Electronic Governance and National Security in Nigeria

Michael I. Ugwueze

Department of Political Science, University of Nigeria, Nsukka
michael.ugwueze@unn.edu.ng

Jonah Onuoha

Professor of Political Science, University of Nigeria, Nsukka

Ejikeme J. Nwagwu

Department of Political Science, University of Nigeria, Nsukka

Doi:10.5901/mjss.2016.v7n6p363

Abstract

Electronic Governance has become an important tool for arresting the continued sophistication of the 21st Century security administration. This explains why virtually all countries of the world are keying into the programme to help curb the difficulties arising from the digitalization and internationalization of violent crimes. The use of Information and Communication Technologies (ICTs) has therefore become increasingly indispensable especially as it minimizes cost while encouraging efficiency and effectiveness in service delivery. However, while a lot of achievements have been recorded in other sectors of the Nigerian economy through the adoption of e-governance, its result in the security sector remains in doubt as the insecurity situation in the country especially in the north continues to deteriorate despite the application of ICTs in security administration. The study aims to know why the utilization of ICTs in security administration has not enhanced the protection of lives and property in Nigeria especially in the north. The work is a documentary research that utilized qualitative methodologies in collecting and analyzing data. Consequent upon this, the paper discovered that the use of ICTs in security administration has not enhanced the protection of lives and property in Nigeria because even the available security gadgets are grossly under-exploited and sabotaged. The study therefore concluded that until the Nigerian government begins to adequately exploit e-governance through installation, utilization and maintenance of ICT gadgets in the management of national security, the insecurity situation will persist.

Keywords: *e-governance, national security, ICT, Nigeria*

1. Introduction

The primary responsibility of any government is the protection of lives and property of its citizens and Nigeria, like many other countries, is seriously faced with the challenges of meeting this primary objective. The security situation in the country especially in the north has continued to worsen and all attempts made to remedy the situation have proven abortive. As noted by Thomas-Greenfield (2014), the security situation in Nigeria is steadily worsening, deeply disturbing and increasingly dangerous with each passing day. Despite the worsening situation of security, the Nigerian government has not rested on its oars in search of solutions. Indeed, the latest quest for solution to security problems in Nigeria especially in the northern part of the country has been the increased utilization of electronic governance (e-governance) in security administration. E-governance, according to some scholars, is the public sector's use of Information and Communication Technologies (ICTs) aimed at improving information and service delivery, encouraging citizens participation in the decision-making process as well as making government more accountable, transparent, efficient and result-oriented (Ingawa, 2011; Akunyili, 2010; Mohammed *et al*, 2010 and Danfulani, 2013).

Interestingly, e-governance has been identified as the panacea for reducing corruption in governance, making government more accountable, transparent and efficient as well as reducing the red-tapism characteristic of public administration, and encouraging citizens participation in decision making process (Babalola, 2013; Oye, 2013; Sharma, 2005; Fatile, 2012; among others). However, in Nigeria like many other African countries, decades of military dictatorship and political instability had stifled all initiatives for technological innovations because the military rulers saw information and communication technology as a security threat rather than a national opportunity (Ajayi, 2003 cited in Babalola,

2013). Hence, the ICT policy was not operational until the return to democracy in 1999. Accordingly, since 1999 till date, the use of ICT in governance is increasingly gaining the required ground for effective administration especially in managing movement of files, recruitment exercises as well as in the areas of national security through launching of satellites into space, Subscriber Identification Module (SIM) registration, installation of close circuit television (CCTV) cameras at designated places, among others. But the critical question still remains, why has the utilization of ICTs in security administration not enhanced the protection of lives and property in Nigeria? While scholars have been contributing on how e-governance has improved productivity in Nigerian public administration, through reduction of corruption and red-tapism as well as encourage citizens participation in decision-making process (Sharma, 2005; Ingawa, 2011 and Oye, 2013), they appear to have glossed over the utilization of e-governance in the management of national security in Nigeria.

Consequent upon this, the work examined why the utilization of ICTs in security administration not enhanced the protection of lives and property in Nigeria especially in the north despite all the technological efforts made.

2. Materials and Methods

The materials for the study were gleaned from secondary source of data like journal articles, government publications, official documents, books and so on. Being a qualitative research, the study relied on documentary method of data collection. The choice of this method is not unconnected to the following advantages it offers:

- It allows the researcher access to subjects that may be difficult or impossible to obtain through direct personal contact, because they pertain either to the past or to phenomena that are geographically distant.
- The use of data gleaned from archival sources is usually important because raw data are often non-reactive. In other words, those writing and preserving the records are in most cases unaware of any future research goal or hypothesis or, for that matter, that the fruits of their labour will be used for research purposes at all. However, record keeping is not always completely non-reactive. Record keepers are less likely to create and preserve records that are embarrassing to them, their friends, or their bosses; that reveal illegal or immoral actions; or that disclose stupidity, greed or other demeaning attributes; or even in some cases, that have security implications.
- Documentary method offers the access to records that have existed long enough to permit analyses of political phenomena over time.
- Another advantage is that, using a written record often enables the researcher to increase sample size above what would be possible through either interviews, questionnaires or other forms of direct observation.
- Lastly but most importantly, documentary method of data collection often saves the researcher considerable time and resources, it is usually quicker to consult printed government documents, reference materials, computerized data, and research institute reports than it is to accumulate data ourselves through the survey methods (Johnson and Joslyn, 1995).

Because security studies are often shrouded in secrecy, obtaining first hand information from security agents or other stakeholders within the security administration is usually very difficult because they are often skeptical and economical with facts that could guarantee lucid scientific conclusion if one should rely on their information. Meanwhile, documentary method offers the research a wide range of opportunities that other methodologies may not guarantee.

