REVIEWED JOURNAL of INTERNATIONAL SOCIAL SCIENCE & HUMANITIES
[ISSN 2663-127X]

Vol. 5, Iss. 1 (2024), pp 257 – 270, May 11, 2024. www.reviewedjournals.com, ©Reviewed Journals

MOBILE PHONE TECHNOLOGY ADOPTION BY THE POLICE AS A COUNTER TERRORISM MEASURE IN NAIROBI CITY COUNTY, KENYA

[1] Daniel S. Kandie & [2] Dr. Stephen Handa, PhD

[1] Candidate, Master of Arts in Leadership and Security Management, School of Law, Arts and Social Sciences, Kenyatta University, Kenya

[2] Lecturer, Department of Security, Diplomacy and Peace Studies, Kenyatta University, Kenya

Accepted: April 22, 2024

ABSTRACT

The study investigated the utilization of mobile phone technology by the National Police Service (NPS) in Nairobi City County (NCC) to combat the increasing threat of terrorism. With a notable gap in existing research on this topic, the purpose was to explore how mobile phone technology was employed within the NPS's counter-terrorism efforts. The objectives included assessing the extent of mobile technology adoption, identifying influencing factors, and understanding the challenges encountered by the NPS in utilizing this technology. Through a focused examination of the Anti-Terrorism Police Unit (ATPU) and specific mobile technologies utilized, the study sought to answer research questions pertaining to the extent, reasons, and limitations of the NPS's use of mobile phones for counter-terrorism. The study reviewed literature objectively with the aid of theories that included: Actor-Network Theory (ANT), the Technology Acceptance Model (TAM), and Unified Theory of Acceptance and Use of Technology (UTAUT). This study used a descriptive survey research design with qualitative and quantitative approaches to investigate the adoption of mobile phone technology by police officers in counterterrorism in NCC, Kenya. The target population of the study was police officers of all cadres from police constable to Gazetted officers based at ATPU. A stratified random sampling method was used to select a sample of 207 respondents. Data was collected using questionnaires and interviews. Quantitative data was analysed using descriptive statistics, while qualitative data was analysed thematically. The findings of the study revealed that police officers in NCC are aware of the benefits of using mobile phone technology in counterterrorism. However, there are a number of challenges that hinder the adoption of this technology, such as lack of training, lack of funding, and security concerns. The study recommends that the government should provide more training and funding to police officers so that they can effectively use mobile phone technology in counterterrorism. In conclusion, although moderate adoption exists, the full potential remains untapped. Factors influencing adoption were identified, including infrastructure, funding, training, collaboration, and policy support. Challenges like limited resources, technological barriers, and privacy concerns hinder optimal utilization. Recommendations focus on investment in infrastructure, securing adequate funding, and providing comprehensive training, fostering interagency collaboration, and addressing privacy concerns. These findings hold significant implications for stakeholders: Policymakers and law enforcement agencies can enhance counterterrorism efficiency and coordination by investing in technology and fostering collaboration. By addressing the recommendations, the safety and security of NCC and similar regions can be improved.

Key Words: *Mobile Phone Technology, Police Counter Terrorism Measure*

CITATION: Kandie, D. S., & Handa, S. (2024). Mobile phone technology adoption by the police as a counter terrorism measure in Nairobi City County, Kenya. *Reviewed Journal of Social Science & Humanities*, 5 (1), 257 – 270.

INTRODUCTION

Rising global threats with criminals who have extensive networks across regions and continents calls for prompt action to have integrated systems that are readily available to curb and mitigate criminal activities (Faith & Bekir, 2015). Terrorist activities are increasingly turning out to be complex and continuously evolving. Furthermore, the motives of terrorism, methods used in attack, financing and rationale for the target are constantly evolving. All these issues have made it hard for actors to fully counter terrorism activities (Ragab, 2015). However, the growing need to fight terrorism around the world has been demonstrated by United Nations (UN) through establishment of the Office of Counterterrorism. The Office of Counterterrorism provides capacity building, coordination, and leadership to member States to effectively counter terrorism (Feyyaz, 2020). Because of the increased role of the Office of counterterrorism in promoting sustainable development as espoused by goal 16 of the Sustainable Development Goals (SDGs), (UNODC, 2019), actors including police should device relevant strategies of countering terrorism.

In the United States of America (USA), the adoption of mobile phone technology has been widespread. As of 2021, 96% of Americans owned a cell phone, and 81% owned a smartphone. The ubiquity of smartphones has facilitated various aspects of law enforcement, including communication, data collection, and information sharing. Mobile apps and technologies have been used in crime mapping, emergency response, and even to improve community policing efforts. In most developed countries around the world like USA, police are relying on mobile phones to trace and detect explosives as a way of countering terrorism (Miller, 2006). This is enhanced and supported by mobile phone technology to counter terrorism. Explosive Tracing Mobile Technology Directive (ETMTD) is a form of mobile telephony with capability to detect explosives over a specified territory (Chakraborty & Chakraborty, 2008). The European Union (EU) has realized the need to embrace mobile phones to counter terrorisms among member States. In 2018, EU had plans to share official alerts to the mobile phones of the Europeans through Reverse 112 system whenever they were nearing terrorist attacks. These efforts were in response to Paris attack whose cause was due to lack of early warning (Boffey, 2018). Similar system also exists in the USA, which alert citizens of terror attacks and how best to remain safe.

