A VISUAL ANALYTIC FRAMEWORK FOR MONITORING TERROR ATTACKS: A CASE STUDY OF MANDERA COUNTY, KENYA

By

MONG'ARE BRION GEKARA

MASTER OF SCIENCE IN DATA ANALYTICS

KCA UNIVERSITY

2025

A VISUAL ANALYTIC FRAMEWORK FOR MONITORING TERROR ATTACKS: A CASE STUDY OF MANDERA COUNTY, KENYA

By

MONG'ARE BRION GEKARA

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN DATA ANALYTICS IN THE SCHOOL OF TECHNOLOGY AT KCA UNIVERSITY

JULY, 2025

DECLARATION

I declare that this dissertation is my original work and has not been previously published or submitted elsewhere for the award of a degree. I also declare that this contains no material written or published by other people except where due reference is made and the author duly acknowledged.

Student Name: MONG'ARE BRION GEKARA Reg. No. 21/08649

Sign:  Date: 14/07/2025

I do hereby confirm that I have examined the master's dissertation of

Mong'are Brion Gekara

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

Sign:  Date: 16/07/2025

Dr. Dennis Kaburu

Dissertation Supervisor

A VISUAL ANALYTIC FRAMEWORK FOR MONITORING TERROR ATTACKS:

A CASE STUDY OF MANDERA COUNTY, KENYA

ABSTRACT

Terrorism remains a persistent and evolving threat in Kenya, particularly in border counties such as Mandera, which face heightened vulnerability due to their proximity to Somalia. The Country's ongoing instability, weak governance structures, and the presence of terrorist groups like al-Shabaab (AS) create fertile ground for cross-border militant activity, posing significant challenges to both regional security and local stability. A critical gap in current counterterrorism efforts is the absence of localised, data-driven frameworks capable of monitoring and predicting terrorist activities in real time. This study addresses that gap by developing a Visual Analytics (VA) framework tailored to monitor, analyse, and predict terrorist incidents, using Mandera County as a case study. Beyond processing complex datasets, the framework offers strategic guidance to decision-makers, enhancing situational awareness and enabling proactive counterterrorism interventions. The core objective is to strengthen counterterrorism strategies through spatiotemporal data mining techniques, such as cluster analysis, association analysis, and outlier detection, to derive actionable insights from both structured and unstructured data sources. The methodology integrates data from social media, security reports, and established databases such as the Global Terrorism Database (GTD) and the Armed Conflict Location & Event Data Project (ACLED). Visuals in the framework are guided by Shneiderman's Visual Information-Seeking Mantra: "overview first, zoom and filter, then details on demand." Through this approach, the system identifies attack hotspots, temporal patterns, and early warning indicators, delivering a user-centric tool for informed decision-making. Findings demonstrate the framework's effectiveness in predicting high-risk areas and attack types, with particular emphasis on armed assaults and improvised explosive device (IED) incidents, which constitute over 50% of recorded attacks in Mandera. The results show improved allocation of security resources, enhanced inter-agency coordination, and timely intervention capabilities. Key recommendations include deploying the framework in high-risk regions, integrating it with existing security infrastructure, and expanding its use to other terrorism-affected areas. The framework's scalable and adaptable design positions it as a valuable tool for strengthening counterterrorism efforts across Kenya and similar contexts.

Keywords: Terrorism, visual analytics (VA), counterterrorism, spatiotemporal data mining, threat prediction, Mandera County, al-Shabaab (AS), early warning systems, decision-making, resource allocation.

ACKNOWLEDGMENT

I am grateful to the Almighty God for granting me strength, good health, and perseverance throughout my studies. I sincerely appreciate the invaluable guidance, mentorship, and unwavering belief in my abilities demonstrated by Dr. Dennis Kaburu. His insightful feedback and constructive criticism have significantly influenced the direction of this work.

Special appreciation goes to my parents and brothers for their steadfast support, love, and encouragement throughout this academic journey. Their unwavering belief in my capabilities has been a driving force, and I deeply appreciate their sacrifices and understanding. Heartfelt thanks also go to my dear friends and colleagues, whose support and camaraderie have continually motivated and inspired me throughout this academic journey.

Finally, I acknowledge all those who have contributed to my personal growth and development as both a student and an individual. The kindness, support, and encouragement I have received from so many have made a significant difference.

TABLE OF CONTENTS

DEDICATION

This work is dedicated to my loving parents, Dr. Moses Mong'are and Mrs. Everlyne Mong'are, whose unwavering support, encouragement, and love have been my greatest source of strength and inspiration. It is through their sacrifices, wisdom, and guidance that the foundation for all my achievements was laid. With profound gratitude and deep appreciation, I dedicate this work to them as a token of my everlasting love and respect.

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

9/11	September 11, 2001, terrorist attacks
ACSS	Africa Center for Strategic Studies
ACLED	Armed Conflict Location & Event Data Project
ADF	Allied Democratic Forces
AI	Artificial Intelligence
AMISOM	African Union Mission in Somalia
AQ	Al-Qaeda
ARIMA	AutoRegressive Integrated Moving Average
AS	Al-Shabaab
ATMIS	African Union Transition Mission in Somalia
CRS	Coordinate Reference System
CVE	Countering Violent Extremism
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
EDA	Exploratory Data Analysis
GIS	Geographic Information System
GoK	Government of Kenya
GTD	Global Terrorism Database

GTI	Global Terrorism Index
IED	Improvised Explosive Device
IS	Islamic State
ISWAP	Islamic State in West Africa Province
KDD	Knowledge Discovery in Databases
NER	North Eastern Region
NGOs	Non-Governmental Organisations
PII	Personal identifying information
SIT	Social Identity Theory
SNA	Social Network Analysis
START	Study of Terrorism and Responses to Terrorism
UCDP	Uppsala Conflict Data Program
USA	United States of America
VA	Visual Analytics

DEFINITIONS OF TERMS

Terrorism: The systematic use of violence, intimidation, or the threat of violence to create fear and coerce a population or government, typically for ideological, political, or religious purposes.