In running the analysis, the study adopted qualitative descriptive method. This method is noted for the following advantages:

- The method is holistic and multi-dimensional
- It is characteristically descriptive.
- It deals with the real world
- It is essentially dialectical and interactive
- It is not aimed at statistical test (and interpretation) of hypothesis (Biereenu-Nnabugwu, 2006: 373-374).

Nevertheless, qualitative descriptive method of data analysis involves rigorous thinking, sufficient evidence and alternative considerations based on a sequential and logical analytic order. Where necessary, tables and figures were adopted for proper clarity of data presentation.

3. Discussion of the Use of ICT in Security Administration in Nigeria

The concept of national security (security for short) have acquired a mystique, and so to many, it has become mystical, mythical and even mysterious (Nnoli, 2006). In fact, issues bothering on security are often shrouded in secrecy, and

civilians, in most cases, are exempted from prompt security information that could guarantee effective civilian oversight of even the military establishments. This makes civilian control of the military almost impossible and generally undermines the improvement of information and intelligence available to the public as the basis for effective monitoring and expertise in military, defense and other security issues (Nnoli, 2006).

Wolfers (1962) noted that although it may be an overstatement to claim that the concept of national security is nothing but a recipe for semantic confusion, when used without specifications, may leave room for more confusion than sound political counsel or scientific usage can afford. Arising from the above, Nnoli (2006) noted that, it is not surprising that national security in the contemporary time is counter-posed to human security, environmental security, economic and social security, and the security of the ethnic group. In the resultant anarchy of perspectives that prevails, individuals, rebel movements, ethnic groups, political parties and even pressure groups implement disparate security measures. He further noted that:

National security is a cherished value associated with the physical safety of individuals, groups or nation-states, together with a similar safety of their most cherished values. It denotes freedom from threats, anxiety or danger. Therefore, security in an objective sense can be measured by the absence of threat, anxiety or danger. However, and more importantly, security has subjective sense, which can be measured by the absence of fear that threats, anxiety or danger will materialize. In order words, it is a value associated with confidence in physical safety and other most cherished values (Nnoli, 2006: 16).

The foregoing citation lays credence to the two prevailing theories of national security – the objective and subjective theories – which in effect are insufficient when treated in isolation. This is because the objective theory entails absence of threat, anxiety or danger which does not mean that they cannot occur in the shortest future. On the other hand, subjective theory of national security measures security in terms of the absence of fear that threats, anxiety or danger will materialize. Even though no matter how much security there is in the objective sense, unless there is confidence that it exists, there is no security, and because immediate safety is an indispensable factor, we cannot take subjective security as wholesome. Ugwueze (2014: 342) is of the opinion that national security can be seen "as the existence of physical safety either of economic well-being or military might, as well as the conviction that upon the existence of social vices whether hunger, poverty, unemployment and crime, the state would be readily available to repel them within the shortest possible timeframe". However, in the context of this study, challenges of national security involve anything that is a threat to the protection of lives and property in Nigeria, especially in the Northern part of the country.

On e-governance and national security, Tomov and Balabanov (2012) conducted a study on the methodology for the information security management and e-government environment and thus, observed that the biggest threat to the government data in the 21st century which hampers smooth administrative process is human error which e-governance has the capacity to address. In line with the foregoing, Alshboul (2012: 215) noted that:

All the world now acknowledges the strategic importance of e-government. Generally, it is a portal – or more – that provides citizens and business with public information, governmental forms to be downloaded, and means to communicate with governmental representatives. E-government main goals and plans are to provide efficiency and full access for services, which consequently increases transparency and higher quality of public government services. That is why there is an increased concern about the security and integrity of e-government applications and websites, the trend now is to provide more secure, reliable services to customers via these applications. Citizens expect high quality services, full access to information with the most possible security that can be offered.

Alshboul (2012) looked at two critical issues in e-governance which are security and vulnerability. He therefore identified certain factors that lead to vulnerability as follows: technical and technology factors, human factors, social factors, political factors; economic and networking factors. Technologically, he noted that:

There are numerous ways that technology offers as security tools, like demanding a username and password for entering a user to his PC for important files or for the entire system, another tool is downloading antivirus programs in order to protect computers, being careful when receiving e-mails from unknown sources, thus look for the e-mail source, security levels increase if the computer is connected to a company or a department which involves classified and important files and information, they may use firewalls. Security file system (SFS) or encryption and decryption tools are methods designed to span the internet and use for example in a facility that has a system of sending and receiving electronic messages (Alshboul, 2012: 216-217).

Indeed, Alshboul's study was more of how to protect the ICT gadgets used in e-governance rather than how e-governance has been exploited to provide security of lives and property.

Similar studies also revealed the security implications of e-governance initiatives. Gupta and Gupta (2012: 97) observed that:

Nowadays, most of financial and non-financial activities are done with computer and computer related services

such as internet. The rapid development of internet and computer technology globally has led to the growth of new forms of transnational crimes especially internet related. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crimes. The use of e-governance the confidential document of government departments and organization is processed and stored which can be hacked using computer.

While Gupta and Gupta (2012) identified the security implications of e-governance which border on computer or ICT related crimes, as well as the necessary cyber law-making to regulate the crimes, the study did not explain how e-governance through the use of ICT has helped in the protection of lives and property. In like manner, Agrawal *et al* (n.d.: 68) opined that:

The e-governance application needs to build the trust of citizens (to enhance citizens to government participation) in the system. It needs to ensure that the data and transactions of the citizen are secured. The information shared by the citizens should also remain safe and the privacy of the citizen needs to be protected.