The use of mobile telephony in countering terrorism is not without challenges. Presently, there are encrypted apps like WhatsApp and Telegram that help jihadists to communicate as they evade police tracking. These encrypted apps also complicate the efforts made by police to decode the messages of terror groups hence making it hard to counter terrorism (Moutot, 2018). In support of this assertion, Graham (2016) shared that mobile telephones are supported by messaging apps that are encrypted, and this is being exploited by terror groups to plan and execute terror attacks securely. Although it is hard to break the end-to-end encrypted message communicated through mobile phones, police officers in some advanced countries like USA have been able to hack software of these devices on ends while accessing information of the terrorists. Getting evidence from terrorism cases can be complex, with some demanding technological or forensic experts which emerge as a challenge especially for less developed and developing countries like Malaysia.

In Nigeria, Boko Haram terror group broke into global limelight in April 2014 after raiding into a state Chibok girl's secondary school in Borno state and abducted 276 schoolgirls from their Dormitories (Hill, 2014). As part of state's counter insurgency measures, a state of emergency was imposed where Nigeria security agencies shut down mobile phone networks in Adamawa, Borno and Yobe states in Northeast Nigeria. While mobile telephony has functioned as a tool for development, it has served as an enabling tool in the hands of boko Haram terrorists. As a capability essential for strategic planning, attacks, surveillance, timings as well as simultaneity of mobile communications for coordination and activation of cell members. Oluniyi (2010) observed that police role is to identify ownership of mobile phone numbers, track the handsets, and thus identifies the geographical location of kidnappers as they solicit for ransom. In Uganda just like South Africa,

police engage the use of MOBI-Applications in mobile phones to aid in location of the nearest police stations in need of help (The Justice Law & Order Sector, 2019).

Kenya has witnessed significant terror attacks that have claimed hundreds of lives in the past decade. The Garissa University attack is one of the high profiled terror incidents in the country in 2015 that claimed the lives of 147 students. The trial court in Nairobi sentenced three accused persons to life imprisonment and 41 years respectively and that the court found the three accused persons had been in constant mobile communication with four other attackers at the time of the attack in the early morning of April 2nd, 2015 before shooting to death the innocent students (DW, News Report, 2020). Responding to these terror concerns, the use of mobile phones to curb terrorism has been on a rise among police in Kenya. There are emergency call numbers (112/999, #FichuaKwaDCI 0800 722 203) where terror or emergency victims can dial through their mobile phones to access police services (Kenya National Police Service, 2021). Besides the emergency calls, police rely on mobile phones to track information on money movement for tracing financiers of terrorism and call logs, messages, pictures as well as videos to track down and bring terror suspects to law (Kenya National Police Service, 2016).

NCC has witnessed a number of terror attacks planned and executed by Al Shabaab group just like in many other parts of the country like Mombasa, Wajir and Garissa Counties. Top on the list of these terror incidences include the Westgate attack and Dusit2 attack. Documents filed in Nairobi court, Kenya by the Anti-Terrorism Police Unit (ATPU) in the recent terror attack in the capital city of Nairobi as evidenced by the ongoing prosecution of terror suspects linked to the attack showed that one of them transacted at least 100 million Kenyan shillings through mobile money some few months before the incident.

Another suspect received over 90,000 US dollars via mobile phone from South Africa and that the same was channelled to the terror suspects through 47 SIM cards. It was further observed that most of the suspects charged before court were mobile money agents who facilitated SIM card and mobile phone registration as well as bulk withdrawals (Nairobi Court Records, 2020). The available literature places emphasis on Kenya as whole without specifically focusing on Nairobi (Tanui & Barmao, 2016). For instance, Magogo (2017) examined the effectiveness of counter terrorism strategies in Kenya and specifically focused on mobile phone tracking technologies in relation to crime prevention and not terrorism. Thus, it is against this background that this study seeks to establish the extent to which police adoption of mobile phone technology has contributed towards countering of terrorism in Nairobi.

Statement of the Problem

Kenya's landscape has borne witness to a marked surge in acts of terrorism, gravely imperilling national security and public safety. In response to the increasing threat of terrorism in NCC, Kenya, efforts have been made to adopt mobile phone technology within the police service as a counter-terrorism measure. Recognizing the importance of mobile technology in enhancing communication, data collection, and intelligence sharing, initiatives have been undertaken to address the lack of mobile telephony infrastructure within the police service. These efforts aim to optimize the utilization of mobile phones in counter-terrorism investigations, with a focus on improving information dissemination, coordination between law enforcement agencies, and rapid response capabilities. While efforts have been made to adopt mobile phone technology within the police service as a counter-terrorism measure in NCC, Kenya, certain aspects have not been adequately addressed. Specifically, there remains a lack of comprehensive assessment regarding the extent of mobile phone technology utilization by law enforcement agencies, factors influencing its adoption, and the specific challenges hindering its integration into counter-terrorism strategies. Additionally, there is a dearth of in-depth studies examining the effectiveness and impact of mobile phone technology in mitigating terrorist threats within Nairobi City. Furthermore, there is limited focus on developing tailored training programs and

capacity-building initiatives to equip police officers with the necessary skills and knowledge to leverage mobile technology effectively in counter-terrorism operations.

Purpose of the Study

The purpose of the study was to explore National Police Service efforts in countering terrorism through adoption of mobile phone technology in Nairobi City County, Kenya. The specific objectives of the study were to:

- Examine extent of mobile phone technology adoption by the NPS in countering terrorism in Nairobi City County, Kenya.
- Assess factors influencing National Police Service in adoption of mobile phone technology in countering terrorism in Nairobi City County, Kenya.
- Analyse the challenges faced by National Police Service in adopting mobile phone technology in counter terrorism in Nairobi City County, Kenya.

