# ELECTRONIC GOVERNANCE IN SECURITY SECTOR IN NIGERIA: A CURSORY EXAMINATION OF BENEFITS AND CHALLENGES

**OKPO, Francis Chibuzor, *fsi, fspsp*, PhD**
National Institute for Security Studies, Bwari, Abuja.
nwaigwenezuruoha@gmail.com
&
**EZEMA, Celestina Nonyelum**
University of Science and Technology, (ESUT), Enugu
ijenuwa@yahoo.com

==========

**Abstract**
E-governance is imperative for simplifying the complexity of the modern security management. Hence, all nations are leveraging on e-governance to mitigate the problems arising from the digitalization and globalization of crimes. The deployment of Information and Communication Technologies (ICTs) has thus become vital, especially as it reduces cost while increasing efficiency and effectiveness in security management. However, while considerable successes have been achieved in other sectors of the Nigerian economy through the adoption of e-governance, its result in the security sector remains minimal as the insecurity situation across the country continues to escalate despite the application of ICTs in security administration. The research seeks to identify why the utilization of ICTs in security administration has not improved the security situation in the country. It is a documentary enquiry that employs qualitative methods in gathering and evaluating data and drawing inferences from them. The main finding is that though the utilization of ICTs in security management has achieved some successes, it has not been able to improve the security management in Nigeria. This is due to the gross underutilization of the existing ICT-driven security equipment, inadequate knowledge of ICT systems/dearth of ICT experts, poor electricity supply, incompetent leadership and pervasive corruption, political interferences in security operations, poor international collaborations among others. To ameliorate the threatening situation, the leadership of the security architecture should consciously key into utilization of available ICT tools, while government at national and sub-national levels should increase funding for the procurement of requisite state-of-the-art ICT-driven equipment in the management of national security, and training of security agencies to be ICT compliant.

**Keywords**: E-Governance, E-Administration, National Security, Security Sector and Information and Communication Technologies (ICTs).

==========

## Introduction

The critical role of information technology, which represents an integral part of globalization, has made the world a global village. Also, the power for effective and efficient management of national security largely depends on the available critical

information and intelligence to the security sector of any nation. Adeyemo (2020) and Akpan *et al*., (2021) note that with information as power, it is expected that improved information sources, processing channels, sophistication, and complexities could better be managed through information technologies; which in turn have strategic and pivotal role to play in a country's e-governance of its complex national security. Significant technological advances are being made across a range of fields, including information communications technology (ICT); artificial intelligence (AI), particularly in terms of machine learning and robotics; nanotechnology; space technology; biotechnology; quantum computing, to name but a few. These breakthroughs are expected to be beneficial but highly disruptive and therefore bring about major transformative shifts in how societies function (Kelley, 2019).

Over the years, ICT has played a very vital role in managing insecurity and other related issues across the globe. In developed nations like the United States, Russia, and Israel, ICT has proven to be effective in curtailing threats, even though there remain pockets of infractions, making the deployment of ICT not foolproof (Ekpo and Offiong 2020). A classic example is the terrorist's bombing of the World Trade Center in USA in September, 2011 that took the US security apparatus unawares. Meanwhile, the United Kingdom is ringed with a total of 1.85 million close circuit television cameras (CCTV). The city of London alone boasts of 422,000 CCTV cameras with a camera assigned to every 14 persons (Bassey, 2020). Similarly in developing nations like Rwanda, Ethiopia, South Africa and Tunisia, the advent of ICT has brought tremendous innovation in the management of security challenges via the deployment of emergency communication systems, GPS enabled devices, social networking tools, intelligence monitoring systems, data mining and data base tracking systems, biometric scanners, satellite imaging among others (Katzenstein, 2018).