They further listed the various security concerns that may be there for an e-government system as follows: client threats, active content, malicious codes, communication channel threats, confidentiality threats, integrity threats, availability, server, web server, database and common gateway interface threats, as well as password hacking. These are all security challenges posed by e-governance initiatives. They therefore identified eight security areas for e-governance. These include:

- Dependency on information systems
- High degree of information sharing
- Increase use of remote access
- Challenges of controlling information
- Laws relating to information security
- Dealing with highly sensitive citizen's and business data
- National security and
- Consequences of security breach can be detrimental.

In fact, the scholars did not examine these areas beyond listing them, and so, did not look at e-governance as a necessary tool embodying adequate strategies for fighting crimes; instead, they see it as an embodiment of security threats itself that needs to be secured. According to them:

More than most IT systems, e-governance applications need to be secured. Technology has proliferated in all spheres of life. Accompanied by the rapid growth of the internet, there has been a concomitant rise in online transactions. The government sector has been no exception to these facts and it has wholeheartedly embraced IT in general and internet-based technologies in particular, of late, in order to extend the benefits of governance to all citizens – urban and rural – through a slew of e-governance projects. As computer systems have become more user-friendly and easy to access, their adoption has grown phenomenally. As a result, we have a scenario wherein multiple operating systems and infrastructure components co-exist. This has increased the potential for security threats (Agrawal *et al*. n.d: 70).

The increasing security threat of e-governance has continually endeared scholars to writing about the security implications to national development rather than its security advantages. As Agrawal *et al* (n.d.: 70) further noted:

Data cannot be confined to one place; the importance of data lies in sharing it. When you share your data, it spreads across several devices including PCs, laptops, data center servers, mobile phones etc. you need to secure the end-point. Rather than securing the environment, greater emphasis should be given to securing the information that is flowing across several networks.

The scholars equally observed that, the aim of attacks is changing from preserving oneself and wiping out the enemy to preserving oneself and controlling the opponent. In that case, a full-fledged cyber attack, which is one of the security implications of e-governance, involves gaining control over networks and there are four steps in it. These include:

- Gain control over network of government and defense establishments
- Bring down the financial systems: the stock markets and banks
- Take control of a nation's utilities (power, telecom, etc)
- Take control over personal identities (passport data, driving license/PAN No, ration cards) (Agrawal *et al* n.d.: 70).

The views of Agrawal *et al* (n.d.) can be summarized as follows:

- Information technology (IT) has a vital role to play in all transactions undertaken by the government
- It helps government cut red tapism, avoid corruption, and reach citizens directly.
- The initiatives help citizens learn about the various policies that government offers and so is part and parcel of good governance and SMART government which embodies the tools necessary for achieving efficiency and

effectiveness, transparency, accountability, and user-friendliness in all the transactions that the citizens and businesses conduct with government.

- Much of e-governance security involves risk management which includes confidentiality, integrity, availability and compliance.

Furthermore, Hwang *et al* (2004: 9) noted that:

> *The time for the electronic-based society has arrived. E-government has received more and more importance and it can provide a non-stop government information services to citizens, enterprises, public officers, government administrations and agencies over a network. There are many issues in e-government which need a careful examination such as security issues.*

What Hwang *et al* (2004) considered in the security issues include the security challenges of e-government. These challenges were demonstrated from four aspects of technical, political, cultural and legal. The scholars noted that, technically, in order to introduce and promote e-government, the first and very important step is to construct the relevant IT infrastructure and that system and security requirements, such as integrity, secure payment mechanism, and promotion of security mechanism are pertinent to e-government as well. Politically, rich variety of different services (example, e-justice) will be more acceptable and convenient for users. Also, process standardization has to be kept and agreements of reparations, authority and responsibilities have to be clearly formulated and recognized in order to protect the users' right. From the cultural perspective, the challenges and obstacles in e-government has a lot of difficulty because it involves the human psychological factor. The principle of "easy-to-use" should be encouraged because it has a great influence on the success of e-government given that it could advertize and promote e-government and allow more people to use the e-government services. Finally, another challenge noted by the scholars is the legal impact. This aspect embraces a lot of problems related to networking crimes and security threats, such as hacker attacks, viruses, masquerades of unauthorized identity, and computer forgery, and that there is a shortage of relevant law in information technology. However, while this study revealed the security challenges confronting e-governance, it failed to highlight how e-governance can enhance or has enhanced the protection of lives and property.

Mohammed-Nasiru and Kasimu (2012: 2) equally observed that:

> *The emergence of new Information and Communication Technologies (ICTs) has revolutionized every aspect of human endeavour. In today's world of insecurity of lives and property, there is need to fathom ways on how to bring about harmony and peaceful co-existence between individuals on one hand and among nations on the other.*

These scholars therefore opined that, it is imperative for security personnel as well as other stakeholders to be armed with proper and efficient tools to respond to ever changing and unpredictable situations they encounter in performing their duties. Considering contemporary developments in the technological world, Mohammed-Nasiru and Kasimu (2012) also noted that, surveillance serves as a valuable and essential tool for information gathering in combating criminal activities and security management. However, these scholars did not delve into how far Nigeria has exploited these ICT gadgets to enhance security of lives and property.

