World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Assessing the Hurdles and Remedies to the Use of ICT for Enhanced Intelligence Gathering and Community Safety in Abuja, Nigeria

Andrew Ubong Bassey *

Department of Mass Communication, Faculty of Social Sciences, Nasarawa State University, Keffi, Nigeria.

World Journal of Advanced Research and Reviews, 2025, 27(01), 2310-2323

Publication history: Received on 16 June 2025; revised on 23 July 2025; accepted on 26 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2759

Abstract

This research examines the challenges and opportunities of implementing Information and Communication Technology (ICT) to enhance intelligence gathering and promote community safety in Abuja, Nigeria. As security threats become increasingly complex, integrating ICT tools such as biometric systems, surveillance technologies, and data analytics has become essential for effective and timely intelligence operations. Despite these potentials, widespread application remains limited due to infrastructural deficits, insufficient technical capacity, financial limitations, and socio-political constraints. Employing a quantitative research approach, data were collected from 384 respondents using a structured questionnaire across key locations in Abuja, achieving a 94% response rate. The analysis reveals that while ICT significantly contributes to intelligence gathering and public safety, its implementation faces ongoing challenges, including unreliable internet access, limited funding, low digital skills among operatives, and concerns about ethical surveillance. Grounded in Technological Determinism and Human Capital Theory and supported by existing empirical literature, this study contributes to current discourse by highlighting the underexplored role of digital technologies in Nigeria's security framework. Recommendations include increasing investment in ICT infrastructure, enhancing training for security personnel, improving policies, and fostering stronger collaboration between government and private stakeholders to support intelligence-led policing and community safety.

Keywords: Intelligence Gathering; ICT; Surveillance Technology; Security Communication; Community Safety; Abuja

1. Introduction

Information and Communication Technology (ICT) has become a crucial tool in intelligence gathering and community safety, transforming security operations globally. Intelligence methods have evolved from traditional surveillance and manual data analysis to technologically driven security frameworks, allowing for enhanced crime prevention, real-time monitoring, and rapid response mechanisms (Clarke, 2019). The integration of ICT in security operations has proven effective in advanced nations, where digital surveillance, artificial intelligence, and data analytics play an instrumental role in combating crime and terrorism (Baldwin & Black, 2021).

Countries such as the United States, the United Kingdom, and China have leveraged ICT to enhance their intelligence networks. In the United States, agencies such as the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) utilise big data analytics, AI-driven threat detection, and cybersecurity tools to monitor criminal activities and national security threats (Singer & Brooking, 2018). The United Kingdom's National Crime Agency (NCA) has adopted advanced facial recognition technologies, digital forensics, and encrypted communication tracking to enhance policing efforts (Williams, 2020). In China, AI-powered surveillance, predictive analytics, and smart city technologies have significantly improved security monitoring and crime deterrence (Creemers, 2021).

* Corresponding author: Andrew Ubong Bassey; ORCID ID: https://orcid.org/0009-0001-5228-9390

The adoption of ICT in intelligence gathering extends beyond Western nations. In Africa, countries such as South Africa and Kenya have implemented digital security initiatives to address threats from crime and terrorism. South Africa, for example, uses cybersecurity measures and forensic data analytics to combat organised crime (Mabunda, 2022). Kenya's security agencies employ biometric identification systems and digital communication tracking to improve national security (Ndung'u & Waweru, 2021). These examples demonstrate the effectiveness of ICT-driven intelligence frameworks in various geopolitical contexts.

Despite the global advancements in ICT usage and intelligence gathering, Nigeria faces significant challenges in implementing these technologies effectively. As the capital city, Abuja is Nigeria's administrative and political centre, necessitating a robust security infrastructure incorporating ICT innovations. However, the nation's intelligence and law enforcement agencies encounter inadequate ICT infrastructure, limited technical expertise, weak policy implementation, and poor inter-agency coordination (Eze, 2021). The Nigeria Police Force (NPF) and the Department of State Services (DSS) rely on outdated surveillance methods, limiting their ability to respond proactively to security threats (Adebayo & Olaleye, 2023). In addition, cybersecurity vulnerabilities, including data breaches and cyberattacks, pose serious threats to intelligence operations (Okonkwo, 2022).

Given these limitations, this study aims to assess the hurdles to ICT adoption in intelligence gathering and propose effective remedies to enhance community safety in Abuja. The study's findings will provide policymakers, security agencies, and technology stakeholders with insights to establish a sustainable ICT-based intelligence framework (Ogunyemi, 2023). The research will also contribute to the broader discourse on digital security in developing countries, offering recommendations tailored to Nigeria's socio-political landscape.

The urgency of adopting ICT for intelligence gathering in Nigeria cannot be overstated. The growing threats of terrorism, cybercrime, and organised criminal activities necessitate a technologically advanced approach to security management. By identifying barriers to ICT implementation and formulating practical solutions, this study seeks to enhance national security, improve law enforcement efficiency, and foster public trust in security institutions. Strengthening ICT integration in intelligence gathering will enhance Abuja's security landscape and set a precedent for nationwide digital security transformation.

Research Objectives

The study examines the challenges and solutions of applying information and communication technology (ICT) in intelligence gathering to enhance community safety in the Federal Capital Territory (FCT) of Abuja, Nigeria. The specific objectives are to:

- Identify the key challenges hindering the effective use of ICT in intelligence gathering for community safety.
- Examine the impact of these challenges on intelligence operations and overall security in Abuja.
- Investigate the adoption and integration level of ICT by security agencies for intelligence gathering.
- Recommend practical solutions and remedies to overcome the identified challenges and improve community safety through enhanced ICT utilisation.

1.1. Scope and Delimitation of the Study

This study's scope is limited to the city of Abuja, Nigeria. It focuses on the use of ICT by local security agencies involved in intelligence gathering and community safety initiatives. The study will target key stakeholders in Abuja's security sector, including law enforcement officers, ICT specialists, and community leaders. The analysis will cover the period from 2018 to 2024, during which significant ICT advancements and security initiatives were implemented in Nigeria. Delimitation excludes other regions of Nigeria and sectors outside intelligence gathering and community safety.

