Introduction

Globally, insecurity is a multifaceted issue that threatens peace, security, and human rights. Acts of terrorism often transcend national boundaries and ideologies and target innocent civilians without distinction, resulting in civilian deaths, psychological distress, and widespread anxiety. In addition to the direct losses of life, insecurity damages the fabric of society by undermining confidence in institutions, polarizing society, and hindering social cohesion. In recent years, the Middle East has seen a surge in the number of terrorist groups operating in the region. This is largely due to the proliferation of Al-Qaeda and other extremist groups in countries such as Syria, Iraq, and Yemen, as well as the rise of Al-Qaeda in Libya (Sahal, 2021). The region's instability has been caused by a variety of factors, such as political unrest, sectarian conflict, poor governance, and economic disparity. In South Asia, terrorism has been a major issue, especially in Afghanistan and Pakistan. The conflict in Afghanistan and the presence of the Taliban and other terrorist groups in the region have created a breeding ground for terrorism around the world. In addition, the ongoing conflict between India and Pakistan has resulted in several terrorist attacks across the border. South Asia continues to have the lowest average GTI score in 2022. There were 1,354 terrorism-related deaths in the region in 2022, down 30 percent from the previous year (Ijide, 2024)

Europe has experienced a series of high-profile terror attacks. Many of these attacks have been carried out by jihadi groups, with many of them claiming to be acting on behalf of the terrorist group known as the Islamic State (IS). Attacks in countries like France, Belgium, and the UK have left a trail of destruction, calling into question the security architecture of the European Union and raising questions about integration, radicalization, and counter-terrorism strategies. Southeast Asia has not seen the same level of terrorism as other parts of the world, but it has seen its share of

major incidents. Terrorist attacks in countries such as Indonesia, the Philippines, and Thailand have been carried out by groups such as Jemaah Islamiyah (JI) and Abu Sayyaf. In addition, the rise of the Islamic State (IS) and its recruitment and radicalization campaigns have affected the region (Malik, 2024).

Africa remains a continent of promise and enduring challenges. Many African countries are becoming increasingly unable to provide security to their citizens, and in some instances, states themselves have become sources of insecurity. The security landscape in Africa is rapidly changing with security threats that are becoming increasingly multifaceted, dynamic, intertwined, and complex. The occurrence, severity, and duration of these security threats are exacerbated by the effects of global megatrends acutely manifested in Africa. Besides the changing security threats, the concept of security is dissociating from state and regime-centric and evolving towards human security. Despite these dynamics and changes in the security landscape, many African countries continue to use traditional approaches to address these security threats. For Africa and its security leaders to effectively deliver sustainable security to their citizens, there is a need to move away from the "business-as-usual" approach to more proactive and strategic approaches (Abiodun, 2020).

The incidences of insecurity in Nigeria have placed the country at a crossroads. In the days of the military, most Nigerians and political analysts had thought that with the entrenchment of democratic government, the country would be crisis-free, there would not be ethno-religious and socio-political squabbles. Experiences so far have ironically revealed that the nation's harvest reverses in its socio-political and material fortunes. Nigeria and Nigerians have become more vulnerable and fragmented than hitherto. The failure of the earlier generation of leadership to

contain the various forms of insecurity manifesting itself in the country that independence bequeathed to them prompted the civil war of 1967 to 1970 and partially led to the avoidable and worrisome 29 years of military incursion (Muzan, 2014).

The security agencies in Nigeria are struggling to combat the menace of insecurity; the country's security architecture has arguably been hijacked by terrorist and insurgent groups like Boko-Haram and local armed militia groups like herdsmen in many parts of the country. The insecurity challenges have grounded governance and socio-economic activities across the nation (Malik, 2024). Even the telecommunications industry is affected by the insecurity challenge as operators lose infrastructure, employees, and revenue to the menace. Thus, the preponderance of armed banditry, kidnapping, terrorism, ethnic militancy, secessionist agitation, and the destruction of oil installations is are clear manifestation of a failed national security. In the current era of globalization, where crime networks increasingly transcend national borders and exploit advancements in science and technology, criminality has become a transnational phenomenon (Okene, 2010)..

Security plays a pivotal role in the national and economic development of any country, while its absence is capable of cascading and causing serious upheaval in various geopolitical zones as well as the well-being of the country. Insecurity is the bane of Nigeria's problem, and it has remained so since the pre-independence era (Comolli, 2022). Though there had been a paradigm shift from the kind of security challenges experienced in the pre-independence era to what is witnessed today. The current democratic dispensation needs to seek solutions to these menaces. Aside from the divisive legacies left behind by the British colonialists, most actions and behaviours of Nigerians now pose an even greater danger to effective national security.