The study ought to answer the following research questions:

- What extent has mobile phone technology been adopted by National Police Service to counter terrorism in Nairobi City County, Kenya?
- What factors influence National Police Service adoption of mobile phone technology in counter terrorism in Nairobi City County, Kenya?
- Which challenges are faced by the National Police when adopting mobile phone technology in counter terrorism in Nairobi City County, Kenya?

LITERATURE REVIEW

Theoretical Framework

Actor-Network Theory

ANT is a theoretical and methodological approach to social theory where everything in the social and natural worlds exists in constantly shifting networks of relationships. It posits that nothing exists outside those relationships. All the factors involved in a social situation were on the same level, and thus there were no external social forces beyond what and how the network participants interacted at present. Actors or actants are not objects, but an association between different elements that in themselves created their own network (Cresswell, Worth, & Sheik, 2010) and emphasizes the interplay between human actors and non-human actors (including technology) in shaping social systems. In this sense, analyzing the adoption of mobile phone technology by police for counterterrorism purposes involved understanding the complex network of relationships between different stakeholders, including police organizations, technology providers, policymakers, and the wider public.

Among the several influential scholars in the field of ANT included Bruno Latour who was widely regarded as the founders of ANT. Latour's studies emphasized the agency of both human and non-human actors and the complex network of relationships between them. Michel Callon’s work focused on the processes of enrolment and translation, emphasizing how actors and technologies were mobilized and transformed through networks of relations. This work explored the interplay between human and non-human actors in shaping social order and technological change. John Law was another contributor and supporter of the theory, whose work highlighted the role of power, politics, and the materiality of technology in shaping networks of actors. The concept of "heterogeneous engineering" underscored the idea that the development of technologies involved multiple actors with diverse interests and influences.

The Technology Acceptance Model

The TAM or theory was developed in 1989 by Fred Davis and models the user's intention on how to adopt and make use of technology. It suggests that when users adopt a new technology it becomes challenging on how to use the said technology. Marangunic & Granic (2015) posits that the model intends to find out factors that facilitate integration of technologies into an organization and why users accept or reject technology. It provides insight into a thorough examination of many factors that explains software enjoyment and performance. It provides a focal point as regards technology on whether users will adopt appertaining to perceived usefulness and ease of use of that technology. Davis (1989) observed that using a given system would intensify job performance and further perceives to be so beneficial for what they intend to achieve.

The TAM and the subsequent TAM2 and TAM3 which, were later the extension of the original TAM, were redefined to pave way for a worthy theoretical model that suits emerging mobile policing dimension. Based on this study, it identified the following four categories of issues of concern that are: the acceptance factors, performance, security/reliability/ usability, management style and finally the cognitive. Venkatesh & Davis (2000) in their study included subjective norm, voluntariness, image, experience, and cognitive instrument processes such as job relevance and output quality. In their study they further observed that they were likely to have some effects or consequences in an individual job performance, the possible influence of the peers on their behaviours based on their experience (subjective norms) and further how an individual may always examine how a given system performs while using the technology.

Unified Theory of Acceptance and Use of Technology

The proponents of this theory (Venkatesh *et al*, 2003) explained the intention of the users by making use of the information system while observing their behaviours. It is guided by four factors of intention and usage. Further subdivided into four moderators showing their relationships. According to these proponents, there are several core constructs to these theories. The proponents further cited social influence as a strong reflection that indicates the level at which an individual could use the system and facilitate conditions which an organization and its infrastructure exists to support the use of the system. Police officers when using mobile phone technology need to ensure that they meet the required performance. The more police officers get used in utilization and usage of mobile phone technology the more they get used to it. The perception of others using the technology will influence the adoption of mobile phone technology by police officers themselves. When other colleagues in the organization perceives the important usage of the technology will motivate them to make use of it.

Empirical Literature Review

Extent of Mobile Phone Technology Adoption in Counter Terrorism

According to Cornish (2010), technology is instrumental in countering terrorism. The study proceeded with studying counter terrorism strategies using technology in the UK which they applied in a bid to tackle international terrorism. The study opines that there is need to understand how relevant technology is in the context of counter terrorism practices. The rhetoric is on the premise that there may emanate a need to develop or maintain a greater advantage over the adversary without underestimating or overestimating their capability in using sophisticated technologies in countering attacks. The study highlights on technologies such as the use of surveillance systems and Closed-Circuit Televisions (CCTVs). Though relevant, the study presents contextual gaps as it was conducted in the UK. Further, the study does not include mobile phone technology which is the basis for this study.

Kumar (2019) studied the use of modern technology to counter terrorism. The study highlights, communication technology which allows the terrorist groups to easily share information through encrypted messages thereby giving them an upper hand in launching attacks. Terrorists further leave no stones unturned, by pursuing the use of technologies themselves to increase the likelihood of success of operations which

culminated in using improvised technologies to launch attacks. The booming of new technologies such as AI can guarantee that the groups would eventually seize them for their use. For this reason, there is need for countries to develop systems to keep up with the evolution and diverse use of technologies by their adversaries not only for the sake of competitive advantage but also to ensure that counter terrorism approaches remain relevant and strategic. Therefore, traditional systems for countering terrorism are by far weak as they are outdated. The study highlights a variety of technologies including AI, facial recognition systems, self-driven vehicles, using cyber space amongst others. The study however does not include mobile phone technology which this study explores.