1.2. Significance of the Study

This study is expected to make a significant contribution to both the academic literature and practical policy. It will provide new insights into the barriers and opportunities for improving intelligence gathering through ICT in Abuja, Nigeria. The findings will inform policymakers, security agencies, and ICT professionals about the challenges they must address to implement ICT solutions for community safety successfully. Furthermore, it will serve as a foundation for future research on ICT in security, offering practical recommendations that can be adapted to other regions or contexts.

1.3. Conceptual Clarification

This section clarifies the critical terms associated with the use of Information and Communication Technology (ICT) in intelligence gathering and community safety. Understanding these concepts provides a strong theoretical foundation for assessing the challenges and solutions related to ICT-driven security measures in Abuja, Nigeria.

1.3.1. Information and Communication Technology (ICT)

ICT refers to the diverse range of digital tools, systems, and networks that facilitate the collection, processing, transmission, and retrieval of information (Castells, 2020). It includes advanced technologies such as artificial intelligence (AI), big data analytics, cloud computing, biometrics, and cybersecurity frameworks, which enhance communication and decision-making processes in security operations (Clarke, 2019). In the context of intelligence gathering, ICT provides sophisticated tools such as surveillance systems, encrypted communication channels, and forensic data analysis, all of which strengthen crime prevention and response mechanisms (Jensen, 2021). ICT enables the real-time sharing of intelligence among security agencies, allowing for proactive crime control and efficient crisis management (Tanner & Campana, 2022). The widespread adoption of ICT in intelligence and community safety is significantly influenced by infrastructural development, policy frameworks, and the technical capabilities of law enforcement agencies (Adeyemi, 2022).

1.3.2. Intelligence Gathering

Intelligence gathering is the systematic process of collecting, analysing, and interpreting data to support security decision-making (Lowenthal, 2021). It involves various techniques such as human intelligence (HUMINT), signals intelligence (SIGINT), open-source intelligence (OSINT), and cyber intelligence (CYBINT), all of which are increasingly reliant on ICT tools (Baldwin & Black, 2021). The integration of ICT in intelligence gathering has revolutionised law enforcement by enabling digital surveillance, geospatial intelligence mapping, and predictive analytics to detect and prevent security threats (Weimann, 2020). Furthermore, advanced ICT applications, such as drones, biometric identification systems, and automated facial recognition, enhance intelligence operations by providing real-time situational awareness (Hassan & Akpan, 2023). However, the effectiveness of ICT-driven intelligence gathering is often constrained by cybersecurity threats, data privacy concerns, and the ethical use of surveillance technologies (Oye, 2021). Addressing these challenges requires robust legal frameworks and enhanced technical expertise among security personnel to maximise the benefits of ICT in intelligence operations (Afolabi & Ogu, 2020).

1.3.3. Community Safety and ICT

Community safety refers to the collective efforts and strategies aimed at protecting citizens from crime, violence, and other security threats (Sampson & Eck, 2020). It encompasses proactive crime prevention initiatives, law enforcement collaborations, and public engagement in security matters, which ICT increasingly supports (Williams, 2020). The application of ICT in community safety includes digital crime mapping, emergency response systems, predictive policing, and neighbourhood surveillance networks (Bassey & John, 2023). These technologies facilitate rapid identification of security risks, enhance public communication on safety issues, and enable data-driven policymaking in crime management (Choi, 2022). ICT-powered public reporting platforms enable citizens to report suspicious activities anonymously, promoting community engagement in security governance (Adeyemi, 2022). Nevertheless, the effectiveness of ICT in community safety is often undermined by infrastructural deficiencies, resistance to technology adoption, and concerns regarding mass surveillance and civil liberties (Olaoye, 2023). Ensuring a balance between security enhancement and individual privacy rights remains critical in leveraging ICT for community safety (Tanner & Campana, 2022).

1.3.4. Hurdles to ICT Adoption for Intelligence Gathering

Despite the transformative potential of ICT in intelligence gathering and community safety, several barriers hinder its full implementation in Abuja, Nigeria. A primary challenge is the inadequacy of infrastructure, as unreliable power supply, poor internet connectivity, and limited access to modern security technologies impede the efficiency of ICT systems (Olaoye, 2023). The high cost of procuring and maintaining ICT-based security solutions presents financial constraints for law enforcement agencies (Afolabi & Ogu, 2020). Another significant hurdle is the lack of technical expertise among security personnel, as operating sophisticated ICT tools requires specialised training in cybersecurity, digital forensics, and data analytics (Baldwin & Black, 2021). Socio-political factors, including corruption, bureaucratic inefficiencies, and political interference, further complicate the adoption of ICTs, as intelligence data may be manipulated or restricted for political interests (Oye, 2021). The ethical concerns related to data privacy, surveillance abuse, and potential human rights violations challenge the acceptance and effectiveness of ICT-driven intelligence

strategies (Weimann, 2020). Addressing these hurdles requires comprehensive policy reforms, sustainable funding models, and enhanced public trust in technology-driven security initiatives (Choi, 2022).

1.3.5. Remedies for Enhancing ICT Adoption in Intelligence Gathering

Several strategic interventions are necessary to overcome the barriers associated with the adoption of ICT in intelligence gathering and community safety. First, significant investment in ICT infrastructure ensures seamless operation and integration of digital security systems (Adeyemi, 2022). Public-private partnerships can play a significant role in funding and developing ICT-driven security solutions, thereby reducing the financial burden on government agencies (Tanner & Campana, 2022). In addition, capacity-building initiatives should equip law enforcement personnel with advanced technical skills in cybersecurity, digital surveillance, and forensic data analysis (Hassan & Akpan, 2023). International collaborations with technology experts and security agencies can further enhance knowledge transfer and improve ICT proficiency within Nigeria's intelligence community (Bassey & John, 2023). Policy reforms should be implemented to promote transparency, accountability, and adherence to ethical guidelines in ICT-based intelligence gathering. Enforcing data protection laws, strengthening institutional oversight, and fostering public confidence in digital security measures are crucial to the sustainable integration of ICT in intelligence operations (Williams, 2020). By addressing these critical areas, Abuja can leverage ICT to enhance intelligence gathering, mitigate security threats, and foster a safer environment for its residents (Olaoye, 2023).

