Pinisi Journal of Art, Humanity and Social Studies
Vol. 1 No 1, 2021. Page 44-53
e-ISSN: 2747-2671
Homepage: https://ojs.unm.ac.id/pjahss/index

The Role of Information Technology in Enhancing National Security in Nigeria (2001 -2020)

Ekwutosi, E. Offiong[1], Effiong, Eke Nta[2]*, Inyang Etim Bassey[3]
[1,2,3]Department of History & International Studies, University of Calabar, Cross River State, Nigeria.
*: eke4god1@gmail.com

Abstract

The security problems of Nigeria have continued to stare at her very ominously and intermittently harass her, both within and outside her shores. These have lingered on and have created a clog on the wheel of the country's progress, indeed dramatically stagnating, and to say the least, truncating the mainstay of the country's survival. Several interpretations, theories, analyses, syntheses, and jingoistic conceptualization have been propagated, all producing the same result. From scientific to technological approach, religious to ritualist approach, political to social approach, the security situation rather than improving, is static and under some regimes retarded. Academic contributions, especially ideas from the humanities and indeed the discipline of history are jettisoned, in fact, quickly dusted into the waste bin. The concern of this paper is to attempt a historical investigation of the security problems in Nigeria, identifying them to show how information and communication technology can help in curbing these challenges, using the realist paradigm as a theoretical framework. This study identifies Nigerians as the cause of her security problems, who rather than face these seismic challenges head-on, abandon them – a cowardly act, ending in futility and deeper chaos. This study adopts both primary and secondary sources of data collection. It is hoped that if academic exercises are not mere, this input may create a turnaround in the security situation in Nigeria.

Keywords: Nigeria, National Security, Information Technology, Security Problems.

1. INTRODUCTION

The world is said today to be a "global village". Part of the reason for this assertion is because of the role of information technology which represents an integral part of globalization. Information has also been described as power. The power for effective and efficient management of national security largely depends on the power of available but dependable information. With information as power, it is expected that improved information sources, processing channels, sophistication, and complexities could better be managed through information technology; which in turn have a strategic and pivotal role to play in a country's national security. Although insecurity is a global issue, the challenge is more pronounced in Third World countries, as compared to the technologically advanced societies with highly sophisticated information technology mechanisms for managing their national security.

National security has remained one of the cardinal objectives of the most responsible states in the world. As a matter of social contract and serious concern, most nations prefer to enshrine the notion of protection of lives and property in their constitution. This explains why the development of any society to a large extent depends on the extent of the security of lives and property of the citizens (Offiong 2016; Ekpenyong *et al*., 2018). In recent times, the increasing level of insecurity in Nigeria evokes serious concern. On daily basis, we hear, witness, or read about one form of killing, a disaster occurring in the various parts of the country. Successive leadership in the country for the past decades has always seen national security only from the prism of the number of barrels of guns, the number of armored vehicles, fighting jets,

and existing recycled security agents. In a global world today, security has gone beyond that. It is more encompassing and complex. It cuts across issues like social security, economic security, environmental security, regime security, energy security, human security, societal security (Akpan *et al*., 2021).

As long as it's power, it is expected that improved information sources and channels through information technology could play a strategic and pivotal role in a country's security outfit and process. Though insecurity is a global challenge and every society strives hard to manage its security outfit, national security has remained one of the cardinal objectives of the most responsible state in the world (Ekpo & Offiong 2020). The development of any society to a large extent depends on the extent of the security of lives and property of the citizens. A secured atmosphere will encourage intellectual minds who will be a great asset to Nation-building; it will also guarantee an environment for the growth of infrastructural development.

Over the years, Information and Communication Technology (ICT) has played a very vital role in the fight against insecurity and other related offenses in Nigeria and the world at large. In developed nations like the United States, Britain, and some less developed ones such as in Africa like Nigeria, Ghana, etc, ICT has proven to be effective in managing threats, even though there remains a huge gap between the kind of insecurity experienced in developing nations like Nigeria and the way they are handled compared to developed nations like the United States of America, Britain, etc. The advent of information and communication technology (ICT) has brought tremendous innovation in virtually all spheres of human endeavor. Technology as it were, is one of the platforms that cannot be ignored, especially when it comes to insecurity whereby a lot of instruments can be deployed to tackle and improve the vigilance of all the organizational activities (Bassey, 2020).