A study by Kshetri and Voas (2017) examined the use of CDRs in counter terrorism investigations in the United Kingdom. The authors found that CDR analysis was a valuable tool for identifying key players in terrorist networks, and for tracking the movements of suspects. They also noted that the use of CDRs raised some ethical concerns, particularly around privacy and data protection. Another way in which mobile phone technology has been used in counter terrorism investigations is using mobile forensics. This involves the analysis of data stored on a mobile phone, such as text messages, emails, and social media posts. This can provide valuable intelligence about the activities and intentions of suspects.

Factors Influencing Police adoption of Mobile Phone Technology in Counter Terrorism

Lee (2007) recognized private risks, information sharing in counter terrorism while examining the websites and exploring the relationship between government and citizens in a turbulent environment. It was established that civilian security and safety lies in the hands of the government. The use of technology in this case; websites, was cited to be embraced in a lukewarm fashion. This is because of the perceived privacy risks which can easily demotivate government actions where citizens show concern for information sharing with law enforcement which may jeopardize their privacy. The study further established that citizen belief in the authorities' competence influences the likelihood of use of a technology to prevent crimes. However, the study fails to outline on the concept of mobile phone technology and its potential to aid in counter terrorism approaches.

Chaudhary (2020) looked at the role of information and communication technologies in combating terrorism. Further, highlights various factors of motivation that can support the need for having technology when it comes to security. Having armed personnel, the need for secure internet services, arm imports, secure trade, and foreign direct investments as well as tourism were dominant motivating elements. It established the development of Information Communication Technology (ICT) as a promoter against terrorism which enhance the development of the tourism industry at large. However, the study discussed technologies in general which did not include the potential of mobile phone technology in counter terrorism investigation which is the objective of this study.

Mwasaa (2010) concentrated on factors that pervade the adoption of mobile phone in Kenya. The study pointed out that perceived usefulness and ease of use informs the adoption of mobile phone technology. This means that when the users believe using a given form of technology like mobile phone would be useful to them, it would readily be adopted among the users. The same case applies when the users perceive mobile phone technology to be easy to use; they would readily take it up. However, this study looked at adoption of technology in general, unlike the present study that will focus on mobile phone technology and its adoption among police in countering terrorism.

Challenges faced by Police in Adopting Mobile Phone Technology in Counter Terrorism

Tanner & Meyer (2015) studied police work and new security devices in Canada. In their study, they noted that mobile technologies have encompassing changes in police work. The study noted that it was challenging for the law enforcement to adapt to new technologies which could create occupational tensions between the imagined benefits of devices and the unexpected outcomes of service. The article features some of the perceptions that police have with mobile devices where the police cited that accessing technological

equipment and resource off campus can be difficult notwithstanding the progressive need to acquaint oneself with sophisticated technology. The study however does not include challenges in police adoption of mobile phone technology in counter terrorism.

Egnoto (2017) observed that various motivations for the adoption of technology amongst the police, would readily use equipment on duty rather than off duty. Further, concerns regarding the use of technology were raised where the police cited difficulty in carrying personal health, and safety concerns as well as security issues. In addition, untrained personnel were reported to be a major hindrance to the use of technology. Although useful, the study focused broadly on challenges of technological equipment on crime prevention rather than mobile phone technology in counter terrorism which prompts the findings of this study to highlight.

Ndonye (2019) on the other hand studied the implications of technological advancement in Kenya on police performance. Ndoye, established that police use cheap technologies which become obsolete in the wake of new technologies in fighting crime. The new technologies were reported to be expensive which is difficult to realize in an under resourced law enforcement. The study further noted gaps in recruitment of the police officers where most of the recruits lacked coursework skills which would equip them with skills relevant for various ICT skills. In addition, new technologies opened opportunities for more even more advanced crimes which exerts an additional burden on police. Though relevant, the study focused on general technologies that the police use to combat crime rather than challenges of police adopting mobile phone technology in counter terrorism operations.