Other studies on e-governance especially in Nigeria revolve around its achievement in national development through the reduction of corruption and red-tapism; among others. According to Johnson (2013), e-governance through the adoption of Integrated Personnel and Payroll Information System (IPPIS) has discovered about 46,000 "ghost workers" and saved the government approximately N119 billion so far. She further noted that, "215 MDAs have been captured onto the IPPIS system and another 321 intended to be added by year end with more savings expected" (Johnson, 2013: 5). Similar to Johnson's observation, Oye (2013: 8) noted that:

> *ICT has had a tremendous impact on our lives. We can do almost nothing without ICT today. The ICT industry over the past decades has led to tremendous changes and progress in economic and social development around the world and has opened up greater opportunities for even faster growth and change than has already occurred. ICT has helped improve efficiency in many sectors and increased the volume and quantity of outputs in almost all sectors, from industry to manufacturing, construction to banking, finance, health, education, development assistance and government services.*

He also maintained that:

> *ICT can through e-governance system support the fight against corruption by raising accountability through digital footprints, raise transparency by publicizing regulation and fees, and reduce face-to-face interaction where most request*

for bribes take place. ICT such as mobile phone, effectively empower citizens by allowing people to collaboratively gather and share evidence of corrupt practices (Oye, 2013: 9).

According to Akunyili (2010), a common feature of e-government is the automation or computerization of existing paper-based procedures to enhance access to and delivery of government services to the citizens. This helps to strengthen government's drive towards effective governance and increased transparency for better management of resources, for growth and development, as well as the integration of government ministries, departments and agencies in a manner that promotes their online interactions. She also noted that Information and Communication Technology is an umbrella term that covers all technical means for processing and communicating information, and that, it is the convergence of Information Technology (IT) and telecom technology that gave birth to ICT which finds expression in digital technology and all it is uses and variants, including the computer, the internet, mobile telephony, the different electronic applications like e-banking, e-governance, e-commerce, among others as well as digital media and broadband technology (Akunyili, 2010). Nevertheless, how these Information and Communication Technologies have been exploited in the protection of lives and property is yet to be studied well enough.

As observed by Babalola (2013), the aim of e-governance was to take advantage of ICT such as the VSAT and fiber optic networks to enhance access to quality education, eradicate poverty, create jobs and investment opportunities and enhance the nation's capacity to compete globally. In line with the stated objectives, the federal government approved the National Policy for Information Technologies in 2001. He further noted that, "Nigeria has made remarkable efforts towards developing an information infrastructure through which the nation can be mainstreamed into the information society" (Babalola, 2013, p.13). He further discovered that these efforts have started yielding dividends in the areas of human capacity development, ICT diffusion and universal access to information. However, whether these have been adequately exploited in the area of security remains a problem which the study did not capture.

Moreso, Olubamise (2013) opined that e-government is very imperative for policy makers in nation-building. Accordingly, he noted that:

E-government investments are needed to improve governance and deliver services to the people whose increasing sophistication like customers in the private sector now demand increasing efficiency from government. Government needs to embrace the potential improvements offered by emerging technologies, that are transforming the ways in which we access information and services. E-governance demands a close collaboration between government, private sector and civil society, built around a shared vision, with appropriate tools to deliver efficient and effective governance in the 21st Century (Olubamise, 2013: 2).

This increasing sophistication demands that the citizens adequately participate in government business. Mohammed et al (2010: 16) held the view that:

There are advantages while implementing an electronic government, at the same time, the advantages out weights the disadvantages of e-governance because of the following reasons: e-government will improve the efficiency of the current system, which would in return save money and time. The introduction would also facilitate better communications between governments and businesses… In addition, moving away from a heavily paper-based system to an electronic system would reduce the need for man power…The society is moving toward the mobile connections. The ability of an e-government service to be accessible to citizens irrespective of location throughout the country brings the next and potentially biggest benefits of an e-government service.

Nevertheless, the level of mobile connections in Nigeria exemplified in the degree of teledensity in the country since 2002 vis-à-vis the application of such connection in securing lives and property of both Nigerians and foreigners residing in Nigeria is yet to be given serious examination. However, the result shows that Nigeria has made the following efforts in terms of applying ICT in security administration:

- SIM card registration
- Launching of satellite into the space
- Installation of CCTV cameras in Nigeria and
- Increase in teledensity

4. Discussion

Every individual, group of individuals, entrepreneurs, organizations, ministries, agencies, churches, mosques, homes, hospitals, relaxation centers, shopping malls, local, state and federal governments need Information and Communication Technology (ICT) for their security activities, operations, business purposes, among others (Shoyombo, 2014). As noted

by Awe (N.D):

Optimum security requires the technology platform. And it isn't just about acquiring technology and new tools. There must be deep understanding of the issues at stake. Change of apparel from analogue to digital won't be enough. A dinosaur with a laptop is still a dinosaur. Mindsets must change. New thinking is needed to support and enhance security. It is about using digital inputs in a meaningful and effective manner to handle threats and outsmart the attackers.

Technology is proactive in security sense and that is why it cannot be waved in the contemporary time when both development and crime have gone digital. No digital crime (crime carried out using sophisticated signals) can be solved using analogue security system in the 21st Century. This is why ICT is absolutely indispensable in governance for security purposes. Nigeria has continued to improve in the e-governance ranking of the United Nations; moving from 162 to 141 out of the 193 member countries of the United Nations in the 2014 e-governance ranking.

There are three components used in assessing the performance of states in the e-governance survey. These include: Online Service Index (OSI), Telecommunication Service Index (TSI) and Human Capital Index (HCI). Notwithstanding that Nigeria is still in the middle of the ranking, the country has grown substantially in two of the three variables used in measuring the e-governance initiative. In terms of online service delivery and telecommunication infrastructure, Nigeria has done a relative good job. Virtually all government Ministries, Departments and Agencies have integrated-online presence thereby offering online services, and telecommunication infrastructure has grown exponentially since the privatization of the telecom industry in 2002. However, it is only in the area of human capital development that Nigeria has not done so well. Let us therefore examine how the use of ICTs in security administration has impacted on the protection of lives and property in Nigeria especially in the north using the combinations of the variables of the result:

- SIM registration and arrest of criminals
- Launching of Satellites into Space, Installation of CCTV Cameras and Prevention of Attacks at Public and Private Places in Northern Nigeria and
- Increase in Teledensity, Free Flow of Information and the Rescue of Kidnapped Victims in the Northern Parts of Nigeria.