In Nigeria, there is steady increase in the use of ICT in security administration especially in recruitment and vetting exercises, managing document and personnel security, intelligence acquisition/analysis, critical security operations and safeguarding national security through launching of satellites into space, Subscriber Identification Module (SIM) registration, National Identification Number (NIN), spatial imaging techniques, installation of close circuit television (CCTV) cameras at critical designated places, among others. More so, the heightened insecurity in the country which centers on wanton gruesome killings, kidnapping, terrorism, banditry, economic and financial crimes, criminality, corruption and poor governance among others that pervade the nation, warrants the effective deployment of ICT to ameliorate the debilitating situation.

However, there seems to exist a gap in knowledge on the use and effective deployment of ICTs in curbing the myriads of security challenges in Nigeria (Bassey, 2020). Owing to the dearth of knowledge and expertise in this area within the Nigerian security sector, this paper seeks to highlight the challenges and

prospects of effective deployment of ICT in managing the myriads of security challenges bedevilling the nation today in line with international best practices.

**Conceptual Clarification/Literature Review**

**i. Conceptual Clarification**

**E-governance and its Domains**: Okwueze (2010) opines that e-governance is the public sector's use of ICT with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective. According to Shilubane (2001), e-government is simply the use of ICTs to carry out public services. Put differently, the use of the internet to make sure that services are delivered in a much more convenient, customer-oriented and cost-effective manner. Ayo (2014) also sees e-government as the application of ICT to the process of government functioning in order to achieve a simple, moral, accountable, responsive and transparent (SMART) governance. Similarly, Ojo (2014) sees e-government as the application of ICT by the government to enhance accountability, create awareness and ensure transparency in the management of governmental business. E-government is primarily aimed at improving government processes (e-administration), connecting citizens (e-citizens and e-services) and building external interactions (e-society) (Heeks, 2010). According to Dada (2019), e-government is seen to have four primary delivery tracks namely: Government-to-Citizen or Government-to-Customer (G2C), Government-to-Business (G2B), Government-to-Government (G2G), Government-to-Employee (G2E). From the above perspectives, it can be deduced that e-government is the radical departure from the traditional method of analogue execution of government businesses, to the digitized use of internet of things (IoT), which facilitates efficient execution of government operations, transparent easy access to information and services by the public at their own convenience among others.

**E-administration**: E-administration is a part of e-government which handles internal administration within government, instead of external users such as citizens and businesses. Dyah (2013) sees e-administration as an application using Information and Communication Technology (ICT) to support back-office administrative tasks and operations. He further notes that e-administration is the use of communication technology to support information flow either in or outside the public authority. Heeks (2014) explains that e-administration covers government to government (G2G) relations to improve administrative processes in hierarchical organisation. According to Tejavee (2014), e-administration refers to any of a number of mechanisms which convert what in a traditional office are paper processes into electronic processes, with the goal to create a paperless office. It is the application of ICT to administration with the goal of improving productivity and performance. E-administration can encompass both intra-office and inter-office communication and operations procedure for any organization (Adeyemo, 2020). In this paper, the objective of e-administration is to introduce efficiency, total

transparency and accountability in service delivery and effective management of operations within the security sector in Nigeria.

**National Security:** National Security remains ambiguous, having evolved from simpler state centric definitions that emphasized freedom from military threat and freedom from political coercion to issues of human security. Collins (2018) avers that it could 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. Ellah (2014), opines that national security could be seen as a state of absence of everything and anything that could be a threat to peace, progress, development, tranquillity and wellbeing of the citizenry within a society. According to Katzenstein (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, therefore, is an action or sequence of events that threatens drastically and over a period to vitiate the quality of life for the inhabitants of a state or disrupt governments and citizens lawful transactions.

**Information and Communication Technology (ICT)**: 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, and utilities (programs) among others to manage information (acquisition, dissemination, processing, storage, and retrieval) (Bashar 2017). Bassey (2020) views ICT as those electronic gadgets, equipment, or technologies for creating, acquiring, storing, processing, communicating, and using 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, alongside cutting-edge ICT pieces such as Artificial Intelligence (AI) and robotics and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning (Ugwueze, Onuoha, and Nwagwu, 2016).

