DIGITAL MEDIA TECHNOLOGY AND SECURITY ARCHITECTURE FOR COMBATING INSECURITY: DYNAMICS FOR SUSTAINABLE SECURITY AND INNOVATIONS IN NIGERIA

Bolanle Morenike ADEOLUWA
Department of Media and Communication Studies,
Afe Babalola University, Ado-Ekiti, Ekiti State, Nigeria.
Email: morenik01@yahoo.com Tel: +2348034735115
&
Adedeji Matthew ADEDAYO
Department of Conflict, Peace and Strategic Studies,
Afe Babalola University, Ado-Ekiti, Ekiti State, Nigeria.
Email: adedayoadedejim@gmail.com Tel: +2347031537294
&
Professor Innocent E. OKOYE
Department of Media and Communication Studies,
Afe Babalola University, Ado-Ekiti, Ekiti State, Nigeria.
Tel: +2347069278170
&
Professor Isiaka Alani BADMUS
Department of Conflict, Peace and Strategic Studies,
Afe Babalola University, Ado-Ekiti, Ekiti State, Nigeria.
Email: isiaka.badmus1@gmail.com Tel: +2348062646295
&
Enioluwa Prince ADEOLUWA
enioluwaadeoluwa@gmail.com
&
Kehinde Oluwatoyin Adabembe (PhD)
Department of Religious Studies, Faculty of Arts,
Federal University, Oye-Ekiti, Nigeria.
.Email: kehinde.adabembe@fuoye.edu.ng Tel: +2348030640642

Abstract

It is indispensable to use digital technology and security architecture to combat insecurity in order to promote sustainable security and innovations and guarantee the security and well-being of the Nigeria populace. The mounting insecurity challenges in Nigeria can be associated to lack of innovative approaches such as digital technology and robust security architecture for effective mitigation.Premised on this background, this study focuses attention on explore the dynamics of employing digital technology in crafting sustainable solutions to combat insecurity within the Nigerian States. The paper also established the nexus between digital technology and security architecture and the roles of digital technology in strengthening security architecture in Nigeria. It examines the various ways digital technology interventions have been contributed to sustainable security in Nigeria. In addition, the paper discusses various categories of digital technology that can be applied and integrated to the Nigerian security scenario. The study derives its data from primary and secondary sources. The study adopted technological determinism theory as a theoretical framework. The study observes that the use of digital technologies has been pivotal roles in combating all forms insecurity menace and strengthen security architecture in Nigeria. The paper reveals that the combination digital technology and security architecture will provide a promising pathway for strengthening Nigeria's defenses against various security threats, promoting sustainable security, and preserving the welfare of its people. The paper concludes that there is need for Nigeria government to promote a comprehensive security strategy that incorporates digital technology in order to surmount insecurity challenges.

Keywords: Digital Technology, Security Architecture, Insecurity, Dynamics, Sustainable Innovations

Introduction

Technological innovations, like digital technology, have led to an explosion of advancements in various sectors during the 21st century. The world is still very concerned about criminal activity, and cybercrime including fraud, espionage, identity theft, and phishing is becoming more and more prevalent (Scott, 2021).Traditional crimes like human trafficking, terrorism, and abuse, among others, continue to be a serious concern despite the rise in virtual crimes. The definition of crime management is "the attempt to deter or reduce crime and criminal elements." It encompasses a wider range of endeavors than just decreasing offenses. Conversely, security control refers to the use of countermeasures in order to identify and reduce security threats. While technological innovations such as digital technology are essential for controlling crime and maintaining security, they are also to be aware that it may encourage insecurity and crime. The rise in technological innovation continues to influence the understanding and dialogue around security architecture. Technological innovations are defined by (Scherer, 2001) as the process of introducing a new technology into the market for use.