4.1 SIM Registration and Arrest of Criminals

Before 2010, suicide bombing and full-scale terrorism were novelties in Nigeria. Though Nigeria was used to armed robberies, ritual killings, political assassinations, among other heinous crimes, suicide bombing was never in the list. However, given the emergence of full-scale terrorism especially of the Boko Haram in 2010 and the attendant suicide bombings that accompanied it, Nigeria had no option than to find lasting solutions to the problems. One of such solutions was the option of Subscriber Identification Module (SIM) registration which was to elicit data of all Nigerians and probably trace their phone calls especially when used to perpetuate crime(s). SIM registration has four critical objectives. These include:

- To assist security agencies in resolving crimes and by extension to enhance the security of the state.
- To facilitate the collation of data by the Nigerian Communication Commission (NCC) about phone usage in Nigeria.
- To enable mobile phone operators to have a predictable profile about the users in their networks and
- To enable the commission to effectively implement other value added services like Number Portability among others (http://www.ncc.gov.ng/index.php?).

In fact, the thrust of the exercise lies with the first objective of assisting the security agencies in the fight against crimes. The registration which started on May 2010 lasted till September 28, 2011 for the old lines while the registration of new lines remain an ongoing process to be carried out by the concerned mobile operators. At the end of the exercise, over 120 millions SIM cards belonging to over ninety million people resident in Nigeria were registered (http://www.ncc.gov.ng).

However, since the end of SIM registration in 2011, it has not been easy arresting Boko Haram sect members, especially their commanders, through the trace of phone calls. Yet, the sect members, especially their commanders, have continued to communicate amongst themselves while dishing out instructions to their foot soldiers and not even the SIM registration appears to have helped out in tracing their whereabouts. While the leadership structure has remained intact with traces of succession on the fall of a commander, their attacks have continued to grow wild. See figure 1 for summary information of the security situation in Nigeria especially as it affects Boko Haram attacks in the North-East.

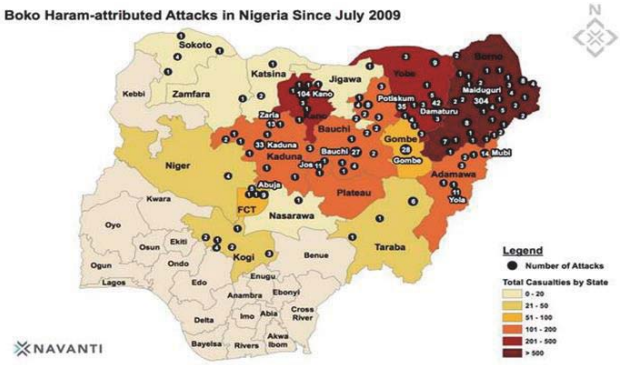

Figure 1: Graphic representation of the security situation in Nigeria especially in the wake of Boko Haram insurgency
Source: http://www.trackingterrorism.org/group/boko-haram

Apart from kidnapping people (the height of which was the kidnap of over 200 school girls in Chibok), Boko Haram sect has continued to kill, maim and displace thousands of people from their homes. Nigerians have lost count of the number of deaths in the Northern part of Nigeria due to the daily blood-shed between the sect members and the Nigerian military. Indeed, representing the number of deaths in a table has become increasingly difficult due to the incessant occurrence of the attacks; hence both figures 1 and 2 show graphic representations of the deaths carried out by the sect members as well as the territories that have fell under their control.

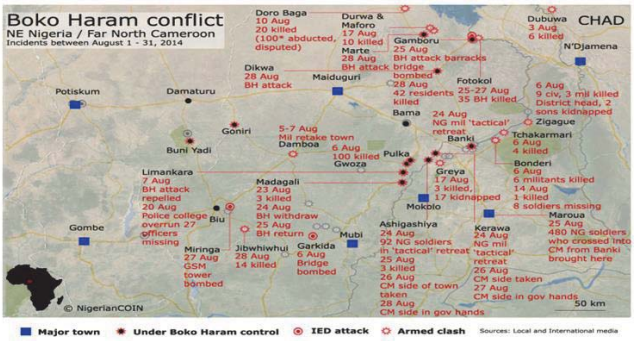

Figure 2: Graphic representation of Boko Haram attacks in the North-East, Nigeria
Source: http://www.trackingterrorism.org/group/boko-haram

The killing of the insurgents, including a rumoured killing of the sect's leader Abubakar Shekau, by the military has not produced the desired result. Arresting the insurgents, especially their commanders, will yield more results than killing them. In fact, the killing of the founder of the sect Mohammed Yusuf in 2009 has produced more calamity than success. It is not surprising that the arrest of some of the sect leaders in the North-West like Kabiru Sokoto and Sadiq Ogwuche (the masterminds of the bombings in St Theresa's Catholic church, Suleja and Nyanya motor pack in Abuja respectively) has led to relative reduction in the number of attacks in the zone especially in Abuja, the Federal Capital Territory as well as Sokoto and Niger states.

4.2 Launching of Satellites into Space, Installation of CCTV Cameras and Prevention of Attacks at Public and Private Places in Northern Nigeria

Nigeria since 2003 has launched five satellites into the outer space. The NigeriaSat-1 was the first Nigerian satellite which was built by a United Kingdom-based satellite technology company called Surrey Space Technology Limited

(SSTL) under the Nigerian government sponsorship for $30 million. This satellite was launched on 27th September 2003 by Kosmos-3M rocket from Russian Plesetsk Spaceport as part of the world-wide Disaster Monitoring Constellation (DMC) system. Its primary objectives, among others, include:

- To give early warning signals of environmental disaster
- To help detect and control desertification in the Northern part of Nigeria
- To assist in demographic planning
- To provide technology needed to bring education to all part of the country through distant learning and
- To aid in conflict resolution as well as border disputes by mapping out state and international borders.