## ii. Literature Review

Sharma (2010) opines that the benefits of using ICT tools are: reduction in corruption, building human capacity, reducing cost of governance, and deepening accountability and transparency. He further states that, electronic governance can be operated by three elements: open data, online services and e-participation. According to Anderson (2009), internet and related ICTs have greatly reduced the cost of collecting, distributing and accessing government information. The tools also have been used to create Treasury Single Account (TSA), thereby reducing corruption and issues of "ghost workers", access information, deliver services to citizens efficiently, and promote accountability and transparency especially in the security sector. Besides, the ICT tools also offer means of engaging citizens and participating directly in e-government initiatives (Hughes, 2011). Furthermore, study by Heeks (2014) on the effect of the use of ICTs to promote good governance reveals that, it

can improve government processes (e-administration), connect citizens (e-citizens and services) and build external interactions (e-society).

It results in better data management and retrieval, quick tracking and management of investments in critical infrastructure, inter-governmental sharing of sensitive data and strategic intelligence, monitoring prevailing and emerging security threats, inventory of armament and ordinances, efficient and effective surveillance and tactical operations, deployment of precision counterintelligence equipment (Drones, Satellite Spatial Imaging among others), harmonizing policies and payroll among others (Oketola, 2012). Thus, when ICTs tools are properly aligned with goals of security sector administration, they can help to create gains in both efficiency and effectiveness of operations, public service delivery, and national security (Sharma, 2010).

However, with the ICT-driven Artificial Intelligence (AI) innovations, Kelley (2019) observes that the national security risks it is expected to pose include AI-related strategic competition and related security dilemmas; cyber-security risks to critical AI-dependent systems; consequential convergences with dual-use technologies in biotech, the nuclear domain, and other fields; and the overall unpredictability surrounding AI algorithms and their vulnerability to bias, theft, and manipulation. He further asserts that, one particularly vexing potential tool of manipulation is deepfakes, which are "realistic photo, audio, and video forgeries" that could be weaponized either by the state or enemy entities for devastating information operations. The foregoing mirrors the inherent complexities associated with e-administration in the security sector.

**Methodology**

The study is qualitative descriptive research and relies on documentary method of data collection. The data utilized for the study were gathered from secondary sources including journal articles, government publications, official documents, textbooks, lecture materials, internet among others. This method was employed because it saves time and resources; it gives unfettered access to classified information that may be difficult to obtain through direct personal contact; it allows for increase in sample size above what would be obtainable through interview, questionnaires, Focused Group Discussions (FGD) or other forms of direct observation; and it enables access to archived data that have existed long enough to warrant analyses of socio-political events over time. Given that security studies are often shrouded in secrecy, obtaining critical strategic information from security agents or other stakeholders within the security architecture is often very challenging as they are usually sceptical and economical with detailed factual data that could guarantee accurate scientific conclusion. However, documentary method of inquiry offers the scholar a wide range of prospects that other methods may not guarantee.

**Utilization of ICT in E-administration in Security Sector in Nigeria**

The prevailing pervasive security threats and other challenges in Nigeria are multi-dimensional in nature and scope. Prior to the introduction of Information and Communication Technology (ICT), the Nigerian security architectures have operated largely as bureaucratic, paper-based institutions which usually made the process of information sharing and conducting critical operations cumbersome (Collins 2018). However, with the ICT revolution, there have been increased transparency, efficiency and effectiveness in doing government business as well as conducting operations within the security sector in recent time. The proliferation of digital technology has led to the deployment of sophisticated security systems that can detect and deter threats in real time. These systems have transformed the role of security officers from passive observers to proactive responders. The following are some areas where ICTs are being deployed to improve national security in the country:

i. ***Human Resource Management***: ICT has resulted in enhanced recruitment process, training, efficient deployment and monitoring of personnel work performance. However, 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 (Oghordi, 2014). The dearth of indigenous experts in the production, operations and maintenance of the ICT tools coupled with the fact that a great majority of security operatives are not proficient in the use of ICT tools impedes its efficient utilization.