ICT can be a great tool in the detection and identification of citizens, their interaction and communication, movement, education, and so on. The rate of insecurity in Nigeria today is alarming (Ekpenyong *et al*., 2018, Betiang *et al*., 2018; Andong *et al.,* 2019). On daily basis, lives and property are wasted due to a high level of insecurity which revolves around killings, kidnapping, and bombing. The security challenge in Nigeria today makes government spend a huge amount of money in fighting the scourge. Of course, these monies that otherwise could have been channeled to other areas of human development. Meanwhile, there seems to exist a gap in knowledge on the use of ICTs in curbing these security challenges in Nigeria.

Owing to this death of knowledge in this area, this paper seeks to highlight the state of insecurity in the country, and the role of information and communication technology (ICT) in tackling the security challenges existing in Nigeria as a nation today. The study is quite important at the moment because it intends to create greater awareness of the surging manner of insecurity in the country which has over time resulted in all manner of crime and criminality. This is of the view that if the growing manner of insecurity in the country is not further checked, it could further result in anarchy, lawlessness, and increased poverty, loss of lives and human resources, etc. Finally, the study will contribute to scholarly works in the field. The study will also contribute to scholarship and equally popularize the existing knowledge in this area.

2. CONCEPTUAL CLARIFICATION

2.1 Information and Communication Technology (ICT)

Though, essentially, Information and Communication Technology (ICT) is used as an umbrella term to refer to the use of communication devices (such as radio, cellular devices, satellite devices and channels, computers, amongst others) and utilities (programs) to manage information (acquisition, dissemination, processing, storage, and retrieval) (Bashar 2017). Put differently, information and communication technology (ICT) are those electronic gadgets, equipment, or technologies for creating, acquiring, storing, processing, communicating, and using information. The concept is also used to refer to the convergence of audio-visual and telephone networks with computer networks through a single cabling or ink system (Bashar 2017).

It encompasses both the internet-enabled sphere as well as the mobile one powered by wireless networks. It also includes antiquated technologies, radio and television broadcasts – all of which are still widely used today alongside cutting-edge ICT pieces such as artificial intelligence and robotics. It is sometimes used synonymously with IT (for information technology). ICT is generally used to represent a broader, more comprehensive list of all components related to computer and digital

technologies than IT. The list of ICT components is exhaustive, and it continues to grow. Some components such as computers and telephones have existed for decades. Others, such as smartphones, digital TVs, and robots, are more recent entries.

ICT commonly means more than a list of components, though it also encompasses the application of all those various components. However, this study adopts a simpler definition of the concept as articulated by Prasad Ramjee, and Vandana Rohokale in *Cyber Security: The Lifeline of Information and Communication Technology* (2020). To them, information and communication technology refers to the digital processing and utilization of information by the use of electronic computers. It comprises the storage, retrieval, conversation, and transmission of information. It is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems, and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

2.3 Security

Security in any objective sense, measures the absence of threat to acquire values, in a subjective sense, the absence of threats to acquired values and the absence of fear that such value will be attacked (Collins 2018). It could also imply both coercive means to cheek an aggressor and all manner of persuasion, bolstered by the prospect of mutually shared benefits, to transform hostility into a corporation. Just like information technology, the concept "National Security remains ambiguous, having evolved from simpler definitions that emphasized freedom from military threat and freedom from political coercion. By the way, security in an objective sense measures the absence of threat to acquire values, in a subjective sense, the absence of threats to acquired values and the absence of fear that such value will be attacked (Barnett 2018). It could be referred to as the ability to withstand aggression from abroad.

Inlay terms, National Security could be seen as a state of absence of everything and anything that could be a threat to peace, progress, development, and tranquility within a society. According to Collins (2018), a nation is secured to the extent to which it is not in danger of having to sacrifice core values if it wishes to avoid war, and is able if challenged to maintain them by victory in such a war.

A threat to national security is an action or sequence of events that threatens drastically and over a relatively brief period to degrade the quality of life for the inhabitants of a state or threatens significantly to narrow the range of policy choices available to the government of a state or to private, non-governmental entities (persons, groups, corporations within the state) (Ellah 2014).

National Security is wider in scope or entails a lot more than military security (Katzenstein 2018). At the same time, while it is easy to see external coercion as a major challenge to national security because of its visible impact, there is doubt if it is more critical than the consequences of internal disequilibrium in a nation's social system. Thus, National Security cannot be equipped for military might, defense of law enforcement alone. It goes beyond all of that to accommodate far more reaching issues. In short, national security is the ability of a state to overcome any of its challenges no matter what the challenge is. Indeed, the issue of national security can be adequately addressed using Information and communication technology.