The second and first communication satellite in Nigeria, the NigComSat-1, was ordered and built in China in 2004. This was Africa's first communication satellite which was launched on 13th May 2007 aboard a Chinese Long March 3B carrier rocket from the Xichang satellite launch center in China. This satellite eventually failed on 11th November 2008 after running out of power due to an anomaly in its solar array and was subsequently switched off to avoid collision with other satellites.

The third and fourth satellites, NigeriaSat-2 and NigeriaSat-X respectively, were built as a high resolution earth satellite by SSTL for DMC system also. Each of these satellites has 2.5-meter resolution panchromatic (very high resolution), 5-meter multispectral {high resolution Near Infrared (NIR) red, green and red bands}, and 32-meter multispectral (medium resolution, NIR red, green and red bands) antennas. The spacecrafts were built at a cost of over 35 million Pounds and subsequently launched into orbit by Ukrainian Dnepr rocket from a Yasny military base in Russia on 17th August, 2011 (Wikipedia the free encyclopedia, 2014). On 24th March 2009, the Federal Ministry of Science and Technology, NigComSat Ltd and CGWIC signed a further contract for the in-orbit delivery of the NigComSat-1R satellite and on 19th December 2011, the fifth satellite NigComSat-1R was launched into orbit by China in Xichang. This satellite, according to President Goodluck Jonathan, would have a positive impact on national development in various sectors such as communications, internet services, health, agriculture, environmental protection and national security.

Similarly, President Jonathan also on assumption of office in 2010 and the increasing insecurity situation in the country organized series of meetings with security experts within and outside Nigeria to fashion ways of solving the security challenges. A decision was therefore reached to install Close Circuit Television (CCTV) cameras in Nigeria. Lagos and Abuja were selected to host the pilot projects aimed at closely monitoring and uncovering possible threats to public security through the CCTV cameras (Okafor, 2013). Against this backdrop, the federal government on 27th August 2010 signed an agreement with a Chinese telecommunication firm, ZTE to install about 2000 solar powered CCTV within the Federal Capital Territory, Abuja and its commercial hub, Lagos at the rate of $470 million. 15 percent of the amount ($70.5 million) would be paid by Nigeria and the remaining 85 percent ($399.5 million) to be provided by the Chinese Exim Bank. The loan would be repaid over time on three percent interest rate within 10 years.

Equally, NigComSat was also expected to utilize the National Public Security Communication System (NPSCS) platform within which CCTV project was embedded to provide quality broadband internet connectivity across Nigeria and at the same time generating Virtual Private Network (VPN) which provides security through tunneling protocols and security procedures such as encryption for both public and private institutions. So far, the pictures below represent some of the installed CCTV cameras in Abuja which according to many remain insufficient even with the huge sum budgeted for it as well as the satellites. The insufficiency of CCTV cameras has prompted the police to mandate all big business establishments like shopping malls to install CCTV cameras within their premises or face sanctions. Indeed, from dysfunctional systems and components to broken units occasioned by explosion from installed batteries of the CCTV cameras at an intercession between the Kashim Ibrahim Way and Aminu Kano Crescent in Wuse 2, as well as incomplete units at various places in Abuja, the CCTV project appears to have added nothing to Nigeria's security outfit. Inability to effectively secure lives and property (as exemplified in some of the attacks) is a testimony to the observation that the installation and utilization of the ICT gadgets are not only insufficient but that even the available ones are yet to be adequately exploited. Remember, the efforts made to elicit information on the whereabouts of Chibok girls from the NigComSat-1R also proved abortive as there was neither voice nor video record of the kidnap.

4.3 Increase in Teledensity, Free Flow of Information and the Rescue of Kidnapped Victims in the Northern Parts of Nigeria.

Teledensity refers to the degree of concentration of communication gadgets like the use of telephony; and according to NCC, this is calculated using the population distribution. Between 2002 and 2005, teledensity was calculated based on population estimate of 126 million. In 2006, it was done using population estimate of 140 million. The percentage of

teledensity from 2002 to 2006 was 1.89, 3.35, 8.5, 16.27 and 24.18 respectively (http://www.ncc.gov.ng). Nonetheless, from 2007, the calculation was based active subscribers. See the table below.

Table 4: Level of teledensity in Nigeria between 2007 and 2014

	Year	2014	2013	2012	2011	2010	2009	2008	2007
Connected lines	Mobile (GSM)	165,716,078	159,758,538	135,253,599	109,822,964	96,684,272	N/A	N/A	N/A
	Mobile (CDMA)	3,974,106	7,684,026	14,041,464	12,687,645	12,132,584	N/A	N/A	N/A
	Fixed wired/ Wireless	342,696	2,233,981	2,419,587	2,290,409	2,736,373	N/A	N/A	N/A
	Total	**170,032,880**	**169,676,545**	**151,714,650**	**124,801,018**	**111,517,229**	**N/A**	**N/A**	**N/A**
Active lines	Mobile (GSM)	128,536,850	124,841,315	109,829,223	90,566,238	81,195,684	65,533,875	59,935,985	40,011,296
	Mobile (CDMA)	2,061,458	2,404,777	2,948,562	4,601,070	6,102,105	7,565,435	6,052,507	384,315
	Fixed wired/ Wireless	182,395	360,537	418,166	719,406	1,050,237	1,418,954	1,303,625	1,579,664
	Total	**130,780,703**	**127,606,629**	**113,195,951**	**95,886,714**	**88,348,026**	**74,518,264**	**64,296,117**	**41,975,275**
Installed lines	Mobile (GSM)	-	218,522,048	182,065,415	147,004,674	131,319,542	121,785,526	95,291,096	76,545,308
	Mobile (CDMA)	-	18,400,000	18,400,000	17,232,725	17,172,670	14,829,931	10,611,867	1,540,000
	Fixed wired/ Wireless	-	11,342,677	11,342,677	9,394,042	9,347,771	9,388,145	6,830,245	6,58,303
	Total	-	**248,353,725**	**211,808,092**	**173,631,441**	**157,839,983**	**146,003,602**	**112,733,208**	**84,663,611**
Teledensity (%)		**93.41**	**91.15**	**80.85**	**68.49**	**63.11**	**53.23**	**45.93**	**29.98**