If there are tools in the world that nations have used over time to combat different challenges they face in the cause of history, technology should be the major. Countries like the United States, Germany, China, India, Russia, and France have used technology to gain prominence and maintain relevance in the international system (Offiong, 2024). Leaders in the developed countries are setting up integrated frameworks to allow them to adopt and deploy technology, particularly Artificial Intelligence (AI), to improve and strengthen their national security infrastructure. In the emerging field of AI, modern tools like surveillance cameras, social network analysis, biometric surveillance, data mining and profiling, corporate satellite imagery, and Geolocation devices have become available to combat insecurity.

Nigeria, in this regard, is disadvantaged due to its inability to invent, produce, and have in its possession the latest technology a country needs to tackle its security challenges (Offiong, 2024). Instead, Nigeria depends on the importation of security gadgets to enhance rapid response to insecurity. According to Ijide (2024), technology is one of the areas affecting the capability and the strength of the security agencies in Nigeria. One clear example of the gap in technology is in the fact that kidnappers can hold their victims in captivity for many days while arranging for ransom via mobile phone calls and without quickly and effectively nipping it in the bud through tracking devices and other technological devices.

By leveraging cutting-edge technologies, the state can make room for proper cooperation and coordination amongst security agencies to lessen duplication of efforts, guard against the mishandling of information as well and enhance intelligent gathering among the different agencies. “Although deplorable, herdsmen attacks, kidnapping for money or ritual killings, ethnic cleansing, cybercrimes, human/material trafficking, and endemic acts of corruption are the realities today.

Now is the time for leaders to wake up to the realization of the need to mobilize resources, human, financial, and technological, to address the diverse issues of national insecurities. The paper, therefore, examines technology and National security in Nigeria.

Conceptual Clarifications

National Security: National security refers to the comprehensive measures adopted by a sovereign nation to safeguard its territorial integrity, political stability, citizens' welfare, and strategic interests from both internal and external threats (Abiye, 2023; Sanni, 2024). It encompasses the protection of lives, property, institutions, national values, and the sustainable functioning of the state in the face of political, economic, social, or technological challenges.

According to Adebayor (2024), the term *national* relates to matters affecting an entire nation, especially in contrast to foreign entities. Security, as defined by Olu (2024), involves the condition of being protected from harm, danger, or threat, while Hornby (1995) adds that it encompasses all activities aimed at preventing attack or harm to people and places. When combined, national security entails a strategic blend of policies, intelligence, and institutional frameworks designed to preserve a country's sovereignty and ensure the well-being of its people (Okeke & Ayodeji, 2021).

National security today transcends mere military defense; it includes economic resilience, cybersecurity, public health, environmental safety, and diplomatic relations (Usman, 2023). A nation's security, therefore, reflects its capacity to anticipate, prevent, and respond to both traditional and non-traditional threats in a manner that ensures long-term peace, stability, and development. In this regard, national security serves as both a prerequisite for governance and a benchmark for national performance in the global arena.

Technology: technology refers to the tools, systems, or methods that are developed and used to solve problems, improve processes, and enhance human life (Jerome, 2015). According to Kumar (2019), technology consists of two primary components: a physical component, which comprises items such as products, tooling, equipment, blueprints, techniques, and processes; and the informational component, which consists of know-how in management, marketing, production, quality control, reliability, skilled labour, and functional areas. Sahal (2021) views technology as 'configuration', observing that the transfer object (the technology) relies on a subjectively determined but specifiable set of processes and products. The current studies on the technology transfer have connected technology directly with knowledge, and more attention is given to the process of research and development (Dunning, 2024).

By scrutinizing the technology definition, there are two basic components that can be identified: knowledge or technique, and 'doing things. Technology is always connected with obtaining certain results, resolving certain problems, completing certain tasks using particular skills, employing knowledge, and exploiting assets (Lan and Young, 2020). Technology, for this study, is the practical application of scientific knowledge to solve real-world problems and improve human welfare

Theoretical Framework

The paper is theoretically anchored on the cybernetic theory by Norbert Weiner propounded in 1948. Cybernetics is the study of human-machine-like interaction guided by the principle of feedback, control, and communications. It compared human interaction to that of a machine, which functions when given a task to perform. Weiner (in Agbodike and Igbokwe-Ibeto, 2017) coined the term cybernetics to incorporate his idea into the existing transmission theory that

people sent messages within a system in an effort to control their surrounding environment. Cybernetics is characterized by the notion of control and feedback, which is the underlying principle of the technological world.