Visual Analytics (VA): An interdisciplinary field that combines data visualisation, analytical reasoning, and interactive interfaces to help people make sense of complex and large datasets. In this study, VA facilitates the monitoring, analysis, and prediction of terror attacks.

Structured Data: Organised and well-formatted information, typically stored in databases or tables, with a high degree of organisation and uniformity in format and syntax.

Unstructured Data: Information lacking a predefined data model or format, commonly including textual data, such as social media posts, news articles, and reports.

Geospatial Alignment: Associating data with specific geographical locations to integrate spatial information. Here, it aids in mapping terrorism events to exact locations within Mandera County.

Temporal Alignment: Synchronising data with timestamps to ensure chronological coherence. In this study, it maintains temporal coherence in the dataset, accurately reflecting terrorism events and discussions over time.

Data Fusion: Combining information from various sources for a comprehensive and coherent understanding. In this context, it merges data from different sources, both structured and unstructured, to create an integrated dataset.

Spatiotemporal Data Mining: A branch of data mining focused on datasets with spatial and temporal attributes. This study utilises techniques such as cluster analysis, association analysis, and outlier detection to understand the geographic and temporal dynamics of terrorism.

Predictive Analytics: The application of statistical algorithms and machine learning techniques to analyse historical data to forecast terrorism-related developments.

Usability Testing: A method for evaluating how easily users can interact with a system. In this study, it assesses the user-friendliness and intuitiveness of the VA framework.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Terrorism, in its many forms, involves the deliberate and often devastating use of violence intended to instil fear and achieve specific political objectives (Jenkins, 2023). This global phenomenon has far-reaching consequences, including the tragic loss of life, widespread property destruction, and significant disruptions to both local and global economies (Olabanjo et al., 2021). Among the various types of terrorism, religiously motivated acts stand out due to their deep roots in faith and literal interpretations of sacred texts, which have had a direct impact on Kenya and are the primary focus of this study (Brennan, 2017).

As the complexity of terrorism has grown, so too has the challenge of effectively countering it. The sophistication of modern terrorist activities necessitates equally advanced tools for analysis and prevention. Visual analytics (VA) has emerged as an alternative approach that combines data visualisation, analytical reasoning, and human insight to analyse terrorism-related data. This fusion enables the interpretation of large and complex datasets, a task with which traditional methods often struggle. This capability is crucial in uncovering hidden patterns, trends, and insights within multi-dimensional datasets, making VA a powerful tool in the fight against terrorism (Kejriwal et al., 2017).

Bergen (2024) asserts that the infamous September 11, 2001, attacks in the United States of America (USA), commonly known as the 9/11 terror attacks, marked a pivotal moment in global counterterrorism efforts, especially for the USA. These attacks, carried out by 19 al-Qaeda (AQ) operatives who hijacked commercial airliners and crashed them into major U.S. landmarks, killing thousands. This tragedy catalysed the development of terrorism informatics,

a field dedicated to using advanced methodologies and information fusion techniques to monitor and analyse terrorism-related content (Aleroud et al., 2020).

In Africa, the threat of terrorism has been particularly severe in regions like the Sahel, the Lake Chad Basin, and the Horn of Africa. AQ and Islamic State (IS) affiliates have wreaked havoc, displacing millions, committing widespread human rights abuses, and causing significant economic disruption (UNHCR, 2021; Williams, 2020). Despite extensive international efforts, including military training, intelligence sharing, and humanitarian aid, these groups continue to pose a substantial threat, highlighting the need for a holistic, multi-dimensional counterterrorism approach that addresses political, social, and economic root causes of extremism (Aning & Abdallah, 2016; Campbell, 2021).

Sub-Saharan Africa, in particular, has become a focal point for terrorist activities, with nearly half of the global victims of terrorism in 2022 originating from this region (Lederer, 2023). Some key perpetrators include the Islamic State in West Africa Province (ISWAP), al-Shabaab (AS) in Somalia, and Boko Haram in Nigeria (Institute for Economics & Peace, 2023). On July 14, 2023, an attack by the Allied Democratic Forces (ADF), an IS affiliate operating in Uganda and the Democratic Republic of Congo (DRC), resulted in the deaths of 41 civilians at Lhubiriha Secondary School in Uganda, underscoring the severity of the threat (Al Jazeera, 2023).

The global nature of terrorism today means that its impacts are not confined to direct victims, with ripple effects across social, political, and economic spheres, affecting communities worldwide. Over the years, the nature of terrorism has evolved from large-scale, high-profile attacks to more decentralised, unpredictable acts of violence. This shift has been driven largely by advances in technology, social media, and the internet, which have enabled

terrorist groups to recruit, plan, and execute attacks with unprecedented reach and sophistication (Nacos, 2016).

As terrorism has evolved, so have the strategies and methodologies employed by states and organisations to counter these threats. The persistence and adaptability of terrorist groups underscore the critical need for effective counterterrorism strategies. However, the success of these strategies varies significantly across different regions. In areas where strong intelligence-gathering and international cooperation exist, terrorist plots are often disrupted, and networks dismantled. In contrast, regions with weak governance and ongoing conflicts continue to see terrorism thrive, presenting a serious challenge to global security. This disparity is often due to differences in political will, resource allocation, and the capacity of local law enforcement agencies (Hoffman, 2017).

One of the most significant challenges in counterterrorism is balancing the need for security with the protection of human rights. This tension is evident domestically and internationally, where the need for pre-emptive actions often clashes with civil liberties and the rule of law (Chalk, 2019). The challenge is particularly pronounced in regions where terrorism is closely linked with ethnic, religious, or political grievances, complicating efforts to counter terrorism without worsening these underlying issues. Additionally, the rise of ‘lone-wolf’ attackers and small, decentralised cells has made traditional counterterrorism methods, often focused on monitoring large organisations, less effective. These newer forms of terrorism are harder to predict and prevent, as they usually involve self-radicalised individuals operating independently of established networks (Byman, 2020).

