Group on International Relations, Stockholm.

Enders, W. & Sandler, T. (2005). *The Political Economy of Terrorism.* Cambridge: Cambridge University Press.

Flammini, F., Setola, R. & Franceschetti, G. (2013). *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*. Chapman and Hall/CRC.

Graham, S., Brooks, J. & Heery, D. (1996). Towns on the television: Closed circuit TV in British towns and cities. *Local Government Studies*, *22*(3), 1-27.

Hughes, G. (2011). *The Military's Role in Counterterrorism: Examples and Implications for Liberal Decmocracies.* Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Ibietan, J., Chidozie, F. & Ujara, E. (2014). International Terrorism and the Middle East: An Expository Approach. *Covenant University Journal of Politics and International Affairs CUJPIA, 2*(1), 66-80.

Joshua, S. & Chidozie, F. (2014). Terrorism in Nigeria. In R. Ajayi, & J. Fashagba, *Understanding Government and Politics in Nigeria* (pp. 347-362). Omu-Aran: Landmark University.

Kreissl, R., Norris, C., Krlic, M., Groves, L. & Amicelle, A. (2014). Preventing and Detecting Crime and Terrorism. *Surveillance in Europe*, 150-210. Washington, DC: Cq Press.

Liscouski, B. (2014, March 1). *Changing the Definition of Surveillance in the Age of Converged Risk*. Retrieved from Security: Solutions for Enabling and Assuring Business: http://www.securitymagazine.com/articles/85274-changing-the-definition-of-surveillance-in-the-age-of-converged-risk

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. New York: McGraw-Hill Education.

Lyon, D. (2003). Surveillance as Social Sorting: Computer Codes and Mobile Bodies. In D. Lyon, *Surveillance as Social Sorting: Privacy, Disk and Digital Discrimination* (pp. 13-30). London and New York: Routledge.

Majekodunmi, A. (2015). Terrorism and Counter-Terrorism in Contemporary Nigeria: Understanding the Emerging Trends. *Journal of Policy and Development Studies, 9*(4), 128-145.

Marrin, S. (2012). *Improving intelligence analysis: Bridging the gap between scholarship and practice*. London: Routledge.

Mickolus, E. (2014). *Terrorism, 2008-2012: A worldwide chronology*. California: McFarland.

Mottram, R. (2006, June). *CONTEST strategy and the key policy themes*. Paper presented at the Technology for Security and Resilience Conference, London.

Obi, W. (2017, May 17). *Stronger than Boko Haram*. Retrieved from Politics in Nigeria: https://politics.naij.com/1004807-stronger-than-boko-haram-new-terrorists-appear-in-nigeria-threatens-government.html

Okauru, A. (2013, July 18). *Information Communication Technology and National Security in Nigeria*. Retrieved from Punch Newspaper: http://www.punchng.com/business/ict-clinic/security-challenges-what-cam-ict-do

Okoli, A. & Iortyer, P. (2014). Terrorism and Humanitarian Crisis in Nigeria: Insights from Boko Haram Insurgency. *Global Journal of Human-Social Science: F Political Science, 14*(1), 39-50.

Okoro, E. (2014). Terrorism and Governance Crisis: The Boko Haram Experience in Nigeria. *African Journal on Conflict Resolution, 14*(2), 103-127.

Oludare, A., Omolara, O., Umar, A. & Kemi, D. (2015). The Use of ICT Tools in Tackling Insecurity and Terrorism Problem in Nigeria. *Network and Complex Systems, 5*(5), 21-40.

Omale, D. (2013). Terrorism and Counter-Terrorism in Nigeria: Theoretical Paradigms and Lessons for Public Policy. *Canadian Social Science, 9*(3), 96-103.

Podesta, D. (2015). *Watchdogs Under Watch: Media in the Age of Cyber Surveillance.* Washington, DC: Centre for International Media Assistance.

Pratt, S. (2010, December 21). *What is The Difference Between Counter-Insurgency and Counter-Terrorism?* Retrieved from E-INTERNATIONAL RELATIONS: http://www.e-ir.info/2010/12/21/what-is-the-difference-between-counter-insurgency-and-counter-terrorism/

Ranade, J. (2010). Surveillance in CounterTerrorism, CounterInsurgency and Warfare. *Claws Journal, Winter*, 46-54. Janczewski, L. (Ed.). (2007). *Cyber warfare and cyber terrorism*. IGI Global.

Richards, H. J. & Pherson, R. H. (2010). *Structured analytic techniques for intelligence analysis*.

Silke, A. (2010). *The psychology of counter-terrorism*. London: Routledge.

Šulovic, V. (2010). *Meaning of Security and Theory of Securitization.* Belgrade: Belgrade Centre for Security Policy.

Taureck, R. (2006). Securitisation Theory and Securitisation Studies. *Journal of International Relations and Development, 9*, 53-61. Retrieved from http://dx.doi.org/10.1057/palgrave.jird.1800072

FBI. (2011). *Texas Resident Arrested on Charge of Attempted Use of Weapon of Mass Destruction*. Retrieved 12 May 2017, from: https://archives.fbi.gov/archives/dallas/press-releases/2011/dl022411.htm

Uhrmacher, K. & Sheridan, B. (2016, April 3). *The Brutal toll of Boko Haram's Attacks on Civilians*. Retrieved from The Washington Post: https://www.washingtonpost.com/graphics/world/nigeria-boko-haram/

United Nations. (2009). *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime.*

Walker, A. (2014, May 14). *Why Nigeria Has Not Defeated Boko Haram.* Retrieved from BBC News: c.com/news/world-africa-27396702

Wilkinson, P. (2011). *Terrorism, Insurgency and Asymmetrical Conflict: Introduction to the Concept of Terrorism.* London and New York: Routledge.

Winkler, T., Winkler, T. H., Ebnöther, A. H. & Hansson, M. B. (Eds.). (2005). *Combating Terrorism and Its Implications for the Security Sector*. DCAF.

Wright, D. & Kreissl, R. (2014). *Surveillance in Europe*. London: Routledge.