Conceptual Framework

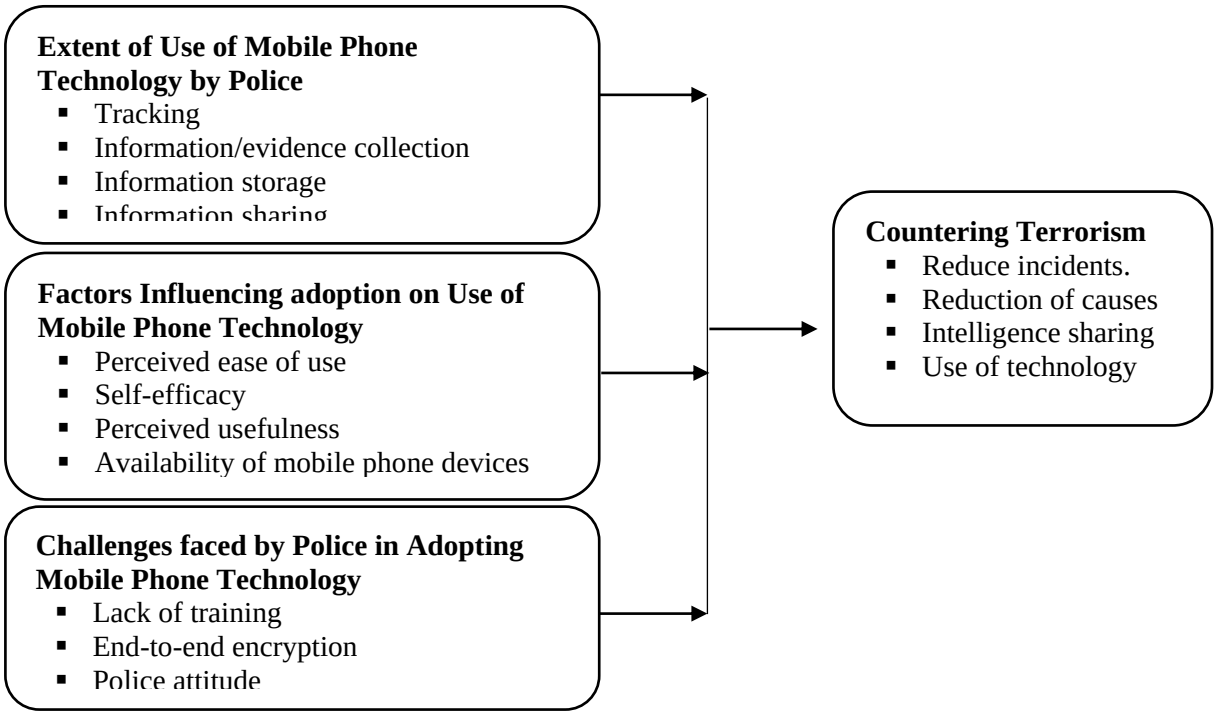

Figure 1: Conceptual Framework

Source; Researcher, 2023

METHODOLOGY

The study used descriptive survey research design with qualitative and quantitative approaches as Krishnaswamy (2018) postulate that it is any specific detailed procedures embraced in carrying out a research study. The target population of the study was 450 police officers of all cadres from police constable to Gazetted officers based at ATPU performing various functions in NCC, including officers from the Directorate of Criminal Investigations (DCI) headquarters Anti-bomb disposal unit, Cyber- crimes, and DCI Nairobi Regional command response team. The sample size of the study was 207 respondents. The study primarily focused on data collection tools that were designed in the best way possible to accurately measure the intended construct under the study and ensure the worthiness of the research findings. Further, the study tested reliability of instruments through test-retest method using a statistical technique which guaranteed a measurement of error for comparison analysis for the same objects under similar environment. The systematic approach of collecting, measuring, and analysing accurate awareness for research using standard reliable technique. Data was gathered from police Constables, Corporals, Sergeants, Senior Sergeants and inspectors in Nairobi County, Kenya by trained research assistants. The research incorporated both quantitative and qualitative data, which were used to formulate questionnaires and arrange interviews.

RESULTS

Presentation of Research Analysis and Findings

The purpose of the study was to establish the efforts in countering terrorism through Police adoption of mobile phone technology in NCC, Kenya. This section presents findings for extent of police use of mobile phones in counterterrorism, factors influencing police adoption of mobile phone technology and challenges faced by police officers in using mobile phone technology.

Extent of Police use of Mobile Phones in Counterterrorism

The first specific objective of the study was to examine the extent of mobile phone technology adoption by the NPS in countering terrorism in NCC, Kenya and the findings presented in Table 1:

Effectiveness of Mobile Phone Use in Tracking Terrorist

Table 1: Various Statements on Police Use of Mobile Phone Technology in Counter Terrorism Investigations

Police use of mobile phone technology	Mean	Std. Dev.
Determine how effective police use of mobile phone technology in locating of terror suspects.	3.921	0.661
Determine the capability of police in evidence collection while using Mobile phone technology.	2.539	1.235
Determine the extent of police training on police use of mobile phone technology	4.337	0.673
Determine usefulness of mobile phone technology in tracking of money transactions?	3.090	0.807
Determine how technological crimes in society are solved using mobile phone technology?	2.433	1.560
Determine the accuracy of mobile phone technology in prosecution of terror suspects.	3.210	1.026
Share information with community members	3.233	0.564
Share Information and intelligence on criminal conduct and other characteristics	2.921	1.234
Determine the reliability of mobile phone technology in evidence analysis	2.102	1.972
Locate, Identify and arrest of suspects	4.250	0.760
Collect and storage of evidence	3.156	0.259
Determine police attitude towards the use of mobile phone technology	2.1860	1.120

Source: Field Data, 2023

Extent of Police Training on Use of Mobile Phone Technology

Doran and Zaykowski (2019), examined the extent of police training on the use of mobile phone technology varies across different law enforcement agencies and regions. Some police departments invest heavily in training officers on the effective use of mobile phone technology in investigations, while others may have limited resources or prioritize other training areas. Krenz (2015), argues that comprehensive training is essential to ensure that officers are proficient in utilizing mobile phone technology for various investigative tasks, including locating suspects, evidence collection, and digital forensics. Adequate training can empower police to maximize the benefits of mobile phone technology and enhance their investigative capabilities.

According to Camacho-Collados and Pilehvar (2018), mobile phone technology can be highly useful in tracking money transactions, especially in cases involving financial crimes and terrorist financing. Mobile payment systems, digital wallets, and online banking applications leave digital traces of financial transactions, making it easier for law enforcement to monitor and track the movement of money. Additionally, mobile technology allows investigators to access real-time financial data, enabling rapid identification of suspicious transactions and potential money laundering activities. The usefulness of mobile phone technology in tracking money transactions significantly contributes to efforts to combat financial crimes and disrupt terrorist funding networks.