It is indispensable to use digital technology and security architecture to combat insecurity in order to promote sustainable innovations and guarantee the security and well-being of the populace. The mounting insecurity challenges in Nigeria can be associated to lack of innovative approaches such as digital technology and robust security architecture for effective mitigation. The relationship between security architecture and digital technology has become a crucial front in the fight against insecurity in the modern national security environment. Nigeria, a country facing a variety of security issues, including cybercrime, urban violence, kidnapping, banditry, terrorism, and insurgency, is at a critical point in its development where it can greatly benefit from technological advancements in security (LeCates, 2018).

Accordingly, around the world, technologies like metal detectors that can be installed in buildings to screen for metal objects like guns and radar guns and satellites are used to detect overspeeding vehicles. Gun violence is on the rise, and some cities. To assist in determining when a gun fires, authorities have invested in gunshot detection technology (Travis, 1998). Closed-circuit television is one of the other technologies (CCTV). Advances in science and technology have led to the beneficial application of thermal and infrared technologies in security (Hou, Zhang, Zhou, Zhang, Lv, and Wu, 2022).

According to Smith and Grabosky (2018), as technology has advanced, a number of information securities-related systems have been created to address the constantly changing wave of criminality. Artificial intelligence and other technological advancements have improved the ability to combat crimes like money laundering and find money intended to fund terrorist activities. According to Worthman (1997), the Global Positioning System (GPS) is now widely available, even on mobile phone technologies, having previously only been available to security agencies. This has a significant impact on how crime is managed. The use of x-ray technology in airports has become commonplace in many nations.

The security industry is experiencing a transformation in the way threats are identified, examined, and countered as a result of the incorporation of cutting-edge digital technologies like artificial intelligence, big data analytics, and the Internet of Things (IoT). These technologies improve the ability of security forces to react proactively to possible threats by enabling more effective surveillance, predictive policing, and real-time communication. Additionally, the use of digital technology encourages increased community involvement, fostering a cooperative atmosphere where residents and law enforcement agencies can cooperate to improve safety and security (Smith and Grabosky, 2018).

In addition to addressing current threats Nigeria, this dynamic interaction between technology and security encourages long-term innovations that can change with the security environment and architecture. Nigeria can create a robust security framework that can withstand upcoming challenges by making investments in R&D and regularly updating security protocols and training programs. Furthermore, the establishment of strict laws and guidelines to control the application of these technologies guarantees moral behavior and defends citizens' rights, which promotes public cooperation and trust (Diegoli and Laudemann, 2018).

Subsequently, this study examines the relationship between Nigerian security architecture and digital technology, examining how technological determinism influences and propels long-term innovations in insecurity prevention. It looks at how security technologies are currently used in Nigeria, assesses how they affect security operations, and talks about how integrating cutting-edge innovations in the future can help create a safe and stable environment for all Nigerians. The study seeks to shed light on the dynamics of technology-driven security solutions and how they might alter Nigerian national security via this lens.

Aims/Objectives of the Study

The broad aim and objective of the study is to explore the dynamics of employing digital technology in crafting sustainable solutions to combat insecurity within the Nigerian States.

The specific aims and objectives are to;

i) establish the nexus between digital technology and security architecture;

ii) examine the roles of digital technology in strengthening security architecture in Nigerian States;

iii) access the various ways digital technology interventions have been contributing to sustainable security in Nigerian States; and

iv) examine the categories of digital technology that can be applied and integrated to the Nigerian States security scenario.

Literature Review

Conceptual Clarifications

Digital Technology

Digital technology is the use of sophisticated information and communication technologies to gather, store, analyze, and disseminate market and physical data at every stage of the product value chain. It is a crucial technological enabler for innovation across a range of industries (Edwards, 2015). Digital technologies include gadgets like tablets and Personal Computers, tools like digital cameras, calculators, and playthings, software and application systems, augmented and virtual reality, and less tangible tech like the Internet.

Digital technology refers to the use of electronic tools, systems, devices, and resources that generate, process and store data. Through social media, video conferencing, email, and instant messaging, digital technology has completely changed the way we communicate, making it easier and faster than ever. These technologies, which encompass hardware and software, are becoming an essential aspect of contemporary life, influencing a range of industries including business, education, entertainment, and communication (Danby, Fleer, Davidson, and Hatzigianni, 2018).