Source: http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:art-statistics-subscriber-data&catid=65:cat-web-statistics&Itemid=73

The increase in teledensity has also brought an astronomical increase in the information flow. The impact of such information flow was felt at the height of Ebola virus attack in Nigeria through the rumour of salt-water bath. However, such free flow of information among Nigerians has not reflected in the fight against crime that could possibly lead to the rescue of kidnapped victims in Nigeria especially the over 200 school girls of Chibok in Borno state. Even the attempt made to elicit information from the communication satellite – NigComSat-I – proved abortive as it was found with neither voice nor video records.

Similarly, other crimes like kidnapping, armed robbery and ritual killings, etcetera have been on the increase (Udeh and Ihezie, 2013 and Onuoha and Ugwueze, 2014). In fact, kidnapping which is taking away of people against their will, usually for ransom or in furtherance of another crime (like the case of Boko Haram) has become a lucrative business in Nigeria. Unfortunate enough, these kidnappers live with us and yet, tracing them has increasingly become difficult.

At this juncture, we can state that the failure to utilize ICTs in security administration is not far-fetched. In fact, not only are the communication gadgets grossly under-exploited, but sabotage also underscores even the little efforts made to elicit information through them. It is therefore suggested that Nigerian government should adequately exploit e-governance through installation, utilization and maintenance of ICT gadgets in the management of the national security. It is also important to initiate programmes designed to bridging the digital divide among Nigerians for effective utilization of the gadgets to enhance protection of lives and property of the citizens while curbing sabotage through the development of indigenous manpower.

5. Conclusion

The study revealed that the use of ICTs in administration of security has not enhanced the protection of lives and property in Northern Nigeria. It noted that, the inability of the Nigerian government to perform this function did not stem from its inadequacies in terms of capability *per se* but inadequacies in terms of exploitation, utilization and maintenance of the Information and Communication Technologies. The satellites launched into space are grossly under-exploited and in some cases sabotaged. NigComSat-1R, for instance, is a hybrid geostationary satellite with a total of 40 transponders which will provide optimal and cost effective voice, data, video and internet applications that can enhance proper security surveillance. Yet, this satellite has not been utilized enough to elicit relevant information that can enhance security in the 21st century Nigeria. Even the effort made at installing CCTV cameras across the country, with Abuja and Lagos as destinations for the pilot project, has been abandoned by the government; instead, the people mostly big business establishments like shopping malls within Abuja are being forced to install the CCTV cameras around their business

premises or face sanction. While some of these business establishments may afford the procurement and installation of CCTV cameras, the teeming majority of Nigerians who wallow in abject poverty cannot. The cheapest amount for procurement and installation of CCTV cameras ranges between £622 and £1886 (that is about N177 270 to N537 510). This amount is simply outrageous for an average Nigerian to afford for procurement and installation of CCTV cameras alone.

Arising from the above, the insecurity especially in the northern part of the country has persisted because the security agents appear incapacitated in terms of information gathering and communication. This has given criminals especially the Boko Haram insurgents an ample ground to keep wrecking havoc to the society. The insurgents make use of sophisticated electronic gadgets (which are almost beyond the understanding of the Nigerian security agents) through which they communicate among themselves as well as relate their activities to the whole world with little or no hindrance. This is a serious challenge to the Nigerian security agents even in tracing the exact location of the insurgents and which place(s) is/are the next target(s). This is not to say that the security agents are not trying. In fact, they have done a lot but their efforts are yet to be sufficiently augmented by the Ministry of Science and Technology and other related agencies, including the global community.

The study therefore found that the level of security of lives and property in Nigeria before 2010 was higher than what it was between 2010 and 2014. The security situation has continued to worsen owing to the digitalization of crimes without corresponding efforts to adequately exploit the digitalized security gadgets and develop indigenous manpower to man them for effective countering of cyber sabotage. The point being made is that until the Nigerian government begins to adequately exploit e-governance through installation, utilization and maintenance of ICT gadgets in the management of national security, the insecurity situation will persist.

References

Adeyemo, A.B. (2011) E-government implementation in Nigeria: An assessment of Nigeria's global e-gov ranking. *Journal of Internet and Information System*. 2 (1), 11-19

Adibe, J. (N.D.) Pervasive kidnapping in Nigeria: Symptom of a failing state? [Online] Available: *http://www.hollerafrica.com/showArticle.php?artId=304&catId=&page1&2*. [November 8, 2014].

Agrawal, P., Pandey, V.C., Kashyap, S. and Agrawal, M. (N.D.) Security issue of e-governance. *International Journal of Advances in Computer Networks and Security*. [Online] Available: *http://www.seekdl.org/nm. php%3Fid%3D1083*. [October 13, 2014].

Ajakaye, T. and Nweze, K. (2004) Obasanjo gives reasons for e-government. [Online] Available: *http://allafrica.com/Stories/200403090158.html/*. [October 12,2014].