3. THEORETICAL FRAMEWORK

Several theoretical underpinnings have emerged for the study of national security and the role of information technology. Prominent amongst them has been the realism approach, the liberalism approach, and the Marxist approach (Historical Materialism). For this study, the realist paradigm is adopted. The proponents of this include; Kenneth Waltz, Hans J. Morgenthau, W.H. Carr, Thucydides, etc (Wynn & Williams 2012). Virtually all states place great value on maintaining their international security-remaining free from attack and coercion by other states. Realism is a theory of international relations that addresses how states achieve security and possibly other goals. Realism attempts to explain the security strategy a state should choose. In broad terms, realism asks whether a state should choose a competitive strategy. Part of such strategy here is the use of information technology in automating national security issues or complex problems such as terrorism, war, threats, nuclear disaster, etc. Realism views power as a defining feature of the international environment that states face. It envisions the state as essentially unitary actors.

This is not an accurate assumption. States are made up of leaders, governing institutions, interest groups, and populations. Realism sees the state as rational actors; states make decisions that are well-matched to the achievement of their interest, given the constraints imposed by their capabilities and the uncertainties they face about other states.

In making decisions such as whether information technology should be deployed essentially for national security purposes, they take into consideration how other states will react to their policies. The theory is silent about who controls the state, who manipulates the state to achieve any defined purpose after all the state is not an inanimate object or entity but must be directed and controlled by human beings (powerful actors).

4. EVOLUTION OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT)

Information technology has been around for a very long time. As long as people have been around, information technology has been in existence because there were always ways of communicating through technology available at that point time. Four (4) main stages divide up the history of information technology. Only the latest stage (electronic) and some of the electrochemical age that affects us today, but it is pertinent we take a look at how we got to the point today. Pre-mechanical stage: This is the earliest age of information technology (Heeks 2010). It is the age between 3,000 BC and 1450 AD. By then, communication was through the use of language or simple picture drawings known as petroglyphs which were usually carved in the rock. Early alphabets were developed such as the Phoenician alphabet. As alphabets became more popular, and people started writing down information, pens and paper began to be developed (Heeks 2010). It started as just marks in wet clay, but later the paper was created out of papyrus plant.

During this period were the first numbering systems. Around 100AD –was the first 1-9 system created by the Indians. However, it wasn't until 875AD (775 years later) that the number O was invented (Heeks 2010). This creation of numbers gave birth to the idea of creating a calculator since people wanted stuff to do with the numbers. A calculator was the very first sign of an information processor. The popular model of that time was the abacus. Mechanical Stage: The mechanical stage signaled the first connection between our current technology and its ancestors. This is the period between 1450-1840 (Heeks 2010).

A lot of technologies were developed during this era as there was a large explosion of interest with this era. Technologies like the slide rule (the analog computer used for multiplying and dividing) were invented. Blaise Pascal invented the Pascaline which was a popular mechanical computer. Charles Babbage developed the different engine which tabulated polynomial equations using the method of finite differences. Electromechanical Age: This is the period between 1840 and 1940 (Swedin & Ferro 2005). This was the beginning of telecommunication. By early 1800, the telegraph was already created Morse code was created by Samuel Morse in 1935. The telephone (one of the most popular forms of communication ever) was created by Alexander Graham Bell in 1876. The first radio was developed by Guglielmo Marconi in 1894 (Swedin & Ferro 2005). All of these were extremely crucial emerging technologies that led to big advances in the information technology field.

The next Age which incidentally is the last is the Electronic Age. The mechanics from the last era were replaced with vacuum tubes which made electronics possible. The age started in 1940 and continued until the 2000s. Vacuum tubes were not used for cleaning. The first general-purpose computer was called the UNIVAC (Universal Automatic Computer) (Swedin & Ferro 2005). However, then digital computing came along still in the Electronic Age: Digital computing came in the form of four generations. The first generation relied on vacuum tubes, punch cards, and a computer. The second generation replaced the vacuum tubes with transistors. Transistors were used first by AT & T (American Telephone &Technograph) – a large US company that provides telephone and digital services and equipment. These new inventions were smaller, they were more energy-friendly and they created less heat all great qualities for a general use computed. External storage and programming language were evolving as punch cards were replaced with magnetic tape disks.