Security

According to Adabembe and Adedayo (2022) cited by Familugba, Ibitoye, Adedayo and Ojo (2024) define security as the protection of person's life, propertiesand possessions. In the same vein, security also means absence of risk or threat. It covers a wide range of situations and, depending on the situation. Recent times have seen the replacement of the conventional understanding of security with a non-traditional one. Political theorists like Thomas Hobbes believed that the primary function of a state is to maintain law and order, which can only be accomplished through effective security. This suggests that historically, the state has played a one-sided role in security.

Any society needs security and safety for its functions. Safety and security represent many things, including food supplies, health, housing, environmental security etc. It’s seen as moral rights and intrinsic to development; Security and safety of men and women encourages well-being and financial health; It promotes in productivity of individual and economic life integration; It helps individual to be calmer, understanding, mind control and be more responsive than reactive, more observant, and achieve cognitive awareness; Security and safety is vital for survival (Adabembe and Adedayo, 2022).

Security Architecture

The term “security architecture” describes the methods and techniques utilized to safeguard the availability, integrity, and confidentiality of security organization's data and information systems, as well as the structured framework, design principles, security policies and

procedures, and mechanisms and procedures. Ensuring protection against threats, vulnerabilities, and unauthorized access requires a comprehensive set of security measures, policies, and controls that are seamlessly integrated into the overall Information Technology (IT) architecture (Soomro, Shah and Ahmed, 2016). It also refers to methods like encryption, data masking, and secure data storage that guarantee data privacy and integrity as well as safeguards for data while it is being transmitted over networks. Software applications are protected from attacks and vulnerabilities by security architecture. Application firewalls, secure coding techniques, and frequent security testing are required for this. To build a strong security posture that can respond to changing threats and safeguard the vital resources and data of an organization, security architecture is indispensable (Lavanya and Dunstan, 2024).

Security architecture is also defined as the architectural design that includes all the threats and potential risks which can be present in the environment or that particular scenario. This also includes the security controls and the use of security controls (NIST 80018). For the security architecture, the proper documentation is done that include all the security specifications and include all the detailed information about the architecture. Security Architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment (National Institute of Standards and Technology).

Security Architecture is a set of security principles, models and methods designed to align to the state objectives and assist to keep the state safe from threats (NIST 80027).Security architecture is the foundation of security strategy (NIST 80030). It is a type of security design composed to multiple components, including the processes, tools, and technologies used to protect the state from external threats. Security architecture helps to position security controls and breach countermeasures and how they relate to the overall systems framework of your society (National Institute of Standards and Technology).

Insecurity

Insecurity is the antithesis of security. However, because of the very many ways in which insecurity affects human life and existence, the concept of insecurity has usually been ascribed different interpretations in association with the various ways which it affects individuals. Some of the common descriptors of insecurity include: want of safety; danger; hazard; uncertainty; want of confidence; doubtful; inadequately guarded or protected; lacking stability; troubled; lack of protection; and unsafe, to mention a few. All of these have been used by different people to define the concept of insecurity. These different descriptors, however, run into a common reference to a state of vulnerability to harm and loss of life, property or livelihood (Akin, 2008).

Beland (2005) defined insecurity as “the state of fear or anxiety stemming from a concrete or alleged lack of protection.” It refers to lack or inadequate freedom from danger. This definition reflects physical insecurity which is the most visible form of insecurity, and it feeds

into many other forms of insecurity such as economic security and social security. Insecurity as the state of being open or subject to danger or threat of danger, where danger is the condition of being susceptible to harm or injury, and insecurity as the state of being exposed to risk or anxiety, where anxiety is a vague unpleasant emotion that is experienced in anticipation of some misfortune. A major point about insecurity implied in these definitions is that those affected by insecurity are not only uncertain or unaware of what would happen but they are also not able to stop it or protect themselves when it happens.