Wiener (1948) took the concept of control and feedback principle as it pertains to electronics to propound the theory of cybernetics, which has inspired a generation of scientists to think of computer technology as a means to extend human capabilities. This principle allows for various systems to be controlled in a way that deals with undesired signals, which helps improve system stability. In simple terms, the idea behind cybernetics is that human beings, just like machines, perform or act based on commands given to them from the environment to have perfect control of the environment. To Weiner, therefore, technology is a tool that every organization and system needs to survive in its environment.

This theory directly applies to the focus of this work, which centers on the use of modern security technologies to improve crime detection, surveillance, and intelligence operations. Cybernetic theory emphasizes that effective systems, whether mechanical or organizational, must incorporate feedback mechanisms for continual adjustment and decision-making. In modern security architecture, technologies such as surveillance cameras, biometric devices, artificial intelligence (AI), and data analytics systems function by receiving inputs (e.g., real-time crime data, behavioral patterns, threat indicators), processing them, and providing outputs (e.g., alerts, reports, heatmaps) that inform further human or automated responses.

In the fight against insecurity, this theory sees security organizations and their environment as a closed-loop system, where the information (output) of an organization to the environment is analyzed and returned as feedback (input) to the same organization. This process enables law

enforcement and security agencies to continuously improve their strategies. Technologies like Geographic Information Systems (GIS), drones, facial recognition software, and crime prediction models rely heavily on feedback loops to adapt to changing criminal tactics and social behaviors. Thus, cybernetic theory provides a conceptual foundation for understanding how technology enhances institutional responsiveness and precision in combating insecurity.

Moreover, by treating criminal behavior patterns as data-driven signals within a system, cybernetics offers a framework for developing predictive policing and preemptive intelligence strategies. This allows security agencies to shift from reactive to proactive measures, using real-time surveillance and analytics to intervene before crimes occur. Cybernetic theory, therefore, supports the integration of automated decision-making processes into security management, ensuring not only effective control but also adaptability in a volatile and complex security environment. The theory thus beams a searchlight on the usage of technologies in collecting and managing data for surveillance, intelligence management, and the prevention, detection, and countering of crime in society. It provides a robust theoretical foundation for appreciating the transformative role of digital innovations in modern security practices.

Security Situations Across the Globe

Terrorism around the world has a long history that dates to many different eras and events. Some of the first examples of terrorism were carried out by Jewish extremist groups during the 21st century. The Sicarii were a group of Jewish radicals who attacked Roman officials and Roman collaborators as part of their campaign against the Roman occupation of Judea. The Sicarii were one of many groups that carried out terrorist activities throughout history. There were anarchist movements during the late 1800s and early 1900s, as well as separatist movements in various

regions. Political assassinations were also carried out by groups or individuals with ideological or nationalist motives. Terrorism can take a variety of forms, including bombing, armed attacks, kidnappings, and hostage-taking. It can also target civilian populations, state actors, and public infrastructure. On a global scale, terrorist attacks and fatalities are rare. However, this is not the case in every country. Attacks are common in some countries and on the rise in others, while in others they are rare or non-existent. In addition, terrorism is a major concern for people around the world. While attacks are rare, they are often shocking as they are designed to frighten and control. (Lan and Young, 2020)

The current era of global terrorism, however, traces its roots back to the late 1980s and early 1990s. Significant events played a significant role in shaping the current landscape of terrorism. One of those events was the Iranian Revolution of 1979, which ushered in the rise of radical Islamic ideologies. The U.S. embassy in Tehran was stormed by Islamic radicals who took Americans hostage. The attack highlighted the growing power and influence of radical groups. Other major terrorist groups emerged in the 1980s and 1990s and carried out major attacks. The war in Soviet-Afghanistan created fertile ground for jihadi movements, with Al-Qaeda emerging as a major player. Al-Qaeda's use of terror tactics in its campaign against Soviet forces brought global attention to the idea of global terrorism (Lan and Young, 2020)

Al-Qaeda, under the leadership of Osama bin Laden, carried out a series of high-profile suicide attacks across the United States. The attacks targeted iconic landmarks such as the World Trade Center and the United States military base at Quantico, Virginia. The attacks killed almost 3,000 people and left a trail of fear and uncertainty across the globe. The events of 9/11 led to a worldwide shift in focus toward counter-terrorism measures and an increase in international

cooperation to fight terrorism. Since 9/11, terrorism has continued to affect nations all over the world in various ways. The impact of terrorism is not limited to the immediate victims of attacks; it also creates a ripple effect that affects societies, economies, and international relations. One significant effect is the erosion of personal freedoms and civil liberties as governments institute security measures to protect their citizens. Increased surveillance, increased security at airports and other public spaces, and the implementation of stricter immigration policies are all examples of measures undertaken by governments in response to terrorism (Offiong, 2024).