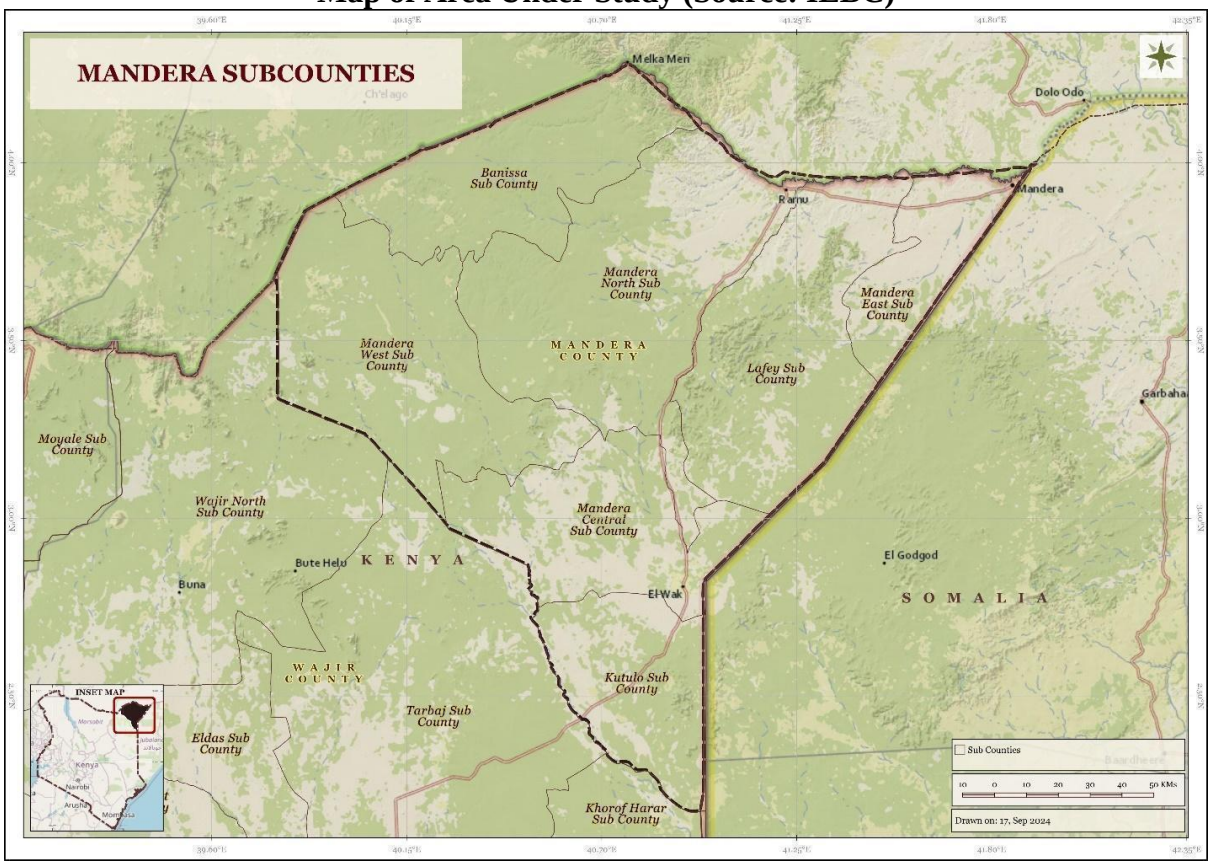
1.1.1 Brief history of the area of study

The history of Mandera County highlights the profound transformation it has undergone due to terrorism. Once a thriving region supported by strong social structures and traditional governance, the County's stability was shattered by the rise of AS in the early 2000s (Mwangi, 2012; Botha, 2014). Originating amid Somalia's protracted instability, the militant group has projected its influence across the border, transforming Mandera into the frontline of an insurgent campaign intent on establishing a regional caliphate (Cannon & Pkalya, 2019).

Kenya's military intervention in Somalia in 2011, known as Operation Linda Nchi, was a response to cross-border attacks and kidnappings by AS. While the operation aimed to stabilise Somalia, it inadvertently exposed regions like Mandera County to retaliatory attacks (Anderson & McKnight, 2015; Ndzovu, 2020). The location and porous nature of the Kenyan borders made Mandera County a prime target, leading to a series of devastating terror incidents that have displaced communities, closed schools, and disrupted the local economy (START, 2019).

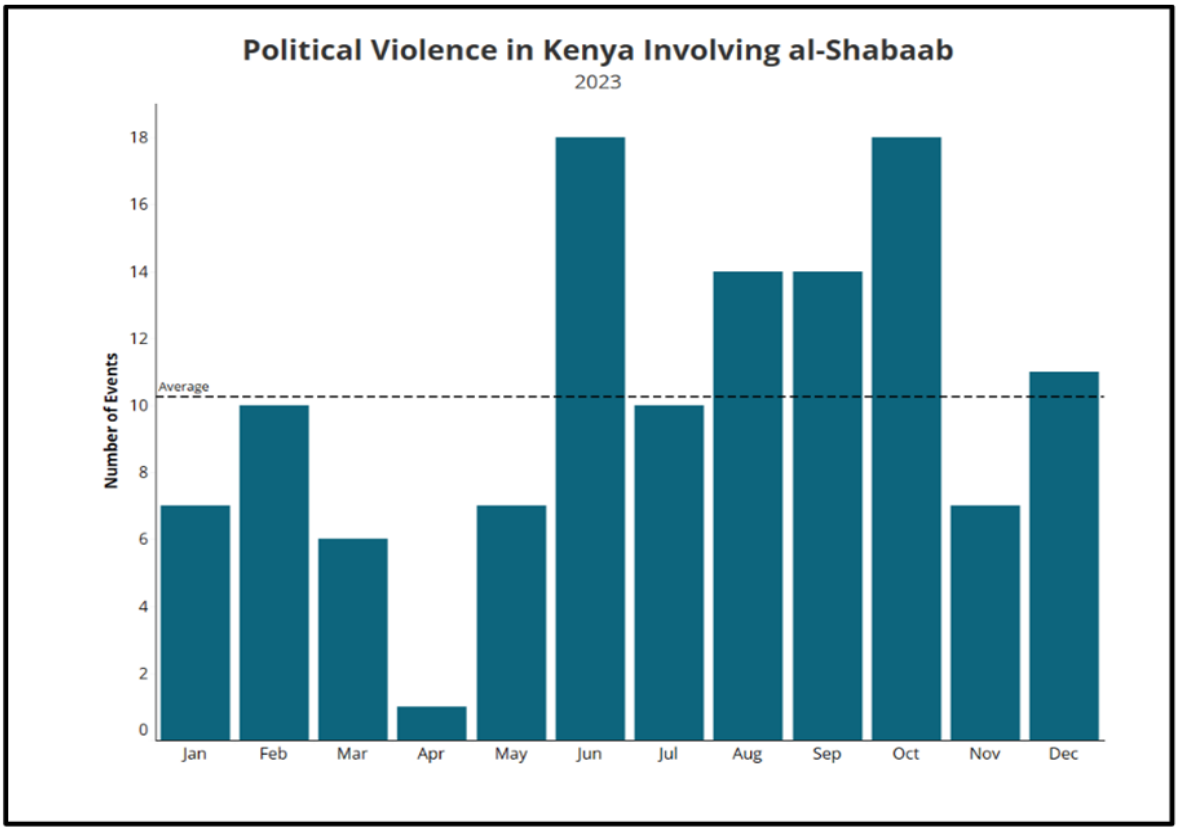
The impact of AS activities in Mandera County extends beyond immediate security concerns. The use of Improvised Explosive Devices (IEDs) and assaults on security convoys has crippled critical infrastructure, impeded service delivery, and undermined social cohesion. This atmosphere of fear has made it difficult for the government to implement effective counterterrorism strategies, as traditional community engagement and intelligence-gathering methods have been compromised (Robbins & Corps, 2019).