ii. ***Financial Management***: According to Anderson (2009), internet and related ICTs have been used to harmonize financial system which eliminates double payment and fraudulent practices which has greatly reduced the cost of collecting, documenting and remitting government revenues. The tools were used to create Treasury Single Account (TSA); reducing corruption and issues of ghost workers, double payments of salaries, non-remittance of generated revenues, misappropriation and misapplication of funds, efficient revenue generation and remittances from Nigerian Custom Service, Nigeria Immigration Service and recovered funds from investigations among others. Information about financial transactions can easily be accessed, promoting accountability and transparency in the security sector.

iii. ***Document Security***: This entails effective monitoring and access control to official documents, data and materials. ICT security tools are therefore deployed to protect sensitive and confidential information and materials from unauthorized use, modification, damage, loss or release. Some of the tools include application of code and cypher, encryption among others.

iv. ***Project Management***: The utilization of ICT tools in the security sector has enhanced easy tracking and sundry monitoring of projects, procurement of

critical security equipment, documentation and their deployment at the touch of a button.

v. ***Tracking and Monitoring Illicit Financing***: The security agencies, particularly the Economic and Financial Crimes Commission (EFCC) and Independent Corrupt Practices Commission (ICPC) have deployed extensively ICT tools for tracking, detecting and investigating suspected financial transactions and illicit financial flows. Often, electronic "sniffers" which track and disrupt international fund-transfer networks are deployed. With the introduction of the cashless society, transactions are forced to be done using electronic platforms where suspicious cash movements are identified and flagged (Danfulani, 2013). This has substantially curbed corruption and the financing of activities that constitute a threat to national security.

vi. ***Communication***: Tracking and monitoring communication between and within terror groups, enemy entities, individuals of interest and enhancing interactions within security agencies have been achieved through the deployment of ICT. Several gadgets and technologies are used in establishing effective communication especially during joint security operations such as tagging and tracking information that is/or was communicated by enemy entities. Interception and decoding of enemy radio communications, jamming, radio stealth, and other related areas as well as cryptography methods used to counter such similar interception by enemy entities against government troops, are some of the ICT measures that are in use during critical operations.

vii. ***Reconnaissance Operations***: The Nigerian military, particularly the Airforce and Navy, have their aircrafts and warships equipped with ICT tools that cover a wide range of areas such as, detection of and avoidance of detection by radar and sonar systems, jamming of communication systems of threat entities/criminal minds. Other tools include signals that can allow own troop in a war theatre to use the enemy stations for a misinformation campaign, computer hacking, wiretapping and listening into and monitoring telephone conversations/communications of threat entities (Akiyode, 2016).

viii. ***Surveillance***: Computer surveillance involving the monitoring of data and traffic - phone calls and broadband internet traffic (emails, web traffic, instant messaging, among others) are available for unimpeded real time monitoring by law enforcement agencies. So many forms of technology are deployed such as surveillance cameras, social network analysis, biometric surveillance, data mining and profiling, corporate surveillance, satellite imagery, geolocation devices. Satellite and navigation systems, and remote surveillance are used across various geographically distant locations either for real time security operations or information gathering purposes. Also, navigations are 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 and Moore, 2002). These systems have proven very valuable in collating intelligence for combating crimes as well as used to signal to citizens in a timely manner in cases of emergencies like flash floods by the Nigeria Meteorological Agency (NiMet).

ix. ***Intelligence Gathering***: ICT tools are used in acquiring information (especially open-source intelligence) that has the potential to enhance national security. The internet, print, and electronic media are useful in providing useful information which when processed as threat and trend analysis, assists greatly in the nation's security efforts. ICT is also deployed for market survey analysis - monitoring prices of goods and services, economic programs and inflationary trends, policy performance and feedback, political activities, maritime surveillance by the Nigerian Navy, NIMASA, NSCDC to checkmate oil theft and deep blue water crimes among others. Call records from mobile phone service providers also help in tracking felons via call record analysis and geolocation tools in conjunction with mobile network providers in Nigeria (Muhammed-Nasiru, and Kasimu, 2012).