The next Age which is the Age we are now could be termed the virtual Age. It began in 1991 when the sales force invented SaaS (Software as a Service). People were able to subscribe to a service without having to buy every expensive update and being able to access the memory from multiple data points. It was easy to access the virtual memory of different devices like smartphones and tablets

(Swedin & Ferro 2005). New input methods like touch screens came to us only a few years ago although now it seems rudimentary. Information Technology is constantly evolving and will keep at the same pace or faster.

5. CAUSES OF THREATS TO NATIONAL SECURITY

There are several reasons put forward by scholars regarding this unwelcomed visitor. Among others, they include:

5.1 Militarization of Youths by Political Irredentists

The root of evil summarizes the psychological forces that spawn such crime. When youths are unable to speak up to defend themselves and those who used them for their self-seeking political ambition, dump them after achieving their selfish ambition and fail to disarm them, what then do we expect? The answer is not far-fetched, it is to unleash terror and violence on their exploiters and cohorts, which consequently has a multiplier effect of wading into national security.

5.2 Border Crime

Otherwise known as transnational crime refers to a crime that takes place across national borders. They include human trafficking, arms trafficking, drugs trafficking, etc (Offiong 2019). Smuggling is a seminal threat to national security as it undermines the security of the nation, for it represents a formidable national security problem.

5.3 Sectionalism

This is also a prominent factor that constitutes threats to national security. Nepotism, tribalism, regionalism, cronyism, and religious bigotry, collectively known as sectionalism rewards mediocrity and relegates competent expertise because the yardstick is who knows you, not what you know. Sectionalism rewards complacency but punishes hard work because the yardstick is where you come from, not whether you are the first to arrive. Sectionalism has been the fundamental cause of Nigeria's underdevelopment and inability to evolve into an egalitarian and prosperous modern nation (Ellah & Otora 2014). If corruption has national security implications, then sectionalism of whatever form is a cause of threat to national security.

5.4 Religious and Political Intolerance

Religious and political intolerance has to do with the unwillingness of some people of particular religious and political beliefs to put up with others who have different religious or political beliefs from theirs. Incidents of religious and political intolerance have been manifested in Nigeria on several occasions. The recent Boko Haram episode in a certain part of Northern Nigeria like Borno, Kaduna, etc is a case in point. Instances of political intolerance include the political crisis of 1956 in the West and the violence which greeted the 1993 General election in the country (The Abiolavs Tofa Saga). The events which led to the civil war of 1967-1970 were not unconnected with this basic manifestation of various shades of intolerance (Doron 2014). The fear being expressed by concerned Nigerians is the danger of the country being torn apart if the various shades of intolerance are not properly managed. In particular, there is the need to de-emphasize religion from the country's body politic.

6. IMPORTANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) TO NATIONAL SECURITY

The benefits or usefulness of Information and Communication Technology to National Security cannot be over-emphasized. It is important not only to the government but to the nation as a whole. However, Nigeria's security concerns and threat perceptions emanated from many quarters. These include the threat of extreme Islamic sects like Boko Haram, Shiite Islamic militant group Fulani Herdsmen group, high level of unemployed youths, Militant from the oil-rich Niger Delta, ritual killings, the widening economic gap between the poor and rich, the influx of illegal migrants from the neighboring countries through Nigerian porous borders. Security threats and other challenges in the country are multi-dimensional in nature and scope.

Traditionally, crime and security establishments throughout Nigeria have operated largely bureaucratic, paper-based institutions which have stifled the process of information sharing, it is, therefore, important to recognize that the traditional ways of meeting the challenges need to be expanded to encompass new non-traditional threats (Collins 2018). The use of Information and Communication Technology (ICT) is slowly emerging as one response to critical issues faced in the country. As such, many ICT implementations are beginning to take shape in response to incidents that have affected the country

which will lay the foundation for further evaluation of regulatory mechanisms for handling crises in the country. Deploying ICT in a certain aspect of the National Transformation Agenda and the ICT policy of the Nation will play a vital role in combating the current national security challenges. Below are some areas where ICT could improve national security in Nigeria.

6.1 Financing

This plays a huge role in the activities of terrorists and disrupting finances should be a priority of national security. ICT is a vital tool for tracking and investigating suspected financial transactions. With the recent introduction of the cashless society, the transaction will be forced to electronic platforms where suspicious cash movements can be identified and questioned. This would go a long way in curbing the financing of activities that constitute a threat to national security.

6.2 Communication

Intercepting communication between and within terror groups and enhancing interactions within security agencies can be achieved through the deployment of ICT. Several gadgets and technologies are used in communication and exercising the role and ethics of those technologies will help in tagging and tracking information that is/was communicated using certain devices. Also in the ethics of IT, every electronic device deployed has a unique identification number (IUID) that makes the device electronically traceable (Raphael and Stoke 2018). This system could be deployed positively in the interest of national security.