FIGURE 1.1
Map of Area Under Study (Source: IEBC)



The rise of AS can be traced back to the collapse of the Somali government in 1991, which plunged the country into lawlessness and chaos. In this power vacuum, AS emerged as a self-proclaimed defender of Islam, rallying disenfranchised youth and warlords under its banner (Hansen, 2018). Their ideology, rooted in a radical interpretation of Islam, fuelled a relentless recruitment drive and expansion of their influence. Before long, AS controlled large areas of southern Somalia and expanded their operations into Kenya and neighbouring countries.

FIGURE 1.2
The Concentration of AS Violence in Border Counties: A Focus on Mandera, Wajir, and Garissa Sub-Counties. (Source: ACLED, 2023)



A VA framework offers an alternative approach for enhancing counterterrorism efforts. Its ability to handle and interpret vast datasets makes it indispensable for monitoring, analysing, and predicting terrorist activities. Through a comprehensive visual overview of data, VA allows analysts to detect anomalies and potential threats that might otherwise remain undetected. This capability is especially critical in regions plagued by persistent terrorism, where timely and informed decision-making can save lives.

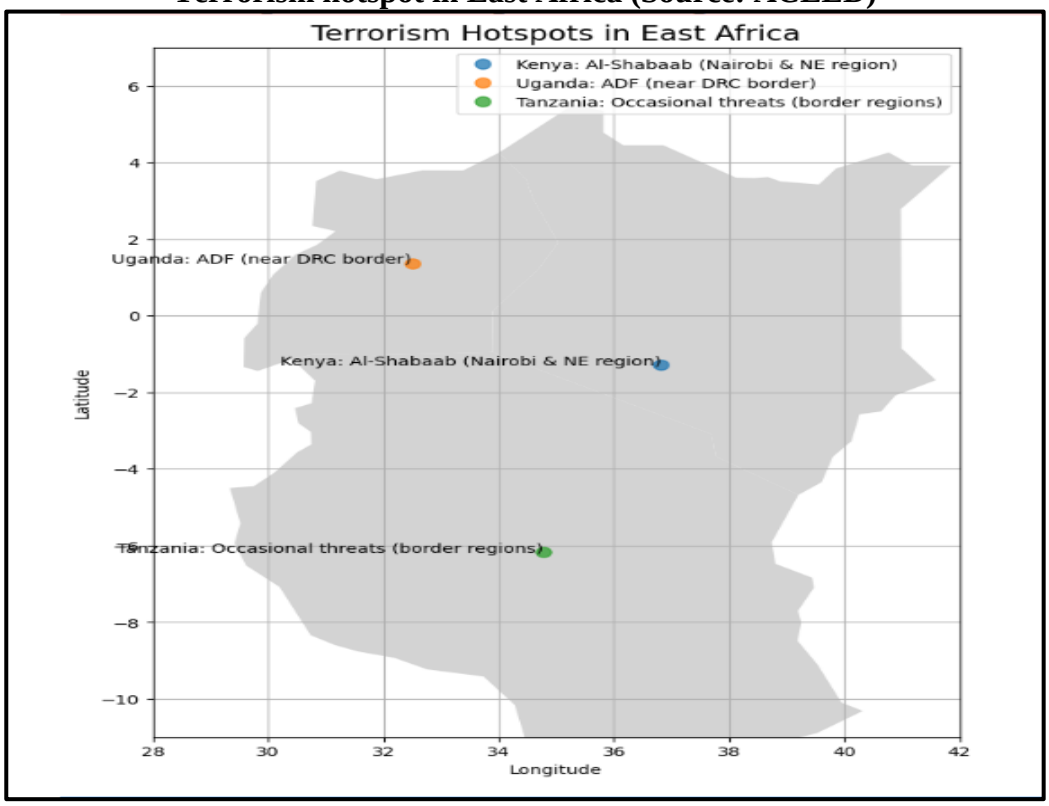
To demonstrate the potential of a VA framework, this study uses Mandera County, a region in the NER of Kenya, as a case study. Mandera County, once a peaceful area known for its pastoralist communities and cross-border trade, has become a hotspot for terrorism, largely due to its proximity to Somalia and the activities of the militant group AS. The challenges faced by Mandera County, including frequent terror attacks, economic decline, and social disruption,

highlight the pressing need for advanced analytical frameworks like VA to enhance counterterrorism strategies.