Terrorism also has a negative economic impact, as it disrupts trade and investment. As a result, countries affected by frequent terrorist attacks often lose out on foreign tourism and investment, hindering their economic development. Furthermore, the cost of increased security measures and reconstruction and recovery after an attack can be substantial and put strain on government budgets. In addition, terrorism has a psychological impact on populations. Acts of terrorism can cause fear and trauma, which can lead to heightened levels of anxiety and insecurity among people. These anxieties can have long-term effects on psychological health and can influence public perceptions and policy responses (Ijide, 2024). Global terrorism is constantly changing and continues to present challenges to countries around the world. Social media and the internet have enabled the spread of radicalized ideologies, allowing terrorist groups to recruit recruits, spread disinformation, and plan attacks more effectively. Lone-wolf attacks, which are carried out by self-radicalized individuals who carry out attacks on their own, have become more common, making it harder for intelligence agencies to identify and stop acts of terrorism (Ijide, 2024).

In response to the global terrorism threat, countries have adopted a variety of measures to reduce the risks. National cooperation has become a priority, with countries sharing intelligence and working together to dismantle terrorist networks and fund terrorism. Border security measures, including tightening immigration controls and enhanced screening at airports and seaports, are aimed at preventing the cross-border movement of terrorists and illegal substances. Preventative measures have also been adopted to combat radicalization and extremism, such as education and community outreach. To sum up, global terrorism has a long and complicated history and is rooted in a variety of ideological, political, and religious causes. Its impact on countries around the world has far-reaching consequences, affecting economies, societies, and people's mental health. Combining security measures with root causes and inclusivity strategies is the only way to fight global terrorism and build a safer, more secure world.

Security Situations in Nigeria

Nigeria is faced with a lot of security challenges, such that the situation has become embarrassing and a dent on the nation's image, it has also threatened the sovereignty of the Nigerian state. These challenges are deeply rooted in structural weaknesses such as endemic corruption, mismanagement of national resources, youth unemployment, poverty, state failure, and entrenched ethno-religious divisions (Eme & Anthony, 2022). These underlying factors have created fertile ground for the emergence and sustenance of various insurgent, terrorist, and separatist groups across the country (Eme and Anthony, 2022). The biggest security threat facing Nigeria today has been that of insurgency and terrorism since the return of civil rule in May 1999. The activities of terrorists started historically with the movement to liberate the Niger Delta people led by Major Isaac Jasper Adaka Boro and which gave birth to a group known as the Niger Delta

Volunteer Force (NDVF), a terror military group composed of Boro's Ijaw tribesmen. In February 1966, the group declared the Niger Delta Republic, which was later crushed by the Federal military forces and Boro was arrested. Muzan (2014) also declared the 6 July 1967 to 15 January 1970 Nigerian civil war, or what is also known as the Biafra war, as another earliest forms of insurgency in the country.

Many years later, other forms of insurgencies appeared in the Southern parts of Nigeria, like the Movement for the Actualization of the Sovereign State of Biafra (MASSOB), formed by Ralph Uwazurike, a lawyer and human rights activist. MASSOB was formed in 1999 to resuscitate the aims and objectives of the failed Republic of Biafra agitation. The same ambition is what characterized the activities of the Indigenous People of Biafra (IPOB) under the leadership of Mazi Nnamdi Kanu. They are all calling for the secession of Biafra, and they have unleashed terror on the people of the Southeast (Ibrahim, 2023).