Akunyili, D. (2010) ICT and e-government in Nigeria: Opportunities and challenges. An address presented at the World Congress on Information Technology held in Amsterdam, Netherland between 25th and 27th May

Aladekomo, D. (2013) ICT can be used in tackling insecurity. [Online] Available: *http://www.informationng.com/2013/05/ict-can-be-used-in-tackling-insecurity-ncs.html*. [November 11, 2014].

Alshboul, R. (2012) Security and vulnerability in the e-government society. *Contemporary Engineering Sciences*. 5 (5), 215-226

Asiabaka, C.C. (N.D.) Imperatives of e-government and the future of Nigeria. [Online] Available: *http://softwareclubnigeria.org/doc/FUTO%25...* [October 21, 2014].

Awe, J. (N.D.) Security: The technology platform. [Online] Available: *http://www.ebusinessnigeria.com/security-platform.html*. [October 21, 2014]

Babalola, Y.T. (2013) Nigeria's information infrastructure policy: Implications for e-Governance. *Arabian Journal of Business and Management Review*. 2 (11), 8-15

Bain, W. (2006). *The Empire of Security*. London: Routledge

Buzan, B. (2007) *People, States and Fear*. London: ECPR

Danfulani, J. (2013) E-governance: A weapon for the fight against corruption in Nigeria. [Online] Available: *http://sahara reporters.com/2013/08/10/e-governance-weapon-fight-against-corruption-nigeria-john-danfulani-phd*. [October 2, 2014].

Fatile, J.O. (2002) Electronic governance: Myth or opportunity for Nigerian public administration? *International Journal of Academic Research in Business and Social Sciences*. 2 (9), 122-140

Gupta, A.K. and Gupta, M.K. (2012) E-governance initiative in cyber law making. *International Archive of Applied Sciences and Technology*. 3 (2), 97-101.

Hough, P. (2004) *Understanding Global Security*. London: Routledge

Hutchful, E. (1998) Introduction: Africa-rethinking security. *African Journal of Political Science*. 3 (1), 1-19

Hwang, M.S., Li, C.T., Shen, J.J. and Chu, Y.P. (2004) Challenges in e-government and security of information. *International Journal of Information and Security*. 15 (1), 9-20

Ingawa, M.S. (2011) E-governance for peace and national development. *JORIND*. 9 (2), 48-51

Johnson, O. (2013) E-government and national security. Keynote Address Delivered at the International Conference of the Nigeria Computer Society (NCS) on July 25

Mohammed, S., Abubakar, M.K. and Bashir, A. (2010) E-government in Nigeria: A catalyst for national development. A paper presented

at Fourth International Conference on Development Studies held at the University of Abuja, Nigeria between 14th and 15th April

Mpinganjira, M. (2013) E-government project failure in Africa: Lessons for reducing risk. *African Journal of Business Management*. 7 (32). p. 3196-3201

Muhammed-Nasiru, I. and Kasimu, S. (2012) Surveillance, information and communication technologies (ICTs) as tools for information gathering and security management. Department of Mass Communication, School of Information and Communication Technology, Auchi Polytechnic, Auchi

Nnoli, O. (2006) *National Security in Africa: A Radical New Perspective*. Enugu: Snaap Press Ltd

Okafor, C. (2013) Abuja: Where are the CCTV cameras? [Online] Available from *http://www.thisdaylive.com/articles/abuja-where-are-the-cctv-cameras/*. [November 8, 2014].

Okwuke, E. (2013) Making ICT facilities critical national security infrastructure. [Online] Available: *http://dailyindependentnig.com/2013/09/making-ict-facilities-critical-national-security-infrastructure/*. [November 11, 2014].

Olubamise, B. (2013) E-government for leadership and policy makers: Imperative for nation-building. A paper delivered at the 11th International Conference of the Nigeria Computer Society held at Iloko-Ijesa, Osun State between 24 and 29 July

Olusina, O. and Okolie, A. (2013) The face of kidnapping in Nigeria. [Online] Available: *http://www.thisdaylive.com/articles/the-new-face-of-kidnapping-in-nigeria/147842/*. [November 8, 2014].

Oye, N.D. (2013) Reducing corruption in African developing countries: The relevance of e-Governance. *Greener Journal of Social Sciences*. 3 (1), 6-13

Sharma, S. (2005) E-governance for conservation in India. A paper presented at the E-Government Conference held at the Grand in New Delhi between 17 and 19 October

Shoyombo, A.O. (2014) Using ICT for securities and business purposes. [Online] Available: *http://nigerianobservnews.com/19022014/features/features4.html#.VEdZGMg1gcA*. [November 8, 2014].

Thomas-Greenfield, L. (2014) United States diplomatic mission in Nigeria. A speech delivered at the US-Nigeria Bi-National Commission Regional Security Working Group on September 4

Tomov, K. and Balabanov, B. (2012) Frame/methodology for the information security management in an e-government environment. A paper presented at ITU Regional Forum on Cyber Security held in Sofia, Bulgaria on October (no particular date).

Udeh, S.C. and Ihezie, U.R. (2013) Insecurity and national economic development: Implication for Nigeria's Vision 20:2020. *International Journal of Development and Management Review*. 8 (1).

Ugwueze, M.I. (2014) Security, governance and wealth creation in Nigeria: The way Forward. *International Journal of Humanities and Social Studies*. 2 (9), 431-348

UNESCO (2006) *Curriculum Guide on E-Governance for African Government Institutions*. N/A: African Training and Research Centre in Administration for Development

Wolfers, A. (1962) National security as an ambiguous symbol. *Political Science Quarterly*. 67 (4)