1.1.2 Understanding the genesis of the problem

The persistent attacks have disrupted economic activities, exacerbated poverty and unemployment, and fuelled a cycle of violence and radicalisation among the youth (Mugwang'a, 2023). Given these challenges, there is an urgent need for a comprehensive strategy that goes beyond military intervention. A VA framework offers a promising solution for analysing and understanding the complex, spatiotemporal patterns of terrorism in Mandera County. This study leverages VA to uncover hidden patterns, relationships, and potential indicators of future attacks, thereby strengthening security measures and supporting informed decision-making in Mandera County and other high-risk regions.

FIGURE 1.3
Terrorism hotspot in East Africa (Source: ACLED)



Kenya has faced significant terror attacks, resulting in substantial civilian and military casualties, prolonged psychological distress, heightened anxiety among Kenyans and international visitors, and an impact on the country's tourism industry and overall economy (Muna, 2017). The number of terror attacks, especially those orchestrated by AS, increased significantly after the launch of Operation Linda Nchi in October 2011, which targeted AS militants in Somalia (Muibu & Cubukcu, 2023). Kenya's subsequent involvement in the African Union Mission to Somalia (AMISOM), now the African Union Transition Mission (ATMIS), further heightened the gravity of the situation. Notable terrorist incidents in Kenya include the DusitD2 complex attack on 15 January 2019, which killed 21 people and wounded 28, and the Westgate Mall siege on 21 September 2013, which caused at least 67 fatalities and many further injuries (BBC, 2019; Gathara, 2021).

1.1.3 Local scenario

Kenya, like many other nations in the Horn of Africa, has grappled with significant regional security challenges, particularly from militant groups such as AS. The severity of the threat posed by AS became evident following the 2013 Westgate Mall attack in Nairobi, a devastating event that claimed 67 lives and marked a pivotal moment in Kenya's counterterrorism efforts. This attack not only highlighted the brutal reality of terrorism but also brought it to the forefront of national consciousness (Kamau, 2021). Since then, AS has continued to carry out high-profile attacks, including the tragic Garissa University College massacre in 2015, where 148 people lost their lives, and the 2019 DusitD2 complex attack, which claimed 21 lives (Mugwang'a, 2023). These incidents have resulted in profound loss of life and heightened security concerns across the country, prompting the Kenyan government to bolster its efforts to combat the group's influence.

In response, the Government of Kenya (GoK) has implemented numerous measures to counter terrorist activities. These include the enactment of new legislation, the establishment of security organs, the construction of a border wall between Kenya and Somalia, initiatives to prevent and counter violent extremism, and the implementation of community policing strategies (Mugwang'a, 2023). A significant development in Kenya's counterterrorism strategy has been a paradigm shift from 'need to know' to 'need to share' within the multi-agency setup, facilitating the seamless exchange of actionable intelligence and enabling swift responses to potential threats. While these efforts have shown commendable progress at tactical and operational levels, there remains room for improvement at the strategic level.

Social media has emerged as a powerful tool for communication and connection, but it has also become a channel for spreading disinformation, sowing divisiveness, and contributing to real-world harm, including violence, persecution, and exploitation (Robbins & Corps, 2019). Platforms like X (formerly Twitter) are particularly favoured by terrorists for disseminating propaganda and coordinating internal communications. These platforms also support security agencies in gathering intelligence, enhancing counterterrorism efforts, and collecting evidence for prosecution (Ngoge & Orero, 2017). Conversely, these same platforms have fuelled the development of terrorism databases and datasets, including the Global Terrorism Database (GTD), the Armed Conflict Location & Event Data Project (ACLED), and, locally, the Countering Violent Extremism (CVE) Research Hub Observatory (Bowie, 2024). The abundance of structured and unstructured terrorism-related data offers a rich foundation for monitoring, analysis, and response; however, its sheer volume, velocity, and variety create substantial challenges that can be overcome through a VA framework integrating automated processing with interactive, human-centred visual exploration.

The importance of geovisualisation in counterterrorism cannot be overstated. Buil-Gil and Langton (2020) emphasise that geovisualisation is essential for knowledge-building, as it facilitates the development of hypotheses, the identification of patterns, and the exploration of new research avenues. They note that crime, including terrorism, tends to cluster in specific locations rather than being randomly distributed in space. Hao et al. (2019) further explain that since the introduction of geo-statistics (also known as the Kriging Method) in the 1960s, Geographic Information Systems (GIS) have evolved significantly, and are now widely used to enhance public security, provide early warnings, and support counter-terrorism operations. Guo et al. (2016) argue that there remains a lack of focus on the intrinsic spatiotemporal characteristics of terrorism events and limited research on the applicability of various visual analysis methods and their use in decision support analysis. Although studies such as Ngoge and Orero (2017) provide valuable insights into terrorist activities in Kenya, a notable research gap persists regarding the spatiotemporal characteristics of terror attacks in the country, underscoring the need for this study.

In Mandera County, the impact of terrorism has been particularly severe due to its proximity to the Somalia border and its long-standing history of marginalisation. The region has suffered frequent attacks, resulting in significant loss of life and widespread disruption of social and economic activities. The County's infrastructure has been particularly hard hit, with frequent assaults on transport networks, communication infrastructure, and government installations (Bowie, 2024). This sustained violence has triggered a mass exodus of non-local workers, particularly teachers and healthcare professionals, further exacerbating the region's development challenges. The withdrawal of these essential service providers has left the local population even more vulnerable, underscoring the need for a comprehensive and inclusive approach to addressing both the security and developmental needs of Mandera County.

1.2 Problem Statement

Despite sustained efforts to combat terrorism in Kenya, counterterrorism strategies remain largely reactive and fragmented, particularly in high-risk regions such as Mandera County. In contrast, developed countries like the U.S. employ advanced early warning systems, such as the National Terrorism Advisory System (NTAS) and Homeland Security's Fusion Centres that integrate intelligence to issue timely alerts (U.S. Department of Homeland Security, 2022). Kenya, however, lacks a comparable, localised framework for real-time threat detection and response. For example, the U.S. often provides pre-attack warnings to Kenya, yet these alerts are frequently underutilised due to the absence of a structured, data-driven system to validate and act upon them (Muibu & Çubukçu, 2023). Existing counterterrorism efforts in Kenya suffer from weak data integration, delayed detection, and limited situational awareness, which hinder proactive interventions. Traditional approaches consistently struggle to integrate structured data (e.g., incident reports) with unstructured sources (e.g., social media and news), resulting in gaps in spatiotemporal analysis and constraining predictive capacities.