1.4. Empirical Study Review

Adelani et al. (2023) conducted a study examining the impact of community policing on security management in Kubwa, Bwari Area Council, FCT-Abuja. The study employed the Gap Theory to analyse the interconnectedness between Nigeria's law enforcement agencies and the communities they serve. It also assessed the extent to which private and informal security providers are integrated into the national security architecture. An exploratory research design was employed, utilising publicly available archival documents as secondary data sources. The study revealed a significant disconnect between security agencies and the communities they are tasked with protecting. It further highlighted the overly centralised nature of Nigeria's security structure, which limits the participation of non-state actors in addressing security challenges. Based on its findings, the study recommended that the effectiveness and funding of security agencies be evaluated based on their engagement with local communities. It also advocated decentralising Nigeria's security architecture by transferring some security responsibilities from the exclusive legislative list to the concurrent list, ensuring that security operations are more community-oriented.

Despite its valuable contributions, this study did not explore the role of Information and Communication Technology (ICT) in intelligence gathering and community safety. The current research aims to bridge this gap by investigating how ICT can be effectively leveraged to improve intelligence gathering and strengthen community security frameworks. This study will contribute to knowledge by examining the technological challenges faced in intelligence operations and proposing practical solutions for integrating ICT tools into Nigeria's security strategies.

Mohammed, Usman, and Yakubu (2024) conducted a study titled "An Assessment of the Roles of Information and Communication Technology (ICT) on National Security: A Case Study of Nigeria Security and Civil Defence Corps, Zaria Division." The study examined how ICT contributes to national security, focusing on the Nigeria Security and Civil Defence Corps (NSCDC) in Zaria. A questionnaire-based survey was employed, using a four-point Likert scale to assess respondents' views. A total of 40 questionnaires were administered, leveraging the literacy of respondents to ensure independent completion. The data was analysed using descriptive statistical techniques, including frequency counts and mean scores. The findings revealed that ICT plays a crucial role in strengthening national security; however, the effectiveness of ICT in crime prevention and intelligence gathering is hindered by several factors, including the low level of ICT skills among security personnel, inadequate security awareness and training, and the lack of governmental commitment to ICT deployment. The study recommended that the NSCDC provide continuous ICT training to its personnel, as equipping security operatives with technological competencies would enhance their ability to combat crime using ICT tools.

While this study provides valuable insights into the role of ICT in national security, it primarily focuses on the functionality and adoption of ICT within a specific security agency. The current study aims to address a broader gap by examining the challenges that hinder the effective use of ICT in intelligence gathering across multiple security agencies and within the broader community. This research aims to identify systemic and operational barriers to the deployment of ICT for intelligence and security management, proposing solutions that enhance inter-agency collaboration and community engagement. By shifting the focus from ICT usage in a single security organisation to a more comprehensive analysis of its role in intelligence gathering and community safety, this study contributes to the growing body of knowledge on leveraging ICT for national security in Nigeria.

Fagbemi, Issa, and Fagbemi (2024) conducted a study on "Intelligence Gathering and Policy Formulation for Addressing Security Threats in Nigeria", examining the role of intelligence in shaping effective security policies. The study underscored the importance of intelligence as the foundation of policy-making, emphasising that national security efforts would be ineffective without accurate and timely intelligence. Using the Triarchic Theory of Intelligence, the research explored the interaction between policymakers and intelligence agencies to formulate security policies that effectively mitigate threats. A qualitative research approach was employed, utilising in-depth interviews with personnel from Nigeria's intelligence community, including the Department of State Services (DSS), the Defence Intelligence Agency (DIA), and the National Intelligence Agency (NIA). Secondary data were also sourced from academic publications, reports, and online materials. The findings highlighted the need for intelligence agencies to gather and disseminate timely information to policymakers, ensuring that security threats are preemptively addressed through informed decision-making. The study concluded that effective policy formulation depends on the seamless collaboration between intelligence agencies and policymakers, emphasising the role of intelligence in national stability.

However, this study did not address the role of Information and Communication Technology (ICT) in intelligence gathering and community safety, nor did it examine the technological challenges affecting intelligence operations. The current research seeks to fill this gap by analysing how ICT tools can improve intelligence processes, enhance surveillance, and facilitate real-time data sharing for community safety. This study contributes knowledge by identifying technological barriers to intelligence operations and proposing actionable solutions for integrating ICT into security strategies, thus improving intelligence efficiency and responsiveness.

Afolabi and Dogi (2023) conducted a study examining the role of intelligence operations by the Economic and Financial Crimes Commission (EFCC) in combating cybercrime among youths in the Federal Capital Territory (FCT) of Nigeria. The study used primary and secondary data sources, employing a quantitative approach in which 150 questionnaires were distributed and successfully retrieved for analysis. The research findings highlighted that intelligence-driven operations significantly enhance cybercrime investigations by aiding in the identification and apprehension of cybercriminals. Furthermore, the study identified a growing public concern over the impact of cybercrime on national security. It recommended enhanced inter-agency collaboration, improved analytical and technological capabilities, and strategic policy interventions to curb the rising trend. Despite these contributions, the study primarily focused on financial crimes and cyber-related offences, leaving a gap in understanding how broader intelligence frameworks, particularly ICT-driven intelligence, can be leveraged to enhance overall community safety. The current research addresses this gap by exploring how ICT tools can be optimised to improve intelligence gathering beyond financial crimes, ensuring a more comprehensive approach to security. By integrating ICT innovations, this study seeks to contribute to the knowledge base on intelligence-driven security management, offering strategic solutions for overcoming the barriers to effective intelligence utilisation in Nigeria.

Awotayo et al. (2023) studied the challenges of data gathering within Nigeria's intelligence system and its implications for national security. The study employed a qualitative research approach, utilising secondary data sources such as newspapers, internet publications, and academic literature. The findings revealed that Nigeria's intelligence system is hindered by inadequate data collection, improper utilisation of available data, and inconsistencies in data management and sharing among security agencies. These limitations contribute to security agencies' inability to anticipate and prevent security threats effectively. The study emphasised the need for intelligence-driven security operations and improved inter-agency collaboration to enhance national security. However, while the research identified critical issues in intelligence gathering, it did not comprehensively explore the role of modern ICT tools in overcoming these challenges. The current study seeks to fill this gap by examining how ICT can be effectively integrated into intelligence gathering to improve community safety. By addressing the technological limitations and proposing innovative ICT-based solutions, this study contributes to the broader discourse on intelligence enhancement, offering practical recommendations for policy and security stakeholders in Nigeria.