x. ***Effective Security Coordination***: The use of cutting-edge technology to centralize and coordinate the entire Nation's data, acts 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 domiciled in the office of the National Security Adviser (ONSA) for effective command, control and coordination of strategic security operations as well as enhancing inter-agency cooperation which has yielded substantive results (Akiyode, 2016).

xi. ***Identification***: Unifying various identification initiatives plays a significant role in national security especially with the existing DNA, facial recognition, and fingerprinting technologies. The introduction of the fingerprint authentication system for the procurement of driver's license, SIM card registration, National ID registration, examination registration and election process, mobile banking among others have, therefore, assisted the security architecture in tackling sundry threats to national security (Raphael and Stoke, 2018).

xii. ***Use of Lawful Interception***: Under the Nigerian Communications Act (NCC, 2019), operators in the telecommunications space are required to install equipment with interception capability that allows law enforcement agencies on the occurrence of any public emergency or in the interest of public safety to access communication data. Lawful interception (LI) is the legally sanctioned official access to private communication such as telephone calls, e-mail messages among others (Heeks, 2010). The security agencies leverage on this regulation to monitor a greater number of individuals under suspicion, while the information of non-targeted individuals remains private.

xiii. ***Social Networking Tools***: This enables community members to be connected to the internet and actively create and share contents in their own time. Security agencies leverage on social networking tools to share security news, strategies and receive feedback particularly by the Nigeria Police Force engagement in community policing and the Joint Task Forces engaged in counterterrorism and sundry security operations (Duru and Anigbata, 2015).

**Challenges of Application of E-governance to Security Administration in Nigeria.**

According to Camino and Cornish (2019), the advances in ICT portend significant social and economic benefits, increased efficiency, and enhanced productivity across a host of sectors. But there are mounting concerns that these technologies and how they are used are posing serious challenges, including labour force dislocations and other market disruptions, exacerbated inequalities, and new risks to public safety and national security. The technologies are mostly dual use, in that they can be used as much to serve malicious or lethal purposes as they can be harnessed to enhance social and economic development, rendering efforts to manage them much more complex. Bassey (2020) collaborates that as e-governance is celebrated globally because of its sterling benefits, it has corresponding potential debilitating threats that came with it. These threats are discussed hereunder:

i. ***Increasing Rate of Cybercrime/Internet Fraud***: All the information in the whole world is stored in global web pages. Thus, with a click of the mouse, an outsider can study, hijack, corrupt or track the system inside his/her room. Once top secret and confidential information of a nation or critical infrastructure or organization is divulged or compromised, that nation or organization will have all its confidential documents and activities seriously endangered.

ii. ***Inadequate ICT Infrastructure***: The effective implementation of e-administration initiatives in Nigerian security sector, faces some technological difficulties such as lack of shared standard and compatible infrastructure platforms among departments and agencies. For a sound transition to e-governance to be actualized, a uniform guiding set of principles, models, ICT platforms and standards for the security agencies are needed. However, this fundamental aspect of efficient coordination of electronic governance application is yet to be adequately established.

iii. ***Accessibility***: A great number of security operatives and citizens in the remote parts of the country cannot access or disseminate vital government information via internet due to poor or non-existent internet service. When the security operatives are constrained in their interaction with community stakeholders via ICT tools and citizens most of who cannot operate ICT tools would not be able to access the vital information provided for their consumption and utilization, it thwarts the very fundamental and cardinal objectives of the e-governance and e-administration particularly in the area of community policing.

iv. ***Cost Implications***: Some of the ICT tools deployed for security operations are very expensive and costly to maintain. Given the pervasive contemporary security threats across the nation, the need to acquire sophisticated ICT security equipment to tackle the debilitating situation with the concomitant upgrade calls for concern given the lean purse of the government.