This study addresses these challenges by developing a Visual Analytics (VA) framework, an interactive system that integrates spatiotemporal analytics, predictive modelling, and user-centric visualisation, to monitor and predict terrorist activities (Islam et al., 2016). Building on the identification of early warning indicators, this framework was developed to strengthen Kenya's and the wider region's counterterrorism efforts. Using Mandera County as a case study, it leverages various data sources and applies machine learning techniques to generate context-specific insights for proactive security interventions. Whereas the U.S. relies on centralised intelligence platforms, Kenya requires a decentralised and scalable solution that accounts for its resource constraints, ethnic and socio-cultural diversity, and the complex regional security dynamics along its borders (Kirwa & Handa, 2025). The proposed VA framework bridges this gap by offering a context-aware, data-driven tool to enhance threat

monitoring, strengthen intelligence-sharing, and enable timely interventions. Validating its effectiveness in Mandera demonstrates its potential for broader application in other terrorism-affected regions.

1.3 Objectives

1.3.1 General objective

The primary objective of this study was to develop a VA framework for monitoring and analysing terrorist activity.

1.3.2 Specific objectives

i. Identify the challenges impeding counterterrorism efforts in Kenya and early warning indicators of terrorist activity.

ii. Develop a VA framework for monitoring terrorist activities, based on the challenges and indicators identified.

iii. Test and validate the effectiveness of the developed VA framework.

iv. Propose an intervention strategy using the VA framework to enhance counterterrorism efforts in Kenya.

1.3.3 Research questions

i. What are the major challenges hindering counterterrorism efforts in Kenya, and what terror pre-indicators can be identified?

ii. How can a VA framework be developed to monitor terrorist activities based on these identified challenges and indicators?

iii. How effective is the developed VA framework in monitoring and analysing terrorism-related activities in Mandera County?

iv. How can the VA framework be applied as an intervention tool to support counterterrorism strategies in Kenya?

1.4 Motivation of the Study

The motivation for this study stems from the alarming escalation in the frequency and complexity of terror attacks in Kenya. The grave repercussions of these attacks, inflicting substantial harm on human lives, local economies, and the region's stability, underscore the urgency for an effective and data-driven counterterrorism strategy. The amalgamation of structured and unstructured data, synergised with the power of VA, presents a compelling avenue to unveil obscured patterns, detect early warning signals, and spot potential indicators of impending terror activities.

Central to this endeavour is the creation of a robust VA monitoring framework. This framework aims to equip security agencies and decision-makers with effective tools and actionable insights to enable proactive responses to the persistent threat of terrorism. Organising data comprehensively enables the study to provide stakeholders with a strategic advantage, supporting informed decision-making and enhancing the protection of public well-being.

1.5 Significance of the Study

Harnessing historical data, this study draws insights from structured terrorism databases such as GTD, ACLED, and CVE, as well as unstructured data mined from social networks, primarily X, and online news sources. Fusing insights from diverse sources enhances the credibility, validity, and depth of findings.

The proposed VA monitoring framework, using Mandera County as a case study, has the potential to enhance security by proactively identifying and mitigating threats, thereby preventing attacks. It will also support informed decision-making by providing actionable insights based on a comprehensive analysis of both structured and unstructured data.

In addition, it will optimise resource allocation by analysing the geographical and temporal distribution of terrorist incidents, enabling the targeted deployment of security resources in high-risk areas. Furthermore, it will provide a holistic understanding that facilitates a nuanced exploration of the root causes of terrorism in the region. It will also help authorities adopt proactive strategies to counter attacks, thereby reducing their impact and supporting effective post-attack responses. The findings will contribute to academic knowledge and offer baseline data for future research.

1.6 Structure of the Research

The subsequent chapters are organised as follows: Chapter 2, Literature Review, examines research on spatiotemporal visualisations, terrorism analytics, and data integration techniques, while identifying variables that influence terror attacks. It also proposes a conceptual framework to support the formulation of the study's hypotheses. Chapter 3, Methodology, outlines the study design, data sources, and analysis methods, and addresses ethical considerations across all research stages. Chapter 4, Results and Discussion, presents the research findings, including descriptive analyses, correlation statistics, and model validation, offering interpretations that provide context and relevance. Finally, Chapter 5, Conclusion, revisits the main results, highlights contributions to existing literature, discusses study limitations, and offers recommendations for future research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The literature review aims to build a robust theoretical foundation by identifying key concepts, methodologies, and findings from previous research, with a particular emphasis on VA. VA is essential across various fields, particularly within counterterrorism, due to its ability to analyse and interpret large, complex datasets. The chapter explores the evolution and significance of VA, emphasising how it is applied in spatiotemporal visualisations, terrorism analytics, and data integration techniques. Later, the review contextualises these advancements within Mandera County, discussing how the VA framework can address the region's unique security challenges. The chapter concludes by summarising key findings, highlighting gaps in existing research, and laying the groundwork for the VA framework tailored to monitoring terrorist attacks in Kenya.

2.2 Evolution and Importance of Visual Analytics (VA)

VA has developed into a multi-disciplinary approach that combines data visualisation, analytical reasoning, and human judgement to interpret complex datasets. VA is increasingly valued in counterterrorism, as conventional analytical methods often falter when confronted with the scale and complexity of data, impeding the extraction of timely and actionable insights (Turkay, 2017; Sacha, 2017). VA's ability to analyse fused data from multiple sources makes it a powerful tool for identifying patterns and trends, especially given the multidisciplinary nature of terrorism-related data (Andrienko, 2017; Wu, 2017)

2.3 Spatiotemporal Visualisations and Terrorism Analytics

VA facilitates the analysis of spatial and temporal patterns in terrorist activities, enabling analysts to identify hotspots, anticipate potential threats, and monitor the evolution of terrorist networks over time (Andrienko et al., 2017; Wu et al., 2017). Integrating VA into terrorism analytics enables a more nuanced understanding of how terrorist incidents are distributed across different regions and periods, which is crucial for effective counterterrorism strategies (Demsar, 2017).