Other terror groups like Ateke Tom and Mujahid Asari Dokubo's Niger Delta People's Volunteer Force saw to the creation of a movement known as the Movement for the Emancipation of the Niger Delta (MEND), both from the Niger Delta sub-region of Nigeria. In 1997, there was the emergence of a Yoruba nationalist group known as the Oodua People's Congress (OPC), founded by Dr. Fredrick Fasheun, with its militant arm led by Ganiyu Adams in the South West region of the country (Mohammed & Abdulhamid.2019)

The northern zones of the Nigeria were not immune against the geometric rise of violent crimes during this period with the zones taken over by brutal intra-religious crises between various Islamic sect that refused to accept each other's kind of Islam. There are also the challenges of Arewa Youth Congress (AYC) in the north. The activities and unrest caused by the AYC are

similar to those of the insurgents. Similarly, the activities of Islamic Movement of Nigeria, otherwise known as the Shi'ite movement, led by Sheikh Ibrahim el Zakzaky, have caused serious unrest in some selected states of the north (Muzan, 2014; Mohammed & Abdul Hamid, 2019)

The coming into public glare of the Boko Haram insurgency in 2009 seems to have demystified all possible solutions proffered by the Nigerian government. This group has become so antagonistic and a dangerous threat to the people and security agents in Nigeria. To this end, Afegbua, (2017), have argued that insurgency in all its forms, either from the BH, bandits and herders' attacks or militancy both in the northern and southern regions of the country, the safety of lives and properties and the future of the country have been put to test or danger since the emergence of these groups in the country. The emergence of Boko Haram in 2009 has worsened the security threats and posed a security challenge. BH terrorists operate in their deliberate style of inflicting fear by way of planned attacks to weaken the government and undermine the sovereignty of the country.

Attacks on people, communities, and infrastructures by terrorist organizations have imposed fear and tension around the world and in Nigeria in particular. There are different terror organizations in Nigeria with different ambitions that carry out terrorist attacks within the country. Some harbour secessionist ambitions (IPOB, MASSOB, Afenifere), some seek bigger shares in the national cake (Niger-Delta Avengers), while the religious groups are agitating for the implementation of sharia law (Maitatsine, Boko Haram). With the global rise in terrorism, terrorist activities are today classified as a foremost menace to global peace and security. This has led to transnational cooperation among international security agencies to gather information on the causes and the implications of terrorism on people and the country. A closer analysis reveals that

these security crises are not merely ideological or ethnic, but are deeply rooted in **socioeconomic** alienation, political exclusion, inter-group rivalry, and state incapacity. The high rate of youth unemployment, widening inequality, lack of civic education, and poor access to social services continue to feed radicalization and armed resistance. Moreover, the corruption and politicization of security institutions have eroded public trust in the state's ability to protect its citizens.

Technology and National Security

There is no doubt that modern technologies have aided and promoted peace, security, and development across the globe. The emergence of these technologies has created new opportunities in the areas of peace, security, and development, especially in conflict prevention, peace operations, peace peacebuilding. Modern technologies have also made it possible to collect data in crime and conflict, enhancing the efficiency of early warning and response. Peace operations can now be implemented in an asymmetric threat environment, and monitoring and observation can be performed more efficiently as a result of this advancement. Modern technologies, particularly with the advent of the Internet and mobile phones, have greatly expanded opportunities for ICTs to support sustainable development, prevent conflict, improve humanitarian action, and transform state-society relations have greatly expanded. Technology is now integral to security. CCTV, access control systems, and alarms, as well as integrated IT management systems, can support the security operation to keep organisations and their people safe.

The UN Mission in Sudan (UNMIS) was the first instance where a Security Council Resolution (1706) explicitly called for ‘aerial means’ and ‘aerial reconnaissance’ to be used to help protect civilian populations (UN Security Council 2006). The organisation also used drones for the protection of refugees and internally displaced populations (IDPs) in Chad in 2009. In 2013,

the UN officially adopted the use of drones for its mission in Congo (MONUSCO) (BBC News, 2013), not only as a means to respond to violence but also as a tool of deterrence (UN News Centre, 2013)

Drones, for instance, in Africa, have improved healthcare services in Rwanda as they are being used to deliver blood in remote areas, thus helping to ensure the security of the people. Some of these emerging technologies are being researched and tested. Others have already been deployed, including mixed reality merging the virtual and the real world, Augmented Reality (AR) and Virtual Reality (VR), 5G, Artificial Intelligence (AI), and Blockchain, among others. Currently, Africa is also engaged in technological Research and Development and deployment. Some countries on the continent already have thriving AI hubs, such as Nigeria and Ethiopia. Google has its own AI hub in Ghana, and the United Nations (UN) has an AI centre, the UN Global Pulse lab, in Kampala. Google has an Artificial Intelligence (AI) hub in Ghana. Just like the rest of the world, modern technologies are becoming highly influential on the security and stability of African states. Among others, the rapid spread of the internet across the African continent has been heralded as a key driver of prosperity and a sign of the continent's technological coming of age.