Role of Digital Technology Innovations in Security Architecture and Control

Information sharing has become a key pillar of security architecture, control and crime management in the world. In response to the insecurity and its destabilizing effects across the world, the United Nations, ECOWAS and the African Union have put concerted efforts to ensure better information management to address insecurity. A key solution to the insecurity is the reinforcement of coordination of cross-border surveillance and the strengthening of national actions to address insecurity. The African Union, in a bid to address insecurity, launched the AU Strategy for the Sahel (African Union, 2014) and the Nouakchott Process (African Union, 2014). Both sought to address the glaring gaps in cooperation and coordination among stakeholders.

Theoretical Framework

This aspect of the study discusses the theory that forms the framework with which the research works is built. For the purpose of this study, the theory used is technological determinism theory.

Technological Determinism Theory: The theory that has been selected to examine digital technology and security architecture for combating insecurity as dynamics for sustainable security and innovations in Nigeria. Technological Determinism state that media technology shapes how we as individuals in a society think, feel, act, and how society are operates as we move from one technological age to another (Tribal- Literate- Print- Electronic). The theory ‘technological determinism’ is a branch of determinism in sociology that was coined by the American economist and sociologist Thorstein Veblen (1857-1929). Technological determinism theory is a reductionist theory that presumes that a society’s technology drives the development of its social structure and cultural values. Technological determinism is the idea that technology shapes social change. It determines the future. Technological determinism believes that advancements in technology are the moments that bring on each new phase in human history. For instance, the invention of the wheel revolutionized human mobility, allowing humans to travel greater distances and carry greater loads with them. Thus, a technological advancement changed the course of human history for all time. Various technological advances that caused great leaps in human history include: the invention of

digital technology, discovery of various new means of communication, the invention of steam engine, the internet and emergence of artificial intelligence.

The application and use of digital technology and security architecture in the fight against insecurity in Nigeria can be directly linked to the theory of technological determinism, which holds that technological development drives societal change and shapes human behavior. According to the theory of technological determinism, social structures and practices will eventually change as a result of the development of digital technologies. The way security is managed and enforced in Nigeria has fundamentally changed as a result of the integration of cutting-edge digital technologies into security architecture. As an illustration: Surveillance Systems: The installation of advanced biometric, drone, and CCTV cameras improves monitoring capabilities, which has an immediate effect on crime prevention and response tactics.

The way that information is disseminated and incidents are reported through social media and mobile applications has made citizens more aware and involved, which has changed the conventional dynamics of community policing. Rapid response to security threats has been improved by the widespread adoption of mobile technology, which has made it possible for security forces and the public to communicate and coordinate in real-time.The creation of integrated security systems, which integrate multiple technologies (such as GPS tracking and cybersecurity measures), is indicative of a deterministic approach in which the structure and functionality of security architecture are determined by technological capabilities. Laws and regulations pertaining to cybersecurity, data privacy, and the moral application of technology in security operations are developed as a result of the need to control and oversee the emerging digital environment.

The theory of technological determinism offers a framework for comprehending how security architecture and digital technology impact and transform initiatives that combat insecurity in Nigeria.The idea of technological determinism, which holds that societal shifts are driven by technological advancements, offers a convincing framework for comprehending how digital innovations can alter Nigeria's security infrastructure, tactics, and architecture.

Methodology

Both primary and secondary data were sourced and utilized for the study. The primary data was collected through a well-designed Google Form and printed (hardcopy) questionnaire and interview guide which was later administered to two hundred (200) respondents randomly chosen across states in six (6) geopolitical zones in Nigeria. Two (2) states were picked in each of the geo-political zone. South-West: Ekiti and Oyo States; South-South: Rivers and Edo States; South-East: Enugu and Imo States; North East: Taraba and Yobe States; North Central: Kogi and Plateau States; and North West: Kano and Kaduna States. Secondary data was carefully selected through books, journals, newspapers, and internet sources.