6.3 Surveillance

Computer surveillance involving the monitoring of data and traffic e.g. phone calls and broadband internet traffic (emails, web traffic, instant messaging, etc) are required to be available for unimpeded real-time monitoring by federated law enforcement agencies. So many forms of technologies can be used such as surveillance cameras, social network analysis, biometric surveillance, data mining and profiling, corporate surveillance, satellite imagery, geolocation devices. Using satellite and navigation systems, remote surveillance can be made across various geographically distant locations either for security or information purpose. Also, navigation could be carried out successfully through previously unknown locations using maps and positioning systems (such as the global positioning system-GPS), which are powered by ICT (Kumar & Moore 2002). These systems could prove very useful in building intelligence information and reports that could be very essential and invaluable in the task of thwarting and combating crimes.

6.4 Intelligence Gathering

Using ICT tools to engage the public in acquiring information that has the potential to enhance national security. The internet, print, and electronic media are useful in gathering useful information to assist in the nation's security efforts.

6.5 Coordination

The use of cutting-edge technology to centralize and coordinate the entire Nation's data will act as a proactive and dynamic means of combating insecurity. A basic example is the development of a central intelligence unit or counter-terrorism unit with a robust, dynamic, vibrant, and updated central database. The database should be centralized containing every data and details of the Nation. An example is converting the National Identification Card into an electronic form also making all the identification (driver's license, sim card registration, National ID, etc) into a single digital electronic form and uploaded on a central database.

6.6 Identification

Birth and death registration in addition to unifying various identification initiatives could play a significant role in national security especially when combined with DNA, facial recognition, and fingerprinting technologies e.g. The introduction of the fingerprint authentication system during JAMB examination registration and election process, mobile banking, global system for mobile communication in almost all parts of the country, use of geographic information systems, e-commerce, etc. Also, various sectors of the crime and security forces have been moving towards the implementation and use of ICT. Such as the Public Security Communication System (PSCS) to install CCTV Cameras in areas like Lagos and Abuja, to monitor crimes and address criminality to assist the security agencies in their effort to combat crime.

However, while ICT' does not represent a panacea to crime and security issues facing Nigeria, it does present very viable opportunities for enhancing

collaboration efforts already in existence to effectively tackle the country's security challenges. Informing the factors for consideration to put in place an effective framework for effective implementation in the area of crime and security using ICT's, it is instructive to look at the issues from a global perspective, to identify possible best practices which can be contextualized and used in Nigeria.

6.7 ICT Education

Every efficient use of technology begins with knowledge and skill acquisition. Therefore, to use ICT to tackle insecurity in Nigeria, security agents must be well trained in the use of ICT tools. Information and Communication Technologies (ICT) education is the teaching and learning of valuable ICT knowledge and skills around computing and communications devices, software that operates them, applications that run on them, and systems that are built within them (Oghordi, 55).

6.8 Use of Lawful Interception

Many of the crimes carried out today include the receipt of threat messages from an anonymous individual. These messages must be lawfully intercepted. Lawful interception (LI) is the legally sanctioned official access to private communication such as telephone calls or e-mail messages (George 2010). Such lawful interception of information should be transmitted on internet traffic or mobile phones. With lawful interception laws, it will be easier to monitor a greater number of individuals under suspicion, while the information of non-targeted individuals remains private. In summary, (ICT) is useful to National Security thus; (a), For national integration which opposes national insecurity, (b) Fighting crimes, (c) Regulating the society.

7. PROBLEMS AND PROSPECTS OF INFORMATION AND COMMUNICATION TECHNOLOGY IN NIGERIA.

7.1 Problems

Available historical evidence reveals that after the Nigerian civil war in 1970, the security situation in Nigeria has been relatively stable (Idoko, 2014). People had peace and can move freely from one part of the country to another without harassment or molestation, life was easy going. No many problems among different ethnic groups living together. Everybody struggled to make two ends meet. Lives and property of people were secured because of the alert of security agents like the police, the soldiers, and different societal vigilante groups. People feared causing problems because of the wrath of the law. Security in the country was highly maintained.