2.4 Data Integration

Another advantage of VA is its ability to support comprehensive analyses of data drawn from multiple sources. Alexander et al. (2021) assert that data integration enhances collaboration, provides enriched contextual insights, and leads to actionable outcomes. In counterterrorism, data often comes from various platforms, including social media, surveillance footage, intelligence reports, and public records. VA frameworks enable the fusion of diverse information sources to produce a cohesive analysis, revealing hidden connections and insights that might otherwise remain undetected.

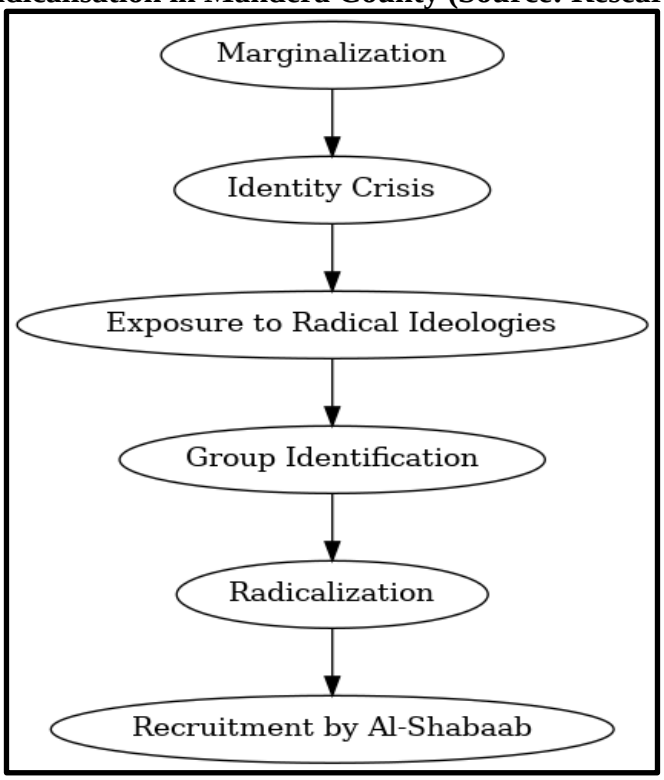
2.5 Theoretical Review

The theoretical framework that underpins this study is essential for understanding the complex dynamics of terrorism, security challenges, and counterterrorism strategies. The literature on these topics is extensive, drawing from multiple disciplines including political science, security studies, and social psychology. This section reviews and synthesises the most relevant theories, emphasising their applicability to the research problem. The discussion critically examines the strengths and limitations of these theories, compares their perspectives, and relates them to the specific context of Mandera County.

2.5.1 Social identity theory and radicalisation

Social Identity Theory (SIT), originally developed by Tajfel and Turner, is pivotal for analysing radicalisation and extremist behaviour (Strindberg, 2020). SIT posits that individuals derive their identity from group affiliations, often reinforcing an 'us versus them' mentality. Extremist groups like AS exploit this sense of belonging by manipulating social and religious identities to recruit members and justify acts of violence (Hogg, 2016). In the context of Mandera County, where socio-economic marginalisation and ethnic divisions are prevalent, SIT provides a lens to understand how young people are drawn into radicalisation.

FIGURE 2.1
SIT and Radicalisation in Mandera County (Source: Researcher, 2024)



SIT's application in terrorism studies is well-documented. Studies have shown that individuals who feel alienated or marginalised are more likely to identify with radical groups that promise a sense of purpose and belonging (McCauley & Moskalenko, 2017). The theory expounds on AS's recruitment strategy, which frequently targets disenfranchised youth in Mandera County, offering them a sense of identity and community otherwise perceived as

inaccessible. Although SIT effectively explains group dynamics in radicalisation, critics argue that it oversimplifies the multifaceted motivations behind individual involvement in terrorism (Hogg, 2016). While the theory explains radicalisation through group affiliation and identity-based exclusion, the VA framework translates these dynamics into observable behavioural indicators and relational visualisations. This synthesis transforms SIT's theoretical principles into actionable intelligence, enhancing its practical utility for proactive counterterrorism efforts. Using the framework clarifies the spatial and behavioural links between recruitment patterns and attack locations, offering deeper strategic insights.

2.5.2 Theories of counterterrorism and state response

The theories of counterterrorism have evolved significantly in recent years, shifting from a predominantly militaristic approach to more nuanced strategies that include socio-economic interventions. The Hard vs. Soft Power Dichotomy is central to these discussions, with 'hard power' involving military force and security measures, whereas 'soft power' emphasises winning hearts and minds through economic development, education, and community engagement (Nye, 2019). In the case of Mandera County, Kenya's reliance on hard power, such as security operations and border security, has had mixed results. While these measures have been necessary to curb immediate threats, they have not addressed the underlying issues of poverty, unemployment, and marginalisation that fuel radicalisation (Smith, 2017).

Recent studies advocate for a more balanced approach, integrating hard and soft power strategies to achieve long-term stability (Byman, 2020). Community policing initiatives and local development programs have shown promise in reducing the appeal of extremist groups by enhancing governance and creating economic opportunities (Byman, 2020). However, the effectiveness of soft power strategies in Mandera County is contingent on their ability to gain the trust of local communities, which has been challenging due to historical grievances and

mistrust of the central government (Williams, 2019). Despite growing advocacy for a hybrid hard-soft power strategy, a VA framework can pinpoint the temporal and spatial contexts in which each tactic is most effective. The visualisation of attack frequency, community sentiment, and intervention outcomes enables the data-driven optimisation of counterterrorism strategies.

2.5.3 Border security and transnational terrorism

Border security theories emphasise the importance of securing national borders to prevent the movement of terrorists, weapons, and illicit goods. These theories have gained prominence in transnational terrorism, where porous borders are viewed as a significant vulnerability. In Mandera County, the porous Kenya-Somalia border has been a critical factor in the region's security challenges, enabling easy movement of AS militants and the smuggling of arms and resources into the country from Somalia (Buzan & Hansen, 2020).