Kessler (2016) asserts that mobile phone technology plays a critical role in solving technological crimes in society. Cybercrimes, digital fraud, and identity theft are increasingly prevalent, and mobile devices are often the targets or tools used in these offenses. Rogers (2015), highlights mobile phone technology enables law enforcement to conduct digital forensics to trace the origins of cybercrimes, identify perpetrators, and recover digital evidence. Mobile phone data can provide crucial leads and insights into the modus operandi of cybercriminals, helping investigators to reconstruct the sequence of events and build a strong case for prosecution.

Factors Influencing Police Adoption of Mobile Phone Technology

The second specific objective of the study was to assess factors influencing NPS in adoption of mobile phone technology in counter terrorism in NCC, Kenya.

Use of Mobile Phone as Evidence in Prosecution

The respondents were further asked to indicate how frequent the mobile phone technology has been used as evidence during prosecution and the findings in Table 2: shows that majority (91.9%) of the respondents agree that the mobile phone is frequently used as evidence during prosecution while only 8.1 per cent indicated it is rarely used.

Table 2: Frequency of Use of Mobile Phone Technology as Evidence for Prosecution

	Frequency	**Percent**
Frequently	182	91.9
Rarely	16	8.1
Total	**198**	**100**

Source: Field Data, 2023

According to Casey and Richards, (2011) mobile phone technology is frequently used as evidence for prosecution in criminal cases, including counter-terrorism efforts. Call records, text messages, social media activity, and location data extracted from mobile devices are often presented as crucial digital evidence in court, supporting the prosecution's case against suspects. Rogers, (2015) claims in some cases, the use of mobile phone technology as evidence for prosecution may be rare due to challenges in obtaining and preserving digital evidence. Issues related to data privacy, encryption, and access to locked devices may limit the frequency of using mobile technology as evidence in court.

According to one of Key informant

> "Mobile devices often have encryption features that can hinder law enforcement's ability to access data during investigations. Additionally, concerns about data privacy and the need for proper legal authorization can complicate the process of obtaining evidence from mobile devices". (Respondent 001)

Another key informant said.

> "Mobile phone technology and applications can be complex, requiring specialized training for officers to effectively utilize digital forensic tools and extract evidence from different types of devices and operating systems" (Key Informant 002)

Mobile phone technology is frequently utilized as evidence in counter-terrorism prosecutions to establish communication links between suspects, plan activities, and establish the suspects' movements and associations during the investigation. Clarke and Newman, (2006), discusses in some counter-terrorism cases, the use of mobile phone technology as evidence for prosecution may be rare due to the complexity of the investigation or the involvement of highly skilled terrorists who take precautions to avoid leaving digital traces. Mobile phone technology is frequently employed as evidence in counter-terrorism prosecutions to establish the suspect's online radicalization, recruitment activities, and ideological affiliations through social media and internet communication.

Challenges faced by Police Officers in Using Mobile Phone Technology

The third specific objective was to analyse the challenges faced by NPS in adopting mobile phone technology in counter terrorism in NCC, Kenya and the respondents were asked to indicate if there are challenges in the use of mobile phone technology.

Table 3: Challenges Police Officers Face when Using Mobile Phone Technology

Statement	Mean	Std. Dev.
There exist challenges emanating from lack of specialized training of officers to use sophisticated mobile phone technology equipment	3.104	0.263
The police officers lack equipment to support mobile phone technologies	2.846	1.561
Presence of unqualified police	2.198	0.754
There are financial constraints that prevent adoption of new and updated technologies	3.461	0.912
Presence of unskilled personnel	2.645	1.972
Dynamic crimes due to new technologies pose a threat to counter terrorism operations	1.480	0.312

Source: Field Data, 2023

European Commission, (2019), Mobile phone technology is continually evolving, and new devices, operating systems, and encryption methods can outpace law enforcement's ability to keep up with the latest advancements. This was shared by several respondents who found technology ever changing and need to continuously adapt. On the other hand, Rogers, (2015), postulates that communication apps with end-to-end encryption, such as WhatsApp and Signal, present challenges for law enforcement in intercepting and deciphering messages sent between suspects. This concurs with view of a Key Informant

> "Sophisticated criminals may use security bypass techniques or exploit vulnerabilities in mobile devices to hide incriminating data, making it difficult for law enforcement to retrieve evidence*"* (Key Informant 006)

According to Casey, (2014), the manipulated or tampered with if not properly secured and documented. Unauthorized access to digital devices or data can compromise the integrity of the evidence. There may be a lack of standardized protocols and guidelines for handling technological evidence, leading to inconsistencies and potential issues in preserving and documenting the chain of custody, (Carrier and Spafford, 2003). In

complex investigations, digital evidence may pass through the hands of multiple custodians, increasing the risk of errors, mishandling, or unauthorized access during the transfer process. This was well noted by a key informant who said.

> "Maintaining the chain of custody for digital evidence from mobile devices is crucial to ensure its admissibility in court. Mishandling of devices or evidence may lead to legal challenges". (Key Informant 007)

The verbatim highlights the critical importance of maintaining the chain of custody for digital evidence retrieved from mobile devices to ensure its admissibility in court. By emphasizing the significance of proper handling and documentation throughout the evidence collection process, the statement underscores the potential legal ramifications associated with any mishandling or improper management of devices or evidence. However, it also prompts further inquiry into the specific challenges or scenarios that may arise due to mishandling and how these challenges could impact the admissibility of digital evidence in court proceedings. Additionally, it raises questions about the procedures and protocols in place to prevent mishandling, the training provided to law enforcement personnel regarding chain of custody protocols, and the potential consequences of legal challenges stemming from mishandled digital evidence.