2. Theoretical Framework:

The study was anchored on Technological Determinism and Human Capital Theory.

2.1. Technological Determinism

This study adopts the Theoretical Determinism theory as a conceptual framework to examine the role of Information and Communication Technology (ICT) in intelligence gathering and community safety efforts in Abuja, Nigeria. Initially introduced by Thorstein Veblen in 1921 and later developed by Marshall McLuhan in the 1960s, the theory asserts that technological advancement is a principal driver of societal transformation, influencing human behaviour, institutional structures, and modes of interaction (Chandler, 2000).

Veblen's early formulation highlighted how innovations in industrial machinery reshaped labour systems and societal values. McLuhan later extended this idea within the field of media and communication, famously arguing that *"the medium is the message",* a phrase suggesting that the characteristics of communication technologies significantly shape societal experiences, often more so than the content they deliver (McLuhan, 1964). Central to this theory is the belief that technology evolves independently and catalyses social change.

Technological determination provides a valuable lens through which to explore the limitations and potential of ICT in addressing security challenges in Abuja. Despite the emergence of sophisticated tools such as surveillance systems, digital databases, and cybersecurity technologies, their adoption in Nigeria's security operations remains hindered by infrastructural deficiencies, limited technical capacity, and ethical concerns. This gap between technological availability and effective utilisation underscores the theory's relevance in identifying obstacles and recommending practical solutions.

The theory reinforces the understanding that transformative technology is not self-implementing. Its impact depends on accessibility, strategic integration, and competent management. For ICT to make a meaningful contribution to national security strategies, essential infrastructures such as reliable broadband connectivity, drone surveillance, and biometric identification systems must be in place and supported by skilled personnel. Technological Determinism underpins this study's theoretical foundation by illustrating how technological progress can enhance intelligence gathering and improve community safety outcomes when adequately aligned with policy and practice.

2.2. Human Capital Theory:

Human Capital Theory (HCT) provided a compelling framework for understanding the limitations and solutions associated with using Information and Communication Technology (ICT) in intelligence gathering and community safety in Abuja, Nigeria. Initially introduced by Theodore W. Schultz in 1961 and later expanded by Gary Becker in 1964, the theory posits that investment in human abilities such as education, training, and healthcare significantly contributes to individual productivity and broader economic development (Schultz, 1961; Becker, 1964). Emerging from the realisation that economic growth depends not only on physical infrastructure but also on individuals' knowledge, skills, and competencies, the theory positions human abilities as a form of capital requiring deliberate investment. Education and skill acquisition are crucial tools for enhancing institutional performance and driving innovation. While widely applied in fields such as economics, education, and public policy, Human Capital Theory has gained increasing relevance in security and intelligence studies, where personnel effectiveness is closely linked to national security outcomes.

This theoretical perspective is highly applicable to the focus of this research. It underscores the notion that the success of ICT tools in intelligence operations hinges not solely on the availability of technology but, more crucially, on the proficiency of those who manage and utilise them. Human Capital Theory aligns with this view by suggesting that without sufficient investment in training, technical expertise, and continuous professional development, the potential of ICT for improving intelligence gathering remains underutilised.

Accordingly, the theory supports the argument that bridging gaps in Nigeria's intelligence architecture requires strategic investment in human capital. Capacity-building programmes, specialised ICT training, and institutional reforms must be prioritised to strengthen the operational competence of security personnel. In doing so, Human Capital Theory reinforces the rationale for a skilled and knowledgeable workforce. It provides a theoretical basis for advocating policies that promote sustainable security solutions through human development.

3. Methodology

3.1. Research Design

This study employed a descriptive survey research design to investigate the challenges and prospects of ICT adoption in intelligence gathering and community safety within Abuja, Nigeria. This design was deemed suitable as it enabled data collection from a representative sample of security personnel, ICT professionals, and community leaders to gain insights into the integration of ICT in intelligence operations (Creswell & Creswell, 2018). The approach facilitated an in-depth examination of obstacles to ICT adoption and provided data-driven recommendations for improving security strategies in Abuja.

3.2. Population of the Study

The study focused on security personnel, ICT professionals, and community leaders actively involved in intelligence gathering and security initiatives in the Federal Capital Territory (FCT), Abuja. The estimated population size was 12,000 individuals, encompassing members of key security organisations such as the Nigeria Police Force, Department of State Security (DSS), Nigeria Security and Civil Defence Corps, private security firms, and ICT experts working in security-related fields (National Bureau of Statistics [NBS], 2022). Community leaders were included as they are crucial in intelligence dissemination and community safety measures.

3.3. Sampling Technique and Sample Size

A cluster sampling technique was used to represent the diverse target population adequately. Abuja was divided into three clusters based on geographical and security significance: the Central District, which houses government security institutions; Urban Districts, consisting of residential and commercial areas with significant security presence; and Peri-Urban Areas, covering the outskirts where community-led security initiatives are prevalent (Patton, 2015). Within each cluster, participants were randomly selected to achieve an unbiased representation. Cochran's formula, well-suited for large populations (Cochran, 1977), was used to determine the appropriate sample size. Three hundred eighty-four (384) respondents were selected, ensuring the reliability and generalizability of the findings (Babbie, 2020).

3.4. Sources of Data Collection

This study used both primary and secondary data sources. Primary data were collected through structured questionnaires administered to security personnel, ICT specialists, and community leaders (Bryman, 2016). The questionnaire was designed to capture demographic details, barriers to ICT adoption in intelligence gathering, the extent of ICT usage, and potential solutions. Secondary data were obtained from government security reports, policy documents, and scholarly articles on ICT applications in intelligence operations (Ajayi, 2019).