The data derived from the study was transcribed and classified into themes and sub-themes based on the research objectives. The data content was analyzed descriptively, using a deductive approach. Descriptive analysis is the transformation of data into a form that will make them easy to understand and interpret; re-arranging, ordering, schematized and manipulating data to generate descriptive information and content analyzed.

Data Presentation and Analysis

The Demographic Characteristics of Respondents

Table 1: Socio-Economic Characteristics of Respondents

S/N	Respondents Bio Data	Frequency	Percentage
1	**GENDER:**		
	Male	122	61.00%
	Female	78	39.00%
	Total	**200**	**100%**
2	**Age Distribution:**		
	18-25	31	15.5%
	26-40	55	27.5%
	41- 55	63	31.5%
	55years and above	51	25.5%
	Total	**200**	**100%**
3	**Educational qualification:**		
	Primary Education	24	12.00%
	Secondary Education	57	28.5%
	Tertiary Education	96	48.00%
	No Formal Education	23	11.5%
	Total	**200**	**100%**
4	**Religious**		
	Christianity	117	58.5%
	Islam	80	40.00%
	African Traditional Religious (ATR)	3	1.5%
	Total	**200**	**100%**

5	**Occupation/Groups Affiliation:**		
	Government Officers	12	6.00%
	Security Policymakers and Experts	37	18.5%
	Security and law enforcement Personnel	33	16.5%
	Members of Academics Community	17	8.5%
	Digital Technology Experts and IT professionals	21	10.5%
	Grassroots and Community Leaders	20	10.00%
	Members of NGOs	15	7.5%
	Members of CSOs	15	7.5%
	Youth and Students	20	10.00%
	Politicians	10	5.00%
	Total	**200**	**100%**

Source: Researcher's Fieldwork, 2024

Findings on Research Objective 1: Various Digital Technology Deployed in Crafting Sustainable Solutions to Insecurity within the Nigerian States

Table 2: Various Digital Technology Deployed in Crafting Sustainable Solutions to Insecurity within the Nigerian States

Variables	Frequency	Percentage (%)
Closed-Circuit Television (CCTV)	45	22.5%
Drones	33	16.5%
Surveillance Cameras	30	15.00%
Biometric Identification Systems (BIS)	28	14.00%
Crime Mapping Applications (CMA)	21	10.5%
Social Media Monitoring Tools (SSMT)	19	9.5%
Geospatial Intelligence Tools (GIT)	16	8.00%
Radar Systems	8	4.00%
Total	**200**	**100%**

Source: Researcher's Fieldwork, 2024

Table 2: Above shows variousdigital technologies deployed in crafting sustainable solutions to insecurity within the Nigerian States. This is evident from respondents' responses. The majority of respondents 45 (22.5%) agreed that closed-Circuit Television (CCTV) was the digital technology deployed in crafting sustainable solutions to insecurity in their areas and respective states, while 33 (16.5%) of the respondents indicated Drone. It was revealed that 30 (15.00%) of the respondents indicated Surveillance Cameras. In addition, 28 (14.00%) agreed on Biometric Identification Systems (BIS); 21 (10.5%) agreed on CrimeMapping

Applications (CMA); 19 (9.5%) of the respondents agreed on Social Media Monitoting Tools (SSMT) severed as digital technology tools to curb insecurity in their areas, 16 (8.00%) agreed on Geospatial Intelligence Tools; while 8 (4.00%) of the respondents agreed that Radar Systems serves as digital technologies deployed in crafting sustainable solutions to insecurity in their area. It was indicated that all these factors influenced and enhanced security and security architecture in Nigerian States.

Findings on Research Objective 2: The Nexus between Digital Technology and Security Architecture

Digital technology and security architectural design are strongly related, as digital technology plays a significant role in enhancing the ability to protect systems, information, data and infrastructures from various threats. Digital technology provides tools to automate threat modeling and risk assessments, identifying potential vulnerabilities and threats in the architectural design phase. For instance, digital technology such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA) enhances security by requiring multiple forms of verification before granting access. In the same vein, Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) were use to monitor and control incoming and outgoing network traffic based on predetermined security rules.