SUMMARY

Police officers ease of use of mobile phone in locating terror suspects was assessed in terms of their ability to proficiently use the mobile phone applications, their experience in using the respective apps and the likelihood of them adopting the mobile phone in execution of their daily police duties. Majority of the police officers argued that they easily learnt to use mobile phone applications quickly and the respective mobile apps provided them with the information needed to respond to the call of service. Most of the officers reported that they tend to rely on their own experience than using mobile applications while several of the outlined their intention to adopt the mobile phone application in conducting their daily police tasks. Officers also noted that the use the mobile phone was helpful in that it assists in cases of tracking the suspects through their gadgets; the approach had also eased the passage of information about suspects and in the research of information records.

Findings point to the proper training and support in the use of mobile phone technology are essential for its successful adoption by police officers. It agrees with study by Lynch et al. (2019) that found that training and support were critical factors in the adoption of mobile technology by police officers. Findings agrees that the perceived security and privacy of mobile phone technology is also a factor in its adoption by police officers. If officers believe that their use of mobile technology is secure and private, they are more likely to use it. A study by Kyobe et al. (2017) found that perceived security and privacy were significant factors in police officers' intention to use mobile technology.

Challenges faced by Police Officers in the use of Mobile Phone Technology in counterterrorism was evaluated in terms of the aspects of the police officer's management style. Most of the police officers were not sure on the attribute of having been using the mobile phone application due to technical support by the police management. The officers posited that in order to improve the implementation of the mobile phone application in the police organization plan to prevent terrorism, the police officers organization management should come up with a new application that will be accessible to the police officers only to enhance their privacy in handling crimes cases, in-servicing or training the police officers on the mobile applications usage to facilitate the efficiency of service delivery regarding terrorism investigations, equip police with smart phones and every police station be serviced with free Wi-Fi alongside the integration of data sharing with government and mobile phone services providing companies to enable the police officers access timely data that will enable police have identity of all individuals. Byrne and Marx (2011) observed that adoption of mobile technology is hampered by lack of policy enforcement. Clarke (2004) also observed technological

changes and its diverse in nature discourages the adoption. In the case of this study access to internet facilities and compatible mobile phone remains a challenge in the Kenyan scenario.

CONCLUSION

In conclusion, this study has shed light on the adoption and utilization of mobile phone technology in countering terrorism within NCC. It has successfully achieved its objectives, revealing a moderate level of adoption of mobile phone technology in counterterrorism efforts. While progress has been made, there is still room for improvement, indicating that the full potential of mobile phone technology in countering terrorism has not yet been realized in the region. Factors influencing adoption, including technological infrastructure, financial resources, training, interagency collaboration, and policy support, have been identified, emphasizing the importance of addressing these factors to enhance adoption and effective use of mobile phone technology in counterterrorism operations.

Moreover, the study has highlighted the challenges faced by the police in adopting mobile phone technology for counterterrorism purposes. These challenges, ranging from limited resources to technological barriers and privacy concerns, underscore the need for comprehensive policies, protocols, and training programs. Addressing these challenges is crucial to ensure successful adoption and implementation of mobile phone technology in countering terrorism in NCC. Policymakers, law enforcement agencies, and counterterrorism units must invest in technological infrastructure, allocate sufficient financial resources, foster interagency collaboration, and address privacy and security concerns to leverage the potential of mobile phone technology effectively.

The findings of this research have significant implications for stakeholders operating in NCC and similar contexts globally. By addressing the recommendations provided, including investing in technological infrastructure and fostering collaboration among stakeholders, policymakers and law enforcement agencies can enhance the efficiency and coordination of counterterrorism efforts. Ultimately, this will contribute to the safety and security of NCC and similar regions.

RECOMMENDATIONS

Based on the findings, several recommendations can be made:

- Invest in the necessary infrastructure to support the effective use of mobile phone technology in counterterrorism. This includes improving network coverage, ensuring reliable communication systems, and providing necessary hardware and software resources.
- Adequate funding should be allocated to procure and maintain mobile phone technology resources, including devices, software, and security systems. This will ensure the sustainable and efficient implementation of these technologies.
- Develop and implement training programs for police officers on the effective use of mobile phone technology in counterterrorism operations. This will enhance their skills and knowledge in utilizing the technology to its full potential.
- Encourage collaboration and information sharing between police departments, counterterrorism agencies, and technology providers. This will promote effective coordination and enhance the integration of mobile phone technology in counterterrorism efforts.
- Develop robust policies and protocols to address privacy concerns associated with the use of mobile phone technology in counterterrorism. Ensure that data protection measures are in place to safeguard sensitive information.

Areas for Further Research

From the findings of the study, the following could be explored.

- A study to assess the cost-effectiveness of mobile technology in counter-terrorism operations, analysing its economic benefits and potential drawbacks. Such findings could highlight the positive impact of mobile technology in enhancing operational efficiency, reducing response time, and improving information sharing among law enforcement agencies.
- Research can be carried out to examine the ethical, legal, and privacy implications associated with the use of mobile technology in counter-terrorism operations. It can explore the potential risks of data breaches, infringement on individuals' privacy rights, and the ethical considerations surrounding surveillance.
- Research that examines the role of mobile technology in facilitating coordination and collaboration among different law enforcement agencies. It can emphasize the importance of seamless communication and information sharing among agencies to enhance overall operational effectiveness.