3.5. Instrument for Data Collection

A structured questionnaire served as the principal data collection tool. It comprised sections covering demographic characteristics, ICT adoption challenges, the impact on intelligence activities, ICT integration levels, and possible interventions (Fowler, 2014). The questionnaire primarily featured closed-ended and Likert-scale questions to facilitate quantitative analysis.

3.6. Validity and Reliability of the Instrument

To ensure the validity of the research instrument, experts in security studies and ICT from the Department of Security and Strategic Studies at Nasarawa State University, Keffi, reviewed the questionnaire for content and face validity (Bell, 2022). A pilot study was conducted with 30 security personnel to assess the clarity and relevance of the questionnaire items. Based on feedback, minor modifications were made to enhance comprehension. Reliability was assessed using Cronbach's Alpha, yielding a coefficient of 0.82, which indicates strong internal consistency and reliability (Kline, 2015).

3.7. Method of Data Analysis

The collected data were analysed using descriptive and inferential statistical techniques (Pallant, 2020). Descriptive statistics summarised the responses, including percentages, means, and standard deviations. Inferential statistical methods, specifically chi-square tests and regression analysis, were used to explore the relationship between ICT challenges and intelligence-gathering efficiency (Field, 2018). The Statistical Package for the Social Sciences (SPSS) version 26 was employed for data analysis to ensure precision and reliability.

4. Data Presentation and Analysis

The survey administered 384 questionnaires, of which 373 were successfully retrieved and deemed valid, resulting in a 96% response rate. Only 11 questionnaires (6%) were either unreturned or invalid. This high retrieval rate underscores the effectiveness of the data collection process, ensuring the reliability and representativeness of the results. Figure 1 illustrates this distribution.

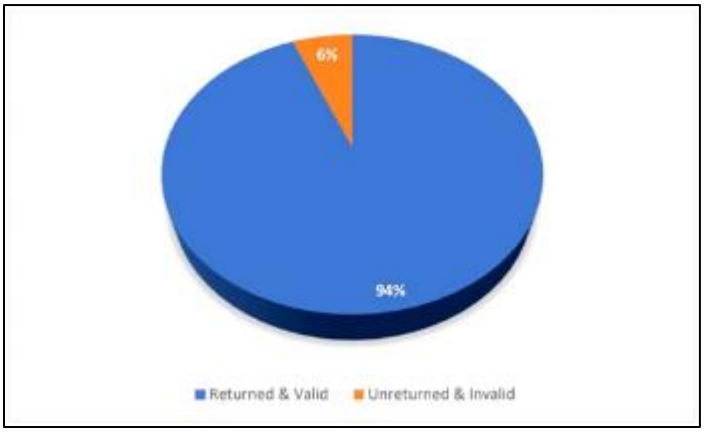

Figure 1 Analysis of Response Rate

Table 1 Demographic Characteristics of Respondents

Variable	Category	Frequency (N=373)	Percentage (%)
Age	18–30 years	82	22.0%
	31–40 years	134	35.9%
	41–50 years	98	26.3%
	51 years and above	59	15.8%
Profession	Security Personnel	175	46.9%
	ICT Specialists	108	29.0%
	Community Leaders	90	24.1%
Years of Experience	1–5 years	97	26.0%
	6–10 years	145	38.9%
	Above 10 years	131	35.1%

Source: Field Survey, 2025

The findings presented in Table 1 reveal that the most significant proportion of respondents (35.9%) fell within the 31–40 years age bracket, followed by those aged 41–50 years (26.3%). Regarding professional distribution, security personnel formed the majority at 46.9%, while ICT specialists and community leaders accounted for 29.0% and 24.1%, respectively. In addition, most respondents (74%) had over six years of experience in their respective fields, highlighting their substantial expertise in security operations and ICT-driven intelligence gathering. These demographic characteristics enhance the credibility and relevance of the responses, ensuring that the study captures informed perspectives on the challenges and opportunities in intelligence gathering through ICT integration.

Table 2 Key Challenges in ICT Adoption for Intelligence Gathering

Challenge	Mean	Standard Deviation
High cost of ICT infrastructure	4.21	0.86
Lack of government funding	4.45	0.79
Cybersecurity vulnerabilities	4.10	0.92
Inadequate ICT training for security personnel	4.32	0.85
Diversion of allocated funds	4.58	0.74
Resistance to technology adoption	3.94	0.97

Source: Field Survey, 2025

Table 2 highlights the significant challenges hindering the effective use of ICT in intelligence gathering across Abuja. The most critical issue identified was the diversion of allocated funds (Mean = 4.58, SD = 0.74), revealing that financial resources meant for intelligence tools are often misused. Similarly, inadequate government funding (Mean = 4.45, SD = 0.79) limits access to essential ICT equipment. A lack of proper ICT training for security personnel (Mean = 4.32, SD = 0.85) further weakens their operational capacity. The high cost of ICT infrastructure (Mean = 4.21) and ongoing cybersecurity threats (Mean = 4.10) remain significant barriers. Although resistance to technology (Mean = 3.94) ranked lowest, it still reflects a need for policy reforms and enhanced staff training.

Table 3 Impact of ICT Challenges on Intelligence Gathering and Security Operations

Options	SD	D	N	A	SA	Mean	Standard Deviation
To what extent does limited access to ICT resources affect intelligence gathering and security?	5%	3%	1%	15%	76%	4.61	0.89
Do you believe insufficient funding for ICT infrastructure hinders effective security operations?	4%	4%	2%	20%	70%	4.54	0.88
How significantly do cybersecurity vulnerabilities expose intelligence data to digital threats?	6%	5%	3%	22%	64%	4.44	0.91
In your view, does the lack of skilled ICT personnel reduce the effectiveness of intelligence work?	7%	6%	4%	18%	65%	4.35	0.92
Do ICT-related issues cause delays in response time during security operations in Abuja?	8%	7%	5%	19%	61%	4.33	0.93

Source: Fieldwork, 2025

The responses from Table 3 reveal that most participants agree that limited access to ICT resources, insufficient funding, and cybersecurity vulnerabilities significantly hinder effective intelligence gathering in Abuja, Nigeria's capital city. High mean scores ranging from 4.33 to 4.61 reflect widespread agreement that weak ICT infrastructure, a lack of skilled personnel, and delayed response times compromise security operations. These challenges underscore a pressing need for improved funding, enhanced cybersecurity protection, and targeted capacity building to enhance intelligence efficiency and ensure community safety.