However, the case of insecurity resurfaced as far back as the year 2000 in the country, starting from the Niger Delta crisis to insurgency in the Northern part of the country. This crisis with its attendant effect of insecurity started in Nigeria in the area known as the Niger Delta, consisting of Delta, Bayelsa, Rivers, Abia, Akwa Ibom, Cross River, Edo, Imo, and the Ondo States for years where militia groups rose against the Nigeria nation by blowing up some oil flow stations, kidnap foreign oil workers, vandalize oil pipelines, and disrupt oil business generally. This crisis is attributed to greed, selfishness, deprivation, poverty, and social injustice. To tame the crisis, the Nigerian government granted amnesty to the Niger Delta Militants, but as the government of Nigeria was yet to recover from the adverse effect of the militancy in Niger Delta, a terrorist organization, Jama'atu Ahlis Sunna Lidda' await Wal-Jihad, known by its Hausa name Boko Haram; figuratively meaning "Western Education is a Sin" emerged in the Northern part of the country, thereby opening a new ware of insurgency in Nigeria (Comolli 2015).

The group exerts influence in the Northeastern Nigerian State of Borno, Adamawa, Kaduna, Bauchi, Yobe, and Kano. This terrorist group bombed schools, churches, and Mosques, public places, kidnap women and children, raids vulnerable villages and assassinate politicians and religious leaders. The 2014 abduction of 219 female students from the government secondary school in Chibok town in Borno State, Nigeria, and the 2011 bombing of the United Nation House headquarters in Nigeria nation's capital, Abuja are cases in point. Boko Haram, therefore, is Nigeria's synonym for fear and bloodshed.

Unlike the Niger Delta militant, Boko Haram Sect rejected the idea of amnesty. This rejection implied that the Boko Haram Sect was more ready than ever to take up arms against the state, and indeed insurgency increased in the northern part of the country thereafter. With the Niger Delta militancy and insurgency in the North, the crime wave increased in unimaginable proportion across the length and breadth of the country. However, it is worthy of note that, aside from the Niger Delta Militancy and Boko Haram insurgence, security threat

perception meanest from several other quarters such as high level of unemployed youths, ritual killings, the widening economic gap between the poor and the rich, the influx of illegal migrants from the neighboring countries, the emergence of political and regional thugs and the collapse of justice system among others. This is only but a pointer to the fact that Nigeria is tottering towards becoming a failed state if the insecurity situation in the country continues to be handled with kid gloves.

7.2 Prospects

Quite frankly, can Nigeria achieve security of all her territory which includes land and sea without the use of technology? Are our leaders making the right investments in that direction or just playing lip service to the issue of national security? The last couple of years have seen Nigeria grapple with one security challenge or the other. The most recent is the herdsmen challenge that has deeply divided this country. The next in line is the Boko Haram insurgency, Indigenous people of Biafra (IPOB) onslaught, the Niger Delta militant group, etc. One wonders what is stopping us from investing in solutions that can electronically tag every single cow in the country to its owners such that we know where they are at every point in time and as such monitoring becomes a lot easier (Collins, 2018).

Information technology will help us to sort out who is who, where who resides, who owns what, and so on. Some efforts by the successive government in actualizing this dream of using information technology to collect and collate data for national security and development have manifested in areas such as – the Nigeria Identity Management Commission, Central Bank of Nigeria's BVN, Nigeria Communications Commission, The Telecom, the Independent National Electoral Commission, and the Federal Road Safety Commission.

One wonders why the unnecessary and wasteful continuous collection of citizen's data by different government establishments, yet there is shamefully no coordinated effort to centralize the entire process. The willpower to pull all these data into a central database is the first way to go towards using technology to aid our national security. In more technologically advanced societies of the world, birth and death registration in addition to unifying various identification initiate play significant roles in national security, especially when combined with DNA, facial recognition, and fingerprinting technologies which operate on platforms provided by ICT. And that is why it is usually less cumbersome tracing and tracking down terrorist groups or criminal gangs in such countries. Today, our security agents are not meeting the expectation in terms of national security. Incessant killing and bombing in the middle belt region by the herders and Boko Haram sect including organized trafficking, kidnapping, and robberies are all clear testimonies to the fact.

The Nigerian federal government may have invested little in drones and robotics, and maybe our military has unarmed aircraft and equipment, but operations that call for intelligence gathering especially in areas to reach difficult terrain must be taken seriously. It entails the use of electronic compilers and computer software to convert, store, protect, process, transmits, and securely retrieve information. Information technology (IT) will play a critical role in strengthening Nigeria's National Security against potential future attacks. Other modern technologies such as surveillance cameras, social network analysis, biometric surveillance, satellite imaging, RFID, and Geo-location devices are required to mount surveillance on suspected targets.