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, 2018). In recent times, the increasing level of insecurity in Nigeria has evoked serious concern. On a daily basis, we hear, witness, or read about one form of killing, a disaster occurring in various parts of the country. Successive leadership in

the country for the past decades has always seen national security only through 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, and societal security (Akpan, 2021).

Technology has played a 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 even in some less developed ones such as Ghana and Nigeria, technology has proven to be effective in managing threats. However, there remains a significant gap between the nature of insecurity experienced in developing countries like Nigeria and the technological and institutional responses employed, compared to developed nations. 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 addressing insecurity, where a wide range of instruments can be deployed to tackle crime and enhance vigilance across various organizational and governmental functions (Bassey, 2020).

Specifically, in Nigeria, technology has been utilized in various operational and strategic areas. One example is the deployment of surveillance drones in regions such as the Sambisa Forest to track Boko Haram insurgents, which has enhanced military intelligence gathering and reduced direct human risk. Additionally, GPS tracking systems have been integrated into police patrol operations in major urban centers like Lagos and Abuja to monitor crime-prone areas in real-time. Crime-mapping software and biometric identification systems are increasingly used to verify suspects, while digital forensic labs support cybercrime investigations. However, these

implementations are often concentrated in urban areas, reflecting significant regional disparities in access to security technologies. Rural regions in the North-East, North-West, and parts of the Middle Belt suffer from limited technological penetration, thereby weakening the effectiveness of a national response to insecurity.

With the help of technology, the government of Nigeria initiated several policy measures, such as the Terrorism Prevention Policy, Bank Verification Number (BVN), Anti-Money Laundering Laws, and the National Identification Number (NIN), among others, to checkmate the challenges of insecurity in the country. One of the most notable efforts has been the compulsory biometric registration of every mobile telephone SIM-card owner by mobile network operators, alongside the deactivation of all unregistered lines (David, 2017). The registration exercises were successfully executed, and network providers were reportedly able to support security agencies in intelligence gathering through mobile tracking of suspected insurgents.

However, while these interventions are well-intentioned, their impact has been mixed and warrants critical assessment. For instance, the SIM card registration policy was undermined by the continued existence of black-market SIM sales and weak enforcement in rural areas. Similarly, although the BVN and NIN systems were designed to link individuals' financial and personal identities, loopholes in data integration and bureaucratic delays have limited their efficacy. In some cases, fraudulent accounts still operate using false identities, raising questions about the robustness of these systems. Furthermore, these policies have faced criticisms for failing to adequately protect citizens' data privacy and for the exclusion of vulnerable populations who lack access to registration centers. Policy outcomes also reveal gaps in follow-through and enforcement. While there have been occasional arrests and asset seizures facilitated by BVN-linked investigations, the

broader objective of deterring money laundering and terrorism financing remains only partially achieved. Regional disparities in digital infrastructure, power supply, and literacy levels also constrain the uniform application of these initiatives, creating uneven security coverage across Nigeria.

The 2012 coordinated attacks on telecommunication masts in Yobe, Borno, Gombe, and Bauchi States were suspected to be retaliatory attacks for the collaboration between network providers and security personnel (David, 2017). These events underscore the operational risks associated with the technological integration of security functions, especially in insurgency-affected regions. While Nigeria's efforts to deploy technology in security management are commendable, a more coherent, inclusive, and critically assessed implementation strategy is needed to close the existing gaps and improve national security outcomes. The other effort played by the Nigerian government is the proliferation of a comprehensive depository of biometric data of the citizens. This is fundamental to Nigeria's national security. There are different agencies where biometric data are captured in the country, with no central integration of the captured data yet. For effective delivery of their work, the following agencies also collected biometric data of the citizens, just like the mobile network operators:

i. The Independent National Electoral Commission (INEC) for the Permanent Voter's Cards (PVCs).
ii. National Identity Management Commission (NIMC) for national identity cards.
iii. Nigerian Immigration Service (NIS) for the issuance of international passports. iv. National Population Commission (NPC) for census data.
iv. Joint Admission and Matriculation Board (JAMB) for candidates' registration.

v. Federal Road Safety Corps (FRSC) before the issuance of driver's licenses.

vi. Bank Verification Numbers (BVN) for all banking transactions.

It is important for the federal government to harmonize all the different sources listed above, as well as intelligence-based, inter-border cooperation on biometric data within the continent of Africa. There is a lot more to be done on data mining/profiling if the government is to curb the spread of insurgency and insecurity in Nigeria. Importantly, the government should anchor the integration of a citizens' database where all biometric records of citizens and visitors are documented. This is very important to counterinsurgency response and planning. This idea can best be appreciated from the experience of the advanced countries of the world, where news agencies are furnished with pictures of terrorists and criminal suspects within hours after the crimes are committed will inspire Nigeria's efforts.