Table 4 Level of ICT adoption across security agencies

ICT Integration Level	Frequency	Percentage (%)
High adoption	73	19.6%
Moderate adoption	142	38.1%
Low adoption	158	42.3%

The data in Table 4 expresses how ICT has been integrated into Abuja's intelligence gathering and security operations. The results show that only 19.6% of respondents reported a high level of ICT adoption within their agencies. Meanwhile, 38.1% indicated a moderate level, and a majority of 42.3% acknowledged a low level of ICT usage. These findings suggest that ICT tools are not yet widely or effectively used across many security agencies in Abuja, the federal capital city. The dominance of low to moderate adoption levels reflects a continued dependence on traditional, manual intelligence-gathering methods. This limited use of modern technology likely affects the speed, accuracy, and overall efficiency of security operations. As such, the low integration of ICT presents a significant barrier to achieving timely and data-driven community safety interventions.

Table 5 Remedies to the Challenges of ICT Adoption for Intelligence Gathering

Suggested Remedies	Frequency	Percentage (%)
Capacity Building and Training	110	31.4%
Improved Funding and Infrastructure	95	27.1%
Inter-agency Collaboration	80	22.9%
Policy Reforms and Implementation	60	17.1%
Public Awareness Campaigns	28	8.0%
Total	373	100%

Source: Fieldwork, 2025

This section focused on identifying practical solutions suggested by respondents to address the challenges of using ICT in intelligence gathering and enhancing community safety in the Federal Capital Territory of Abuja, Nigeria.

The data presented in Table 5 highlights the key remedies suggested by respondents to overcome the challenges faced in using ICT for intelligence gathering and community safety in Abuja, Nigeria. The most frequently recommended remedy is capacity building and training, endorsed by 31.4% of respondents. This indicates a strong recognition of the need to improve the skills of both security personnel and ICT professionals. Many respondents noted that a lack of technical proficiency in modern ICT tools is a significant barrier. To address this, they suggested regular training programmes, certifications, and continuous on-the-job learning. The second most commonly suggested remedy, identified by 27.1% of respondents, is improved funding and infrastructure. This highlights the need for more financial investment in modern ICT tools, surveillance systems, and secure digital databases. A well-funded infrastructure is crucial for enhancing the effectiveness of intelligence operations. In addition, 22.9% of respondents recommended inter-agency collaboration. They emphasised the importance of creating a centralised intelligence-sharing platform to improve the coordination between key agencies such as the police, the Department of State Services (DSS), and the Civil Defence Corps. Other suggested solutions include updating ICT policies, which 17.1% of respondents mentioned, and raising public awareness about supporting intelligence efforts, indicated by 8.0%. While these recommendations were mentioned less frequently, they are essential in fostering a more coordinated and practical approach to ICT deployment in security operations.

5. Discussion of Findings

The findings of this study indicate that insufficient Information and Communication Technology (ICT) infrastructure poses a significant challenge to effective intelligence gathering in Abuja. Respondents repeatedly cited unreliable internet services, inconsistent power supply, and outdated digital equipment as substantial impediments to the successful use of surveillance systems and data analytics tools. These observations are consistent with Olaoye (2023), who emphasised that infrastructural shortcomings hinder the functionality of technology-driven security systems in Nigeria. Afolabi and Ogu (2020) similarly noted that limited funding further restricts the ability of security institutions to procure and maintain essential technological tools. These challenges reflect the assumptions of Technological Determinism, which argues that societal functions, including national security, are shaped by the availability and quality of technological resources. As such, the absence of robust infrastructure fundamentally limits the effectiveness of intelligence operations. This aligns with the study by Mohammed, Usman, and Yakubu (2024), which found that similar infrastructural challenges weakened the operational capacity of the Nigeria Security and Civil Defence Corps in Zaria.

Additionally, the study revealed a widespread lack of technical competence among security personnel. Many respondents noted that officers are not adequately trained in utilising modern digital tools, including forensic software, artificial intelligence systems, and cybersecurity frameworks. This gap in expertise reduces the practical benefits that ICT can offer in intelligence and crime prevention. These findings align with Baldwin and Black (2021), who pointed to the growing need for specialised ICT skills in contemporary security operations. Hassan and Akpan (2023) advocated for sustained capacity-building programmes to enhance law enforcement capabilities. This position is supported by Human Capital Theory, which holds that investment in education and professional development leads to improved institutional performance. Therefore, the absence of a highly skilled workforce represents a critical bottleneck to the full realisation of ICT in intelligence processes.

The study also highlights ethical concerns associated with the use of ICT in security matters, particularly in areas such as surveillance, data privacy, and the potential for technological abuse. Respondents voiced scepticism regarding the transparency and accountability of intelligence agencies, particularly in the context of limited regulatory frameworks and inadequate data protection policies. These concerns often discourage public cooperation and foster mistrust of security institutions. The findings align with Oye's (2021) observation that public resistance often stems from fears related to civil liberties. Similarly, Weimann (2020) cautioned that excessive surveillance without adequate oversight can erode public confidence and reduce the overall effectiveness of intelligence efforts. Consequently, this study highlights the need for legal reform and institutional checks, in line with Choi's (2022) recommendation for ethical governance models that balance national security and individual rights.

Finally, participants in the study expressed strong support for strategic measures to strengthen the role of ICT in intelligence operations. These include increased funding, international partnerships, and collaborative engagements between public and private sectors. There was a broad consensus on the need for policy reforms, infrastructure upgrades, and sustained capacity-building efforts to enhance intelligence-led security in Abuja. These insights align with Adeyemi (2022), who highlighted the significant role of ICT infrastructure in ensuring public safety, and Tanner and Campana (2022), who underlined the importance of multi-stakeholder collaboration in bridging technological gaps. Moreover, the findings reinforce the arguments of Bassey and John (2023), who advocated for inclusive strategies that engage citizens through digital platforms. Altogether, these perspectives suggest a shift from a reactive and under-resourced security model to a forward-looking system grounded in innovation, accountability, and inclusive governance.