Today, ICT tools such as the internet, mobile telephony, system, social media networks, and the media have become veritable platforms for intelligence-gathering efforts of our security agencies so long as they observe the ethics of using these technologies for intelligence gathering purposes. One issue that needs to be tackled going forward is using technology to ensure that there is proper cooperation and coordination amongst security agencies. Through the development of cutting-edge technologies, security agencies can minimize duplication efforts, guard against the mishandling of information as well as enhance information sharing among themselves.

Coordination can also mean pulling the nation's data into a coordinated and centralized database as a proactive means of combating insecurity. By so doing, we are assured that the words of Chris Uwaje, popularly known as De Oracle of the IT industry would have come to pass - the war of the future will be fought in the cyberspace and we need to focus on building our capacity (Ijezie 2021).

8. LIMITATIONS OF ICT AS AN INSTRUMENT FOR ENHANCING NATIONAL SECURITY IN NIGERIA:

The use of information and communication technology tools in fighting insecurity is not without

some challenges. This challenge among other includes:

8.1 Low level of ICT Skills among Security Personnel

This is one of the major challenges to the use of ICT to combat crime in Nigeria. Available evidence from the International Telecommunication Union (ITU), development index for ICT use and skills ranked Nigeria 122nd position out of the 155 selected economies as of 2011 with an abysmal growth rate of 0.18%. In a related study, out of 255 personnel of the Nigerian Army Signal Corps, only 89 personnel could use ICT tool without assistance.

This is a reflection of what happens in other sections of the Armed Forces and the securities agencies. Gone are the days when the purpose of sophisticated personnel computers and other electronic gadgets were the exclusive preserve of very rich and multi-national corporations and large business organizations. In other words, ICT tools are becoming cheaper and more readily available; therefore, the availability must be translated into effectual use of the tool to tackle problems of life.

8.2 Lack of Government Commitment

Nigerian Government fights insecurity more from her military effort other than the use of ICT. To this end, Nigeria's expenditure on military hardware to combat crime is on the increase. In Nigeria, military expenditure of 2.327 billion dollars (N372.3 billion) in 2012 alone makes Nigeria's military spending to be the sixth-highest in Africa, and it competes with the expenditure of countries like Libya (2.9 billion dollars). Morocco (3.4 billion dollars), Angola (4.1 billion dollars), South Africa (4.4 billion dollars), and Algeria (9.3 billion dollars). A government is combating the rising insecurity in the country occasioned by insurgencies emptying from different segments of the society (through the military), with an embarrassing quietness from the ICT sector. This quietness in using the ICT resources to combat insecurity is coupled with a lack of commitment by the Nigerian Government in deploying the ICT resources to this end. This lukewarm attitude can be seen from the government's inability to put in place the necessary infrastructure.

Another problem is the fact that ICT infrastructure and systems are deployed in most countries without adequate provision for the internal security of these infrastructure systems at the design and implementation stages of the deployment of these infrastructures. These systems are deployed with numerous exploitable vulnerabilities inherent in their very design and fabrication.

9. CONCLUSION

The use of ICT to enable effective management of crime and security in Nigeria is not a one-time event, but a process of continuous development. The main thrust of the strategy will be to thoroughly communicate the benefits of ICT adoption within a knowledge management framework to enable better protection of the borders and the people of Nigeria.
Conclusively, no nation progresses in a state of insecurity. Progress comes when economic activities take place in an environment of safety (Olufu & Offiong 2017). Therefore, every nation including Nigeria must include national security as one of their enduring interest to create enabling environment for economic, political, and social activities to thrive. Nigeria's national security is an issue for every Nigerian. This is because the state of insecurity can hamper Nigeria's vision of becoming one of the leading 20-nations of the world by the year 2030 which is a few years away.

Traditional agencies (the army and others) have done almost all they could to salvage the country from these growing security challenges, but there is still a need for the federal and state government to embrace the application of ICT in the fight against insecurity as this will not only curb the problem of insecurity but will also give more confidence to other countries of the world that indeed Nigeria is a haven where business can thrive well.

In the light of the above, the following recommendations are made to be able to use ICT to confront security challenges in Nigeria. Law enforcement agencies can possess an unprecedented capability to monitor threats. Security agencies should be grounded in the use of modern electronic surveillance technologies. Recruitment of ICT skilled personnel into various arms of the security agencies. Continuous training and retraining of security staff on modern ICT tools. National identify management commission (NIMC) live up to expectations.