Though the federal government had earlier launched NigeriaSat-X and NigeriaSat-2, these two are not enough to provide the aerial surveillance required, given the size of the country, and to view the insurgent hideout like Sambisa Forest in Borno and the Creeks in the South-South region of Nigeria (Ani, 2024). The investment and launching of satellite infrastructure is no doubt capital-intensive, but it is justifiable for the government to spend that amount to avert the loss of life and property of the citizens.

It is also instructive that the Nigerian government insists on an Automated Personal Data Bank (APDB) for all citizens and immigrants. APDB is the use of dedicated devices as a database for the collection and storage of personal information and data of citizens and immigrants that can allow the security agents to trace an individual's data, including suspected criminals or terrorists (Yakubu, Mohammed, and Abdulkadir, 2018). The records of APDB can contain fingerprints,

digital images, addresses, and vehicle registration in order to facilitate the monitoring of the activities of the citizens by government security agencies and departments like the Department of State Security Service (DSSS) and State Criminal Investigation Department (SCID). The drone technology or unmanned aerial vehicle (UAV) exists in developed countries to fight insurgency and other forms of insecurity. A drone is an unmanned aerial vehicle that is capable of flying over the epicenter or hotbed regions to gather valuable visuals that will complement satellite imagery. This technology is being used in developed countries to quietly deploy bombs on the target area with little or no collateral impact.

As good as modern technology may seem to be, its application in the fight against crime in Nigeria is faced with some challenges. These include: lack of technical know-how, uncooperative attitude of the service providers, lack of appropriate software, corruption, the high cost of acquiring the equipment, poor orientation of the security operatives to technological usage, and poor power supply.

Lack of technical know-how. The usage of modern technology in any organization demands a great level of training. According to Uchenna, Chukwuemeka, and Chukwuka (2018), training has often been an overlooked issue with serious implications for technological infrastructure like ICT in the public sector. Most personnel of the Nigerian security forces lack the knowledge, skill, and attitude needed for the utilization of modern technologies in the fight against crime. Maduka (2014) opines that most security agents are not adequately trained, and those trained are not deployed to their area of skill and competency. As a result, the ability of the personnel to utilize modern technology towards achieving the organizational set goal becomes a challenge. In line with the above argument, Onasile (2017) argues that the lack of technical training

in the Nigerian police has been one of the problems of police ineffectiveness in Nigeria. According to Abdel-Fattah and Galal-Edeen (in Abasilim & Edet, 2015), the major challenge of e-governance in the Nigerian public service is the lack of trained and qualified personnel to handle and operate its infrastructures.

Uncooperative attitude of the service provider in telecommunication has been a problem in the fight against crime. One of these problems is the lack of synergy between the telecommunication companies and the security forces, which consequently affects the effective usage of ICT in the security of the nation.

As observed by Adigun, Mutiu, andRaimi (2018) that the unfriendly relationship between the public and the security forces has affected the proper usage of ICT in policing in Nigeria. Again, Ogu and Oyerinde (2014) sadly note that, the mobile telecommunications giants who champion the cause of intelligence surveillance and the monitoring of Cyberspace transmissions in developing countries have been hypnotized by the prospects of profit making in developing and underdeveloped countries that they have failed to realize that the absence of National Peace and Security pose a very potent threat to their business existence and operation within the geographical borders of the Nation. In most cases, the security forces are not given free access to the internet for discreet investigation.

Poor power supply is another challenge that has affected the effective utilization of modern technology in the fight against insecurity in Nigeria. Most, if not all, modern technologies are powered electrically, and this is a function of the government, but unfortunately, Nigeria is besieged with epileptic and irregular power supply. Agbodike and Igbokwe-Ibeto (2017) noted that there is no part of Nigeria that can boast of a twenty-four-hour electricity supply. These,

according to Abasilim and Edet (2015), have e-governance objectives in Nigeria. Okwueze (2010) also noted that adequate power supply is very important for the successful implementation of modern technology in the administration of the public sector in Nigeria. Against the current picture of what exists in most of the public service, most government agencies operate on generators, which, in most cases, cannot adequately power the giant technological facilities.