6. Conclusion

This study establishes that integrating Information and Communication Technology (ICT) into intelligence gathering and community safety operations within Abuja, Nigeria, holds significant potential but faces notable challenges. The major obstacles identified include poor digital infrastructure, limited technical expertise among security personnel, financial constraints, and ethical concerns surrounding surveillance and data privacy. Despite these limitations, the research demonstrates that ICT remains an indispensable tool for advancing national security and enabling a more proactive approach to crime prevention. This study's direct conclusion is that the full impact of ICT on security can only be realised through strategic investment, skill development, and policy reform. The research also affirms that the success of any ICT-driven intelligence system depends on its alignment with ethical standards and public trust.

Recommendations

The Federal Government, in collaboration with the Federal Capital Territory Administration and relevant ministries, should urgently prioritise the development and modernisation of ICT infrastructure across all security and intelligence agencies operating in Abuja. Key investment areas must include high-speed broadband connectivity, a stable and reliable power supply, intelligent surveillance systems such as CCTV with facial recognition capabilities, and integrated digital platforms for real-time data processing and analysis.

To bridge the digital skill gaps within the security sector, agencies must institutionalise continuous professional development programmes focused on ICT competencies. These should include regular in-service training and workshops covering cybercrime detection, digital forensics, the use of artificial intelligence in surveillance, ethical data protection practices, and information systems management. In addition, ICT modules should be embedded into the recruits' curriculum. Investing in the human capital of security personnel will ensure that emerging technologies are effectively used to strengthen intelligence gathering and improve community policing initiatives.

A dedicated budget line for ICT development within national and subnational security funding structures is essential for sustainable digital transformation. This funding should cover the acquisition of up-to-date technological tools, software upgrades, personnel capacity building, and regular maintenance of the digital infrastructure.

Comprehensive legal and policy reform is urgently needed to guide the ethical application of ICT in security and surveillance operations. Laws and regulations should be enacted or revised to guarantee citizens' data privacy, clearly delineate the limits of surveillance, and provide strict guidelines to prevent the misuse of digital tools. These legal provisions must also include oversight, transparency, and redress mechanisms to strengthen public trust.

Security agencies should actively collaborate with private technology firms, academic institutions, and civil society organisations through structured partnerships to drive innovation, facilitate knowledge exchange, and co-design solutions for local security challenges. Establishing ICT innovation hubs and digital capacity-building centres would

promote the development of tailored surveillance technologies and encourage technological literacy. In addition, engaging communities through digital reporting tools and participatory surveillance systems will improve the accuracy of intelligence collected and enhance public trust, as well as a shared sense of responsibility for safety outcomes.

To ensure responsible and strategic ICT deployment, regulatory and oversight institutions such as the National Information Technology Development Agency (NITDA) must be fully empowered to enforce compliance with digital security standards, coordinate policy implementation, and provide technical support to security agencies. Simultaneously, legislative bodies, particularly the National Assembly Committees on Security and ICT, should be more active in monitoring execution, reviewing outdated policies, and evaluating budget performance. A robust and coordinated governance framework will help align ICT use with national security priorities, legal standards, and ethical principles.

Compliance with ethical standards

Statement of ethical approval

The conduct of this study adhered strictly to the ethical principles governing research involving human participants. Before the commencement of data collection, ethical clearance was duly obtained from the *Department of Mass Communication Research Ethics Committee, Faculty of Social Sciences, Nasarawa State University, Keffi, Nigeria*. All participants were adequately informed of the study's objectives, scope, and voluntary nature through a formal consent process.

Informed consent was obtained from each respondent, with assurances given regarding anonymity, confidentiality, and the right to withdraw at any stage without any form of penalty. The research design incorporated measures to safeguard the dignity, privacy, and autonomy of all respondents. No identifying information was collected or recorded, and all data were handled with strict adherence to data protection and ethical governance protocols.

This study conformed to internationally accepted ethical standards, including the principles outlined in the *Declaration of Helsinki*, and complied with relevant institutional and national research ethics regulations. As a scholar, I accept full responsibility for the integrity of the ethical procedures applied in the execution of this research.

Statement of informed consent

According to ethical research standards, informed consent was obtained from all participants before they participated in the study. Each participant was provided with a clear explanation of the study's purpose, scope, procedures, and their expected contributions. They were also informed of their right to decline participation or withdraw at any stage of the research without any adverse consequences.

Participants were assured that their responses would remain strictly confidential and that any data provided would be used solely for academic and research purposes. No identifying information was collected or disclosed in the course of the study. By voluntarily participating, each respondent indicated their understanding and acceptance of the terms outlined in the consent briefing.

All consent procedures were conducted in accordance with institutional ethical guidelines and aligned with international research ethics frameworks, including the principles outlined in the *Declaration of Helsinki*.

References

[1] Adegbite, A., & Okonkwo, C. (2021). ICT and intelligence gathering in Nigeria: Opportunities and challenges. African Journal of Security Studies, 8(2), 112-135.

[2] Afolabi, O. (2022). ICT and urban security: Challenges and opportunities in Nigeria. Journal of African Security Studies, 12(4), 233-245.

[3] Adebayo, T., & Olaleye, K. (2023). Challenges in Digital Surveillance: Assessing ICT Gaps In Nigerian Security Agencies. African Journal of Security Studies, 15(2), 45-67.

[4] Adeyemi, T. (2022). Public-private partnerships and ICT infrastructure development in Nigeria: A pathway to enhanced security operations. African Journal of Security Studies, 14(2), 112–130.

[5] Adelani, S. I., Zamani, A. E., Igwebuike, P. O., Adedayo, L. O., & Mba, U. (2023). Impact of Community Policing in Security Management: Kubwa, Bwari Area Council, FCT-Abuja. International Journal of Conflict and Security Management, 1(1), 42–54. Retrieved from https://ijsmpcr.com/index.php/ijsmpcr/article/view/20

[6] Afolabi, M. B., & Dogi, I. G. (2023). Intelligence, Financial Crimes Commission, and war Against cybercrime among youths in the Federal Capital Territory in Nigeria. Jalingo of Social and Management Sciences, 5(2), 61–75.