REFERENCES

Boffey, D. (2018). *EU plans mobile terror alerts to counter spread of fake news.* Counter-Terrorism policy. Accessed at https://www.theguardian.com/politics/2018/nov/13/mobile-phone-alerts-to-warn-europeans-if-near-terrorist-attack

Camacho-Collados, M., & Pilehvar, M. T. (2018). From Word to Sense Embeddings: A Survey on Vector Representations of Meaning. Journal of Artificial Intelligence Research, 69, 569-632.

Casey, E. (2014). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Burlington, MA: Academic Press.

Casey, E., & Richards, H. (2011). Case Studies in Mobile Device Forensics. In R. Rogers, S. V. Vemuri, & M. Gupta (Eds.), Mobile Forensics (pp. 15-24). London: Springer.

Chakraborty, J., & Chakraborty, M. (2008). Mobile telephony based secured society an anti-terrorism attempt. *TENCON 2008-2008 IEEE Region 10 Conference* in Hyderabad, India

Clarke, R. V., & Newman, G. R. (2006). Outsmarting the Terrorists. Westport, CT: Praeger Security International.

Cornish, P. (2010). Technology, strategy, and counterterrorism. *International Affairs*, *86*(4), 875-888.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-34

Doran, K., & Zaykowski, H. (2019). Police Officer Digital Literacy: Results from a National Survey. Policing: A Journal of Policy and Practice, 13(4), 425-434.

Egnoto, M., Ackerman, G., Iles, I., Roberts, H. A., Smith, D. S., Liu, B. F., & Behlendorf, B. (2017). What motivates the blue line for technology adoption? Insights from a police expert panel and survey. *Policing: An International Journal of Police Strategies & Management*.

Faith, T., & Bekir, C. (2015). Police use of technology to fight against crime. *European Scientific Journal*, *11*(10).

Feyyaz, M. (2020). Countering terrorism in Pakistan: Challenges, conundrum, and resolution. In *Non-Western responses to terrorism*. Manchester University Press.

Graham, R. (2016). How terrorists use encryption. *Combating Terrorism Center*. 9(6), 35-45

Gupta, R., & Jain, K. (2014). Adoption of mobile telephony in rural India: An empirical study. *Decision Sciences*, *45*(2), 281-307.

Kessler, G. C. (2016). The Digital Evidence Handbook: The Nearly Complete Guide to Collecting, Preserving, and Presenting Digital Evidence. Amsterdam: Elsevier.

Krenz, A. R. (2015). Enhancing Criminal Justice Technology Education: An Analysis of Current Courses and Proposals for Future Directions. Journal of Criminal Justice Education, 26(3), 358-376.

Kumar, N., & SM, V. (2019). Use of Modern Technology to Counter Terrorism.

Kyobe, M., Siya, M. J., & Williams, Q. (2017). Exploring the factors that influence the adoption of mobile technology by the South African police. Journal of Contemporary Management, 14(1), 327-351.

Lee, J., & Rao, H. R. (2007). Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: an exploratory study of government–citizen's online interactions in a turbulent environment. *Decision Support Systems*, *43*(4), 1431-1449.

Lynch, J., Salinas, J., McCreary, M., & Bishop, B. (2019). Assessing the impact of mobile technology on police performance: An analysis of the adoption and use of mobile technology by police agencies across the United States. Police Quarterly, 22(3), 364-387

Miller, C. (2006). Cell Phone Bombs: How Law Enforcement Can (and Can't) Prevent Them. *Law Enforcement Technology* 33(11), 86-95

Moutot, M. (2018). *Smartphones: a double-edged sword for terrorists*. Retrieved at https://phys.org/news/2018-11-smartphones-double-edged-sword-terrorists.html.

Mwasaa, C. (2010). *An Assessment of factors Influencing Mobile Phone Adoption: Case of Kenya's Socio-Economic Development* (Doctoral dissertation, University of Nairobi).

Ndonye, R. N. (2019). Implications of Technological Advancement on Performance on Police Officers; Case of Kenya Railways Police Unit.

Oluniyi, A. (2010). NCC Wants to Track Nigerians Movements via Mobile Phones. ICT works. Retrieved at https://www.ictworks.org/

Ragab, E. (2015). Complex Threat: Challenges of Countering Terrorism in the Middle East after the Arab Revolutions. In *Countering Radicalisation and Violent Extremism among Youth to Prevent Terrorism* (pp. 101-112). IOS Press.

Rogers, M. K. (2015). Cybercrime and Digital Forensics: An Introduction. New York: Routledge South University (2016). Fighting Crime with Mobile Technology. Retrieved at https://www.southuniversity.edu/news-and-blogs/2016/08/

Stones, E. K. (2017). *Mobile Communications: M-Crime and Security* (Doctoral dissertation, UCL (University College London)).

Tanner, S., & Meyer, M. (2015). Police work and new 'security devices': A tale from the beat. *Security dialogue*, *46*(4), 384-400.

Tanui, D. K., & Barmao, C. K. (2016). Use of ICT in the Detection and Prevention of Crime in Kenya. *Journal Information Engineering and Applications*.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science, 46(2), 186-204.