Lack of equipment is another crucial challenge to the application of modern technologies in the fight against insecurity in Nigeria. A pilot survey reveals that most of the offices in the Nigerian public service are still lacking in basic infrastructures of modern technology. In line with the above, Abasilim and Edet (2015) argue that some of the offices in the Nigerian public sector still lack common computers, let alone the common skills for their operation. Most of the offices in the Nigerian security sector still do things in the traditional way, which is paperwork. There is still no access to the internet in most of the offices within the security sector. Again, in the business of security in Nigeria, the majority of Nigerians have no access to telecommunication gadgets – mobile phones, internet data, etc, without which, the people cannot adequately share their information with the security agents. Agbodike and Igbokwe-Ibeto (2017) noted that the high cost of these telecommunication gadgets is one of the reasons responsible for the lack of ICT infrastructures.

Poor orientation of both the Security officers and the public towards the usage of technology. Agbodike and Igbokwe-Ibeto (2017) posit that there is cultural resistance to e-government in Nigeria because of the existence of informal relationships among public servants, thus making public servants lack confidence in the new technologies. Most of them are still used to the old way of carrying out government activities. That is, they are still known to be working

with a lot of papers, carrying files from one desk to the other or from one office to the other. Their resistance to e-governance implementation in their services is what has culminated in the poor rating of the implementation of e-governance in he public service. Abasilim and Edet (2015) gave some of the reasons for this as a lack of computer literacy among the personnel of the public service.

Lack of centralisation of data is another problem affecting the use of technology in Nigeria. Thus, there is no central database for all the security agencies in Nigeria to harvest information from. This does not allow for effective synergy among the numerous agencies involved in the fight against crime in Nigeria. Mohammed and Maina (2017) argue that centralized data is a prerequisite for security and sustainable development in Nigeria. They further argue that there is no centralisation of a database for sharing among government agencies in Nigeria; rather, the agencies operate a distributed database.

Corruption is another challenge that has hindered the effective application of modern technology in the fight against insecurity in Nigeria. Corruption in the Nigerian security sector involves the exploitation of their public position, resources, and power to embezzle public funds meant to purchase modern technological tools for an effective fight against crime. In line with the above argument, Emerson (2010) observes that high-level security officers embezzled a staggering sum of public funds meant to cover basic security operations. Kazeem (2015) observes that in 2015, President Buhari ordered the arrest of a former National Security Adviser for allegedly stealing up to two million US dollars in fraudulent arms dealing, which deprived the Nigerian Army of the equipment at the peak of its battle with Boko Haram insurgents. In the same vein, Abiodun (2020) argues that despite the increase in Nigeria's Defense budget, the performance of

the security forces in the fight against crime has remained poor. Regarding the above, Kaoje (2017) earlier argued that corruption in the procurement process within the public service accounts for 70% of the government's total budget, and this potent obstacle to efficiency of public spending and opportunities to improve the quality of service to the public.

Conclusion

With the myriad of security challenges facing the Nigerian state, there is a need for the Federal Government and its agencies to adopt the use of technology to contain the spread of these challenges. These technological infrastructures are very important in mounting surveillance by monitoring and controlling the affairs of the state. The satellites and drones are eyes in the air that monitor the environment as well as gather geospatial information for mapping crime hotspots, surveillance, and security intelligence. The lives and properties of the citizens of Nigeria deserve to be protected better than they are currently experiencing. Security remains one of the necessities of life; without security, citizens are exposed to different forms of attacks.

With the latest technology advancement and applications all over the world, a lot can be achieved and monitored such as CCTV and GPS to monitor movement and visuals to what is going on in a certain location, National identity can also be used to controlled and know the number of people living in a particular location where every member of the society have to uniquely be identified and can be tracked with National Identity card he is holding which is GPS enabled.

Recommendations

The paper recommends the following:

i. As new technology keeps evolving, where more sophisticated and advanced devices emerging, it becomes imperative and instructive that the National Security forces implement technology or ICT applications proactively to manage the new trend of events and data transmission nationwide. The security should be across the nation and not only enforcing it in areas affected by crimes.

ii. Security situations in Nigeria should be the concern of all discerning citizens; every suspicious transmission, movement, or communication within the circle of reach of every citizen must be reported to the nearest and appropriate authorities for prompt action to be taken. The citizens have to be ready to comply and also have in mind that security is everybody's business and not the security agencies alone.

iii. Nigerian scientists at home and abroad should be tasked to produce the appropriate technology for the specific needs in the security sector. The Defence Industry Corporation of Nigeria (DICON) can be challenged to oversee this assignment. Finally, the government should train its personnel on ICT knowledge in all sectors and agencies to ensure maximum use of the ICT facilities.