According to respondents, majority of them posited that digital technology has been playing critical role in enhancing, preventing, detecting and responding to various security threats in the world. The respondents said that digital technology has been helping to mitigate risk by identifying potential incidents, allowing fast responses, deterring criminal behavior, preventing unauthorized access and capturing crucial evidence during a breach by state security agencies and government. It is also averred that digital technology plays considerable role in strengthen the security architecture by creating roadmap for guiding against future internal and external threats and cyber attacks.

Majority of security personnel interviewed postulated that digital technology helps government and various security agencies to identify potential threats, share information and data easily and protect mechanisms in them. In the same vein, respondents opined that digital technology if used appropriately, it will ensure a proactive and effective approach to address security threats and challenges in the world.

Findings on Research Objective 3: Roles of Digital Technology in Strengthening Security Architecture in Nigeria States

Table 3: The Roles of Digital Technology in Strengthening Security Architecture in Nigeria

Variables	Frequency	Percentage (%)
Advancement and promotion of counterterrorism measures	42	21.00%
Curbing of kidnapping and banditry	35	17.5%
Enhancing Customs border operations and maritime security	32	16.00%
Reduction of cybercrime and Yahooyahoo	23	11.5%
Improving Surveillance and Intelligence Gathering	21	10.5%
Improving community engagement and public safety	18	9.00%
Enhancing Infrastructure Security and Protection	11	5.5%
Reduction in highways crimes and criminalities	10	5.00%
Improving emergency responses and disaster management	8	4.00%
Total	**200**	**100%**

Source: Researcher's Fieldwork, 2024

The Table 3 above showed the distribution of respondents based on their opinions on the roles of digital technology in strengthening security architecture in Nigeria. The data showed that 42 (21.00%) of the total respondents indicated that digital technology has been used to advanced and promotes counterterrorism measures. 35(17.5%) respondents agreed that digital technology was used to curbed kidnapping and banditry in Nigerian States, 32 (16.00%) agreed on enhancing customs border operations and maritime security, 23 (11.5%) agreed on reduction of cybercrime and yahooyahoo, 21 (10.5%) agreed on improvement of surveillance and intelligence gathering; 18 (9.00%) agreed on improvement of community engagement and public safety; 11 (5.5%) agreed on that digital technology was used to enhanced infrastructure security and protection; 10 (5.00%) that the use of digital technology reduced highways crimes and criminalities; while only 8 (4.00%) agreed that digital technology was used to improved emergency responses and distaster management in Nigeria States. Based on the data gathered, it was affirmed that digital technology has been played crucial roles of curbing insecurity and strengthening security architecture in Nigerian States.

Findings on Research Objective 4: Various ways Digital Technology Interventions have been contributing to Sustainable Security in Nigeria States

According to respondents, majority of them affirmed the importance of digital technology in addressing insecurity issues in Nigeria States. The respondents said that digital technologyhas helps to identify and analyze potential threats to both human and national security in Nigerian States. Through the conscious and concerted effort of intelligence agencies and enforcement agencies and use of digital technology, the security operatives easily identified the latent and potential threats to both human and national security and deal with them without allowing those threats to see the light of day in majority of the states in Nigeria.

Information acquired from respondents established that digital technology provides insights into effective strategies for preventing and countering security challenges such as kidnapping, banditry, militancy, insurrection, succession movement in various states in Nigeria. With the aid and use of digital technology, data and essential information were gotten from sources and strategize to prevent and combat security challenges was made easy, and executing such combining logistics, tactics, data, real-time monitoring, and physical contact was not be proven difficult for the military and other security agencies in Nigeria. In the same vein, digital technology has also aided in formulating policies and allocating resources to enhance security architecture and capabilities.