v. ***False Sense of Transparency and Accountability***: Critics of e-governance argue that online governmental transparency is very dubious because it is maintained by the government themselves. Incriminating information can be systematically added or removed from the data base without proper notification of the citizens. This is more so as the activities within the security sector are hardly open to monitoring and probe, negating proper accountability and transparency.

vi. ***Inadequate Partnership and Collaboration***: There is the need for regional partnership and international collaborations in order to ensure global best practices in e-administration and exchange of critical information particularly on prevailing and emerging security threats. This is a challenge to the Nigerian security sector and need to be remedied in order to accomplish the desired results. The need to intensify partnership and collaboration with advanced nations and ICT entities is therefore desirable.

vii. ***Hyper-Surveillance***: Increased contact between government and its citizens interacts both ways. Once- e-governance begins to develop and becomes more sophisticated, citizens will be forced to interact electronically with the government on a larger scale. This could potentially lead to a police state and lack of privacy for citizens, as the government obtains more information on them that could be deployed for sinister and or unsavoury purposes.

viii. ***Lack of ICT Maintenance Experts***: Currently, there is dearth of qualified service personnel and experts that could handle the entire digitization of the security sector and sustain continuous maintenance of the existing ICT tools. This has necessitated the need to fall back on foreign experts who have no qualms compromising the nation's security sector through e-administration. This is a huge challenge to the development of e-administration within the security architecture.

ix. ***Lack of Political will on the Part of Government***: The government has not demonstrated enough political will toward mainstreaming the security sector in the global web pages which has slowed the pace of e-administration in the security sector. This is evident where some important and highly sensitive information are still documented in paper form in the official files prone to easy compromise, but they could have been stored in a more secured retrieval system using ICT tools.

x. ***Insufficient ICT Training***: Training is the most and veritable tool of ensuring the sustenance of e-administration in the Nigerian security sector. Very few security personnel have been trained in sophisticated computer application to drive the e-administration in the security sector. For any country to ensure that it achieves e-administration option, a great majority of personnel should be computer literate and are periodically updated to cope with the ever fast evolving ICT revolution.

xi. ***Resistance to Change***: Issues related to uncertainty, fear of job security, privacy intrusion, different agencies' operational tradition, cultural barriers as well as government's slow pace in ensuring citizens' involvement in providing easy and affordable access to basic ICT tools, are huge challenges to e-governance in the security sector.

xii. ***Inadequate Electricity Supply***: According to The *Punch Editorial* (2023), Nigeria has the potential to generate 14,000 MW of electric power but dispatches paltry 4, 803 MW which is insufficient for a country of over 200 million people. Currently, only 45% of Nigeria's population is connected to the energy grid while power supply difficulties are experienced around 85% of the time and almost non-existent in certain regions. This is a huge challenge for the deployment of ICT tools that require constant electricity power supply to function efficiently.

xiii. ***Inadequate Compliance to TSA Directives***: It was a move marked by so much resistance at first due to the pervading nature of corruption and difficulties in adapting to changes in the public sector which still persists (Oyedokun, 2017). Before the advent of TSA, government agencies operated several accounts in commercial banks that were not only untraceable but bred corruption. Akpan *et al*, (2021) note that, at least about 20,000 accounts belonging to Ministries Departments and Agencies (MDAs) in commercial banks were closed. The closure of these accounts and subsequent elimination of ghost workers saved the government N24 billion monthly. Also, the government is said to be in better control of its inflows, since it comes in through a single channel powered by a Fintech solution - Remita. The situation in the security sector shrouded in secrecy and allegations of financial impropriety leaves much to be desired. At the national level, frequently erring agencies like the Nigerian Immigration Service (NIS), Nigerian National Petroleum Corporation (NNPC), Federal Road Safety Corps, Nigeria Customs Service, INEC, Nigeria Police Force and several Federal Universities among others scuttle the envisaged policy gains (Aderopo and Nlebem, 2019).