[7] Afolabi, T., & Ogu, C. (2020). Bridging the digital divide: Capacity building for ICT adoption In intelligence gathering in Nigeria. Journal of African Security and Intelligence, 9(1), 45–62.

[8] Awotayo, O. O., Omitola, A., Omitola, B., & Oderinde, S. L. (2023). Intelligence system and National security in Nigeria: The challenges of data gathering. Janus.net, e-journal of international relations, 14(2), November 2023–April 2024. https://doi.org/10.26619/1647-7251.14.2.8

[9] Baldwin, D. A., & Black, J. (2021). Intelligence analysis: A comprehensive introduction to Methods and practices. Oxford University Press.

[10] Bassey, A. U., & John, P. K. (2023). Surveillance technology and community safety: Examining the role of ICT in urban security management. Journal of Mass Communication and Society, 18(4), 321–345.

[11] Becker, G. S. (1964). Human Capital: A Theoretical and Empirical Analysis, with Special Reference to Education. University of Chicago Press.

[12] Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589-597.

[13] Castells, M. (2020). The Rise of the Network Society (3rd ed.). Wiley-Blackwell.

[14] Chandler, D. (2000). Technological or Media Determinism. Retrieved from http://visual-memory.co.uk/daniel/Documents/tecdet/tdet01.html

[15] Clarke, R. (2019). ICT and intelligence gathering: The new frontier in security management. International Journal of Security and Technology, 5(2), 115-130.

[16] Clarke, R. A. (2019). Big Data, AI, and Cybersecurity: Implications for Digital Intelligence. Cambridge University Press.

[17] Clarke, R. A. (2019). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

[18] Creemers, R. (2021). China's Surveillance State: AI, Big Data, and the Future of Policing.

[19] Cambridge University Press. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and Mixed methods approaches (5th ed.). SAGE Publications.

[20] Eze, C. (2021). Cybersecurity Challenges in Nigeria: Emerging Threats and Strategic Responses. Nigerian Journal of Digital Security, 7(1), 112-130.

[21] Fagbemi, A. S., Issa, A. G., & Fagbemi, C. A. (2024). Intelligence gathering and policy Formulation for addressing security threats in Nigeria. African Journal of Humanities and Contemporary Education Research, 16(1), 139–149. https://doi.org/10.62154/ajhcer.2024.016.010423

[22] Ibrahim, M., & Bello, A. (2020). Cybersecurity concerns in Nigeria's security sector: ICT Challenges and solutions. African Journal of Information Systems, 8(3), 45-60.

[23] Lowenthal, M. M. (2021). Intelligence: From secrets to policy (9th ed.). CQ Press.

[24] Lowenthal, M. M. (2021). Intelligence: From Secrets to Policy (8th ed.). CQ Press.

[25] Mabunda, K. (2022). Digital Policing in South Africa: Opportunities and Constraints. South African Security Review, 10(3), 78-95.

[26] McLuhan, M. (1964). Understanding Media: The Extensions of Man. New York: McGraw-Hill.

[27] Mohammed, S., Usman, A., & Yakubu, J. (2024). An assessment of the roles of information And communication technology (ICT) on national security: A case study of the Nigeria Security and Civil Defence Corps, Zaria Division. Journal of African Advancement and Sustainability Studies, 5(2). Retrieved from https://ssaapublications.com/index.php/sjaass/article/view/250

[28] National Bureau of Statistics. (2023). Annual Security and ICT Report. Abuja, Nigeria.

[29] Olaoye, S. (2023). ICT infrastructure in Nigeria: Challenges and solutions for security intelligence. African Journal of Digital Technology and Governance, 11(3), 210–230.

[30] Oye, J. (2021). Political interference and intelligence gathering: The role of ICT in mitigating manipulation risks. Journal of Political and Security Studies, 15(2), 98–115.

[31] Ogunyemi, F. (2023). ICT and Intelligence Gathering: Enhancing Nigeria's Security Infrastructure. Journal of African Technological Innovations, 6(4), 90-113.

[32] Okonkwo, J. (2022). The Role of Cybersecurity in Nigerian Security Operations. Nigerian Journal of Cyber Studies, 5(2), 34-56.

[33] Olumide, O. (2022). The role of ICT in combating crime in Nigeria's urban centres. Journal of Nigerian Studies, 14(1), 88-102.

[34] Olayemi, M. (2022). The role of digital technologies in crime prevention and intelligence gathering in Nigeria. Journal of African Security, 10(3), 210–228.

[35] Sampson, R. J., & Eck, J. E. (2020). Crime prevention and community safety: New perspectives On policing and security. Routledge.

[36] Sampson, R. J., & Eck, J. E. (2020). Crime Prevention and Community Safety: New Directions (2nd ed.). Routledge.

[37] Schultz, T. W. (1961). Investment in human capital. The American Economic Review, 51(1), 1–17.

[38] Silva, R., & Souza, L. (2020). Predictive Policing in Brazil: An ICT-Based Approach to Crime Prevention. Latin American Security Journal, 8(1), 22-40.

[39] Singer, P. W., & Brooking, E. T. (2018). LikeWar: The Weaponisation of Social Media. Houghton Mifflin Harcourt.

[40] Taber, K. S. (2018). The use of Cronbach's Alpha when developing and reporting research instruments in science education. Research in Science Education, 48(6), 1273–1296.

[41] Veblen, T. (1921). The Engineers and the Price System. New York: B.W. Huebsch.

[42] Waziri, B., & Yakubu, M. (2021). ICT in security management: A focus on intelligence Gathering in northern Nigeria. Journal of African Security and Peace Studies, 9(1), 67-82.

[43] Williams, C. (2020). Intelligence and Surveillance in the UK: The Role of ICT in Modern Security. British Journal of Intelligence Studies, 12(1), 56-79.

[44] Williams, P. (2020). Digital Policing and Crime Prevention: The Future of Technology in Law Enforcement. Palgrave Macmillan.

[45] Wright, A. (2020). Enhancing security through ICT: A review of emerging technologies. Global Security Review, 18(2), 56-78.

[46] Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper & Row.