Findings on Research Objective 5:Categories of Digital Technology that can be Applied and Integrated to the Nigerian Security Scenario

Responses gathered from the respondents onvarious categories of digital technology that can be applied and integrated to the Nigerian States security scenario. Some respondents indicated that there is need for strong surveillance systems, which installation of Closed-Circuit Television (CCTV) cameras and drone technology in strategic places and locations, highways, schools, commercial centres, markets, churches, mosques, government institutions and offices across states in Nigeria, respondents affirmed that all these will be vital for proper monitoring and tracking activities for criminals in their hideout and it will reduce perpetration of attacks by evildoers and anti-states actors. Majority of the respondents opined that if the CCTV cameras are widely used in public areas, government institutions, and commercial establishments to deter crime and provide evidence for investigations. Respondents agreed that integrating this into the security architecture of Nigeria, it will go a long way toward addressing many insecurity issues, aside from revolutionizing the archaic methods of securing people's lives and property.

Respondents also averred that the use of Biometric Identification Systems (BIS) which include facial recognition technology and fingerprint and iris scanning have revolutionizedNigerian security architecture. It was gathered that the use of facial recognition technology which involve advanced algorithms to analyze facial features and match them against a database of known individuals, allowing for quick and accurate identification has helps to minimize the rates of crimes occurrence in Nigeria. Respondents are of the opinion

thatthis can be used at airports, borders, and other places where they are highly needed. Respondents affirmed that this will help to identify and track down criminals, and where finger prints of suspects, otherwise called criminals, are left behind, forensic study using advanced digital technology will make the work of identification and tracking easier for security and law enforcement agencies.

As revealed by the respondents, digital technology through the use digital communication and information systems are needed across all states and security agencies in Nigeria, they affirmed that this technology will improve efficient information sharing in Nigerian States. Majority of the respondents mentioned mobile technology, including the use smartphones and tablets which will enables real-time communication between security personnel, allowing for immediate response to incidents and effective coordination during operations. Respondents also make mention of radio communication systems, they said this will provide reliable and secure communication channels for both short-range and long-range communications.

Furthermore, majority of respondents postulated that there is need for Nigeria government and security agencies to make use artificial intelligence and machine learning techniques to combat insecurity in Nigerian States. Finally, based on data gathered from respondents, if all these mentioned above is put in place by Nigeria government and security agencies, this will make the security agencies to be proactively identify potential threats and take preventive measures.

Discussion of Findings

It was gathered that the importance of digital technology in addressing insecurity issues in Nigeria cannot be underrated. Digital technology has helps to identify and analyze potential threats to both human and national security in Nigerian States. Through the conscious and concerted effort of intelligence agencies and enforcement agencies and use of digital technology, the security operatives easily identified the latent and potential threats to both human and national security and deal with them without allowing those threats to see the light of day in majority of the states in Nigeria.

It was also gathered that digital technology provides insights into effective strategies for preventing and countering security challenges such as kidnapping, banditry, militancy, insurrection, succession movement in various states in Nigeria. With the aid and use of digital technology, data and essential information were gotten from sources and strategize to prevent and combat security challenges was made easy, and executing such combining logistics, tactics, data, real-time monitoring, and physical contact was not be proven difficult for the military and other security agencies in Nigeria. In the same vein, digital technology has also aided in formulating policies and allocating resources to enhance security architecture and capabilities.

Conclusion and Recommendations

Digital technology advancements like satellite imaging can be used to track terrorist groups' movements and the construction of terror camps across vast deserts. Major problems like the illegal goods trade could be addressed with the aid of digital technology. This could be carried out at the ports of entry, making certain that contraband including weapons is apprehended. Technology may also be used to improve intelligence gathering, which aids in tracking and averting armed group attacks.

Nigeria government should intensify effort on the use of digital technology for proactive and effective approach to address various security lapses, threats and challenges in the country. In order to address the mounting insecurity challenges in Nigeria,there is an urgent need to explore innovative approaches that utilize digital technology and robust security architecture for effective mitigation.