**Conclusion and Recommendations**

E-governance majorly entails the effective deployment of Information and Communication Technologies (ICTs) to reduce personnel costs, minimize complexities of procedures and processes of doing government business particularly

in the security sector. There is evidence that the Nigerian security sector is adapting to e-administration in its human resource management and security operations. However, there are certain subsisting challenges, such as dearth of qualified ICT experts and quality ICT infrastructure within the security sector, unstable electricity supply, inadequate comprehensive internet access, cyber security threats, insufficient capacity building and political will among others. Notwithstanding these glitches, there are opportunities for the government to promote e-governance particularly in the security sector, by improving ICT infrastructure, increasing broadband penetration of internet usage, intensifying human capacity building, encouraging indigenous participation in the production/Maintenance of ICT tools and implementing cyber security international best practices.

Based on the challenges identified above, the following recommendations are advanced:

i. There is the need for value reorientation and attitudinal change. The security sector should engage in full digitization of their human resource and operations management. There should be concerted efforts at value reorientation and change of attitudes of security personnel towards the use and efficient maintenance of available computer systems.

ii. Nigeria's security architecture should show a high level of e-readiness in their operations. The government, should ensure that all high commands, tactical operation bases and offices are equipped with functional ICT-driven equipment, employ highly skilled personnel in ICT, make provision for continuous training of the personnel to keep them informed on how best to utilize e-administration in engendering effective service delivery among others.

iii. Adequate funds should be budgeted for installation of requisite ICT infrastructure. The government should provide the critical ICT infrastructure like robust broadband services, required internet network and the availability of constant stable power supply, which has been identified as one of the major challenges against application of e-governance in Nigeria especially, in the security sector.

iv. Security of government ICT infrastructure and information - fiber optics, portals, and other ICT backbones should be adequately protected from vandalism/theft, while sensitive information and equipment should be sufficiently protected from cyber criminals through top notch security technology like several layer passwords, cryptography, operational technology, and monitoring /surveillance tools among others.

v. The resistance to change due to envisaged job loss, pervasive nonchalant attitudes of Nigerian workers among others should be decisively addressed. Similarly, most of the available ICT facilities in government offices are

underutilized. There is, therefore, the need to address the systemic challenge so that the ICT facilities emplaced by government should be put to good use.

vi. The government should also enact and implement Information and Communication Technology (ICT) laws that will make computer literacy a compulsory aspect for every public or civil servant both at the local, state and federal levels. Such policies should also involve the adoption of effective ICT awareness, with computer-related literacy training programmes made compulsory in security training institutes and also in the nation's primary, secondary and tertiary institutions.

vii. The security agencies in carrying out their statutory responsibilities, should ensure the maintenance of citizens' privacy rights in line with global best practices.

viii. Concrete efforts should be made to ensure information security: The ease with which sensitive government information are hacked and divulged calls for concern and should be checked. This can be done through proper vetting of individuals that custody or have access to sensitive information, appropriate periodic pass-wording and encoding of confidential information/data, as well as effectively entrenching the Official Secrets Act of 1963 (Revised, 2021) (need to know principles) to hinder unauthorized access to sensitive public information.

ix. There is the need to ensure that ICT tools are affordable to citizens by government deliberately intervening in the control of outrageous prices of ICT tools, while encouraging the production of same by indigenous players in the sector making waves outside the country. This will obviously minimize the digital divide as it will afford the citizenry unhindered access to ICT to enhance government-citizens' easy interactions, particularly their engagements in community policing.

**References**

Aderopo, K. and Nlebem, A. (2019). Appraising the success of Nigeria's Treasury Single Account*, BusinessDay*, February 15.

Adeyemo, A. B. (2020). E-government implementation In Nigeria: An assessment of Nigeria's E-government ranking. *Journal of Internet and Information System.* 2 (1): 11-19.

Akiyode, J. (2016). Nigeria's ICT industry: 2015 review in view of 2016 developments. *Businessday*, www.businessday online.com, accessed on 5/9/2023.

Akpan, C. O., Akpan, D. C., and Bassey, S. A. (2021). Menace of street urchins in Nigeria. *Pinisi Journal of Arts, Humanity and Social Studies* 5 (3).