REFERENCES

Akpan, C. O., Akpan, D. C., & Bassey, S. A. (2021). Menace of street urchins in Nigeria. *Przestrzeń Społeczna*, 1(21).

Andong, H. A., Betiang, P. A., & Ani, A. (2019). Vocationalizing Community Education in Nigeria: Focus on the Imperatives of Addressing Corruption Concerns. *Journal of Education, University of Calabar*, 15(1), 188-191

Barnette, J. (2010). 'Environmental Security' in Collins, A (ed) Contemporary Security Studies. Oxford: Oxford University Press.

Bashar, L. M. (2017). Human security for sustainable development in Nigeria: The role of information and communication technology (ICT). *Covenant Journal of Informatics and Communication Technology*, *5*(2).

Bassey, S. A., (2020), Technology, Environmental Sustainability and the Ethics of Anthropoholism. Przestrzeń Społeczna, 1(19).

Betiang, P. A., Ekuri, K.A., & Andong, H. A. (2018). Community Development and Conflict Resolution: A Dialectical Approach. *The Environmental Studies Journal*, 1(4), 64-71.

Collins, A. (Ed.). (2018). *Contemporary security studies*. Oxford university press.

Comolli, V. (2015). *Boko Haram: Nigeria's islamist insurgency*. Oxford University Press.

Doron, R. (2014). Marketing genocide: Biafran propaganda strategies during the Nigerian civil war, 1967–70. *Journal of Genocide Research*, *16*(2-3), 227-246.

Egbe, B. O., & Okoi, I. O. (2021). Ethnic Conflicts in Post-Colonial Nigeria: A Discourse. *International Journal of Humanitatis Theoreticus*, 5(1) 144-153.

Ekpenyong, V. O. Ebinyi, D. W., & Ushie, G. B. (2017). Gender Equality and the Empowerment of Women for Sustainable Development in Nigeria. *Education for Today: Journal of Faculty of Education*, 13(3), 10-17.

Ekpenyong, V. O., Tawo, C. N., & Oboqua, E. D. (2018). Non-formal education for empowering adults in Nigeria for sustainable development. *Adult Education in Nigeria*, 23(II), 120–127.

Ekpo, C. E., & Offiong, E. E. (2020). Nigeria: The Paradox of a Secular State. *Politics and Religion Journal*, *14*(1), 149-172.

Ellah, T.O. (2014). Nigerian Foreign Policy After 50 Years of Independence: Problems and Prospects. *MENDYENG Journal of Central Nigeria Studies*, 3(2), 191-201.

Ellah, T.O., & Otora, O. A. (2014). ECOWAS Prospects For Regional Integration in the West African Sub-Region. *The Legion: An Academic Journal of Interdisciplinary Studies*, 6(1), 90-98

Heeks, R. (2010). Do information and communication technologies (ICTs) contribute to development?. *Journal of international development*, *22*(5), 625-640.

Ijezie, L. E. (2021). Youth Responsibility in Making the World Liveable: A Theological Perspective. *Journal La Sociale*, *2*(4), 9-15.

Katzenstein, P. J. (2018). *Cultural norms and national security: Police and military in postwar Japan*. Cornell University Press.

Kumar, S., & Moore, K. B. (2002). The evolution of global positioning system (GPS) technology. *Journal of science Education and Technology*, *11*(1), 59-80.

Offiong, E. E. (2016). Society in transition: The encounter of traditional African socio-cultural and religious practices with modernity in Calabar. *Lafia Journal of African and Heritage Studies*, 1(1).

Offiong, E. E. (2019). Language and discourse in Nigerian education: historic implication of gender issues. *Society Register*, *3*(4), 37-56.

Oghorodi, D. (2014). *Development of Information and Communication Technology as a means of combating National Insecurity in Nigeria*. Warri: Open Access press.

Olufu, G. O., & Offiong, E. E. (2017). Bekwara and Tiv relations in the Benue-Cross River valley to 1960. *Journal Mandyeng Journal of Central Nigeria Studies*, *1*(1), 76-86.

Prasad, R., & Rohokale, V. (2020). *Cyber Security: The Lifeline of Information and Communication Technology*. Springer International Publishing.

Raphael, S. and Stoke D. (2018). 'Energy Security in Collins A (ed) Contemporary Security Studies. Oxford: Oxford University Press.

Swedin, E. G., & Ferro, D. L. (2005). *Computers: the life story of a technology*. Greenwood Publishing Group.

Wynn Jr, D., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *MIS quarterly*, 787-810.