There is need for every security agencies in Nigeria to use digital technology to transform their security operations for optimal, effective and efficient security service delivery. The use of digital technologies will assist in achieving transformation of security architecture and curbs all menace of insecurity and social vices in Nigerians States.

There is need for Nigeria government to initiate Community policing and work mobile applications for reporting crimes, and online portals for accessing security information promote collaboration between law enforcement agencies and the public to enhance overall security.

Cybersecurity services should be used to track terror financing through covert channels, combat online radicalization, and spread terrorist propaganda. Digital technology resources should be used to combat online criminal activity in a way that is cautious to guarantee focused interventions.

References

Adabembe, K.O. & Adedayo A.M. (2022) Ethno-Religious Crises and Its Implications on Security and National Development in Nigeria, British Journal of Multidisciplinary and Advanced Studies: Arts, Humanities and Social Sciences 3 (2), 1-20.

African Union. (2014). The African Union Strategy for the Sahel Region. Addis Ababa, Ethiopia: Peace amd Security Council, African Union.

African Union. (2022). Profiles of AU Special Envoys, High Representatives, Special Representatives and the Panel of the Wise - August 2022. Retrieved from African Union: https://www.peaceau.org/en/page/120-profiles-of-au-special-envoys-highrepresentatives-special-representatives-and-the-panel-of-the-wise

Danby, S., Fleer, M., Davidson, C., & Hatzigianni, M. (2018). Digital Childhoods across contexts and countries. In S. Danby, M. Fleer, C. Davidson, & M. Hatzigianni (Eds). *Digital childhoods: Technologies and children's everyday lives* (pp. 1-14). (International Perspectives on Early Childhood Education and Development; Vol. 22). Springer, Springer Nature). Doi: 10.1007/978-981-10-6484-5_

Diegoli, B. B., & Laudemann, J. (2018). Automated Inspection of Human Presence Inside Vehicles Through Heartbeat Detection Technology. Florianópolis: V Cidesport.

Edwards, S. (2015). New concepts of play and the problem of technology, digital media and popular-culture integration with play-based learning in early childhood education. *Technology, Pedagogy and Education*, *25*(4), 1-20. Doi: 10.1080/1475939X.2015.1108929

Familugba J.O; Ibitoye, M.O; Adedayo, A.M & Ojo, C.M. (2024)The Resurgence of Military Coups in West-Africa States: The Case of Niger Republic and Its Implications on Peace, Security and Transnational Activities in Nigeria. *Global Journal of Humanities and Social Sciences*, Vol. 03, Issue 03. Pp. 26.37.

Hou, F., Zhang, Y., Zhou, Y., Zhang, M., Lv, B., & Wu, J. (2022). Review on Infrared Imagine Technology. MDPI.

Lavanya, B and Dunstan, R (2024). Bibliometric insights on mapping the landscape of cybersecurity: Uncovering the research potential in banking industry

LeCates, R. (2018). Intelligence-led Policing: Changing the Face of Crime Prevention. Police Chief Magazine .

NIST 80018: Guide for Developing Security Plans for Information Technology System

NIST 80027: Engineering Principles for Information Technology Security (A Baseline for Achieving Security)

NIST 80030: Guide for Risk Management for Information Technology Systems

Scherer, F. M. (2001). Innovation and Technological Change. International Encyclopedia of the Social & Behavioral Sciences, 7530-7536.

Scott, S. M. (2021). COVID-19 and Crime: Analysis of Crime Dynamics amidst Social Distancing Protocols. PLOS One.

Smith, R., & Grabosky, P. (2018). Crime in the Digital Age: Controlling Telecommunications and

Cyberspace Illegalities (1st Edition ed.). New York: Routledge. doi:https://doi.org/10.4324/9780203794401

Soomro, Z. A. Shah M. H. and Ahmed, J. (2016) "Information security management needs more holistie approach: A literature review", International Journal of Information Management, vol. 36, no. 2, pp. 215-225.

Worthman, E. (1997). Global Positioning Systems. Mobile Radio Technology, 5, 58.