Anderson, T. B. (2009). E-government as an anti-corruption strategy. *Information Economics and Policy,* 21: 201-‘10.

Ayo, C. K. (2014). Information and communication technology as a lever for innovation in leadership. *Mediterranean Journal of Social Sciences*, 7(6): 363-374.

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. *Pinisi Journal of Art, Humanity and Social Studies*. 1(19).

Camino K. and Cornish P. (2019). Preventive diplomacy, ICT and inter-state conflict: A review of current practice with observations. *Swiss Federal Department of Foreign Affairs*.

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

Dada, D. (2019). The failure of e-government in developing countries. A literature review. *The Electronic Journal of Information Systems in Developing Countries*. 22 (3).

Dyah, P. (2013). *Analysing e-Administration in Developing Countries: Challenges and Best Practices in the use of ICT for Development*. The University of Manchester.

Danfulani, J. (2013). E-governance: A weapon for the fight against corruption in Nigeria. *Sahara Reporters* (Online) Available: http://saharareporters.com/2013/08/10/e- governance-weapon-fight-against-corruption-nigeria-john-danfulani-phd. (Retrieved October 5, 2023).

Duru, E., and Anigbata, D. (2015). *Public administration: A conceptual approach*. Abakaliki: Felico Press.

Ekpo, C. E., and 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.

Heeks, R. (2014). Understanding e-governance for development. *Government Working Paper Series*, Paper No 11. Manchester Institute for Development Policy and Management. University of Manchester.

Heeks, R., (2010). *Achieving Success/Avoiding Failure in E-government Projects*, IDPM. University of Manchester.

Hughes, M. (2011). The challenges of informed citizen participation in change. *Transforming Government People, Process and Policy,* 5: 68-86.

International Data Corporation (IDC). 2015 Report. National ICT Policy.

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

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

Kelley, M. S. (2019). Artificial Intelligence and National Security. *Congressional Research Service*. January, 11. https://fas.org/sgp/crs/natsec/R45178.pdf. Accessed on 25/10/23.

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

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.

Nigeria Communication Commission (NCC) (2019, January 23). The Lawful Interception of Communications Regulations (the "Regulation").

Official Secrets Act (1963). Revised, 15th April, 2021. Abuja: Government Printing Press

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

Ojo, J. S. (2014). E-governance: An imperative for sustainable grassroots development in Nigeria. *Journal of Public Administration and Policy Research*, 6 (2): 77-89.

Oketola, S (2012). Electronic Participation of Citizens and the Business Community in e-Government. Study on Behalf of the Federal Ministry of the Interior, Division IT 1 Nigeria.

Okey Chikeleze (2023). E-governance in public sector, lecture notes on PUB 813, ESUT.

Okwueze F. O. (2010). E-governance as a tool for public sector development in Nigeria. Nsukka: *Society for Research and Academic Excellence.* http://academicexcellencesociety.html. Accessed on 14/09/23.

Olaopa, T. (2014). Seminar on Sharing Success Stories and Challenges in E-Governance/E-Administration. http://www.cafrad.org/Workshops/Tanger21-23_04_14/olaopa.pdf. Accessed on 04/11/23.

Oyedokun, G. E. (2017). Imperative of treasury single account (TSA) in Nigeria. http://papers.ssrn.com/sol3/papers.cfm. Accessed 24/4/ 2023.

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

Raphael, S. and Stoke, D. (2018). Energy Security. In A. Collins (Ed.) *Contemporary Security Studies*. Oxford: Oxford University Press.

Sharma, P. (2010). *E-Governance*. New Delhi. APH Publishing Corporation.

Shilubane, J. (2001). E-government: An overview, service delivery review. *A Learning Journal of Public Services Managers.*

Tejavee, S. (2014). E-governance and effective deliverance of information and services to citizens architecture, *International Journal of Computer Science and Information Technologies*, 1(4).

*The Punch* (2023, October 9). FG Grows National Grid Power Capacity. Editorial