Buzan and Hansen (2020) argue that effective border security requires more than physical barriers; it necessitates comprehensive surveillance, intelligence-sharing, and cooperation between neighbouring states. In Mandera County, Kenya's strategy to combat terrorism has included constructing border fences and deploying security personnel. However, the success of these measures has been limited by corruption, inadequate resources, and the complex terrain, which makes surveillance and patrols challenging.

Moreover, the focus on border security alone may not be sufficient. Studies suggest that without addressing the root causes of conflict and providing socio-economic support to border communities, these security measures can exacerbate tensions and drive more people into the arms of extremist groups (Williams, 2019). Thus, while border security is essential, it must be part of a broader strategy that includes diplomatic efforts, economic development, and regional cooperation. Employing VA to pinpoint specific border-crossing locations enables data-driven,

targeted interventions, enhancing the allocation of counterterrorism resources in Mandera County.

2.5.4 The role of technology in counterterrorism

In recent years, the role of technology in counterterrorism has expanded, with advances in data analytics, surveillance, and communication technologies playing a crucial role in monitoring and preventing terrorist activities. The use of big data and artificial intelligence (AI) to predict and respond to terrorist threats is a growing area of interest, with significant implications for security in regions like Mandera County (Chen, 2019). Predictive analytics can help identify potential hotspots for terrorist activities by analysing patterns in historical data, social media activity, and other relevant sources (Johnson, 2017).

Chen (2019) highlights how AI and machine learning algorithms have enhanced surveillance capabilities, allowing for real-time monitoring of potential threats. In Mandera County, such technologies could be instrumental in overcoming the challenges posed by the region's difficult terrain and the limitations of traditional intelligence gathering methods. Nevertheless, the application of technology in counterterrorism raises significant ethical and legal concerns, especially related to privacy and the risk of misuse by state actors.

The effectiveness of technology-based solutions also relies on their integration with on-the-ground intelligence and community engagement strategies (Byman, 2020). Even advanced technological tools may fail to predict or prevent terrorist incidents without integration with local intelligence and community cooperation. While technology enhances counterterrorism, it often generates vast, complex datasets that are difficult to interpret and act upon in real time. A VA framework addresses this challenge by transforming fragmented, high-volume data into intuitive, interactive visual formats, enabling faster insight generation, improved situational awareness, and more coordinated responses across security agencies.

2.6 Empirical Review

This section reviews empirical studies on the application of VA frameworks in counterterrorism, with a focus on mapping, predicting, and managing terrorism-related data. The review highlights how VA has been used to uncover spatiotemporal patterns and threat dynamics. Mandera County, Kenya, is used as a case study to demonstrate the practical relevance of VA tools in identifying threats, guiding interventions, and optimising strategic decision-making.

2.6.1 Prior studies on VA in counterterrorism

Empirical research indicates that VA frameworks can significantly enhance counterterrorism by enabling the analysis of large and complex datasets. Hegde (2016) developed a VA approach combining Social Network Analysis (SNA) with terrorism-related data from sources such as the GTD and social media. The methodology employed visual tools, including pie charts, maps, and network diagrams, to illustrate trends, relationships, and spatial distributions of terrorist incidents. These visualisations helped uncover hidden patterns and produced actionable insights for informed counterterrorism planning.

Similarly, Mansoour (2017) introduced a VA tool known as Terrorist Watcher, which used interactive visualisations to examine demographic profiles and relational networks among terrorists. This approach enabled analysts to examine the individual-level characteristics of suspects, providing a deeper understanding of radicalisation pathways and informing targeted intervention strategies.

Both studies demonstrate the capacity of VA to enhance the detection of terrorist networks and hotspots. However, they also highlight a critical gap: the underrepresentation of spatiotemporal characteristics in existing frameworks. These limitations underscore the need

for VA models that incorporate predictive analytics to forecast future threats based on historical trends, thus enabling more precise and proactive counterterrorism strategies.

2.6.2 Spatiotemporal analysis in terrorism research

Spatiotemporal analysis has emerged as a powerful tool for understanding how terrorist activities evolve across time and space. Andrienko et al. (2017) applied spatiotemporal VA techniques to geospatial datasets to identify concealed attack patterns, helping security agencies detect movement flows and predict likely hotspots. This method holds particular value for border regions like Mandera County, where identifying cross-border infiltration points can inform pre-emptive security measures.

Wu (2017) employed temporal heatmaps to track social media activity and monitor the diffusion of extremist narratives over time. These visualisations enabled analysts to detect surges in online radicalisation and identify critical timeframes linked to recruitment and attacks. Such techniques facilitate the timely allocation of security resources in response to temporal spikes in threat activity.

While these tools have proven effective in other regions, their adoption in Kenya remains limited due to infrastructural and technical constraints. A tailored VA framework that integrates spatiotemporal visualisation would support more accurate monitoring and intervention in high-risk areas like Mandera County.

2.6.3 Terrorism trends in Mandera County

Abdi (2018) conducted a detailed analysis of radicalisation patterns in Mandera County, revealing how marginalised youth are often targeted for recruitment by extremist groups like AS. The study stressed the role of local socio-economic conditions in shaping susceptibility to radical ideologies. Muna (2020) assessed the impact of military interventions in the County and found that while such operations reduced the frequency of large-scale attacks, they also intensified local grievances, creating conditions conducive to continued radicalisation.

These findings suggest that counterterrorism strategies in Mandera County must consider not only tactical disruptions but also the underlying social and economic drivers of extremism. Evidence from the Sahel and Somalia similarly supports the use of hybrid hard-soft power approaches that combine military action with community engagement. VA tools can aid this process by visualising where and when each approach is most effective, ensuring interventions are evidence-based and context-sensitive.

2.6.4 Impact of data integration in counterterrorism efforts

The effectiveness of counterterrorism efforts increasingly relies on the integration of diverse data sources. Chen (2017) demonstrated how combining structured datasets (e.g., incident reports) with unstructured sources (e.g., social media and surveillance footage) through VA tools significantly improved the timeliness and accuracy of threat detection. Integrated VA systems offer a holistic understanding of terrorist networks and enable faster responses to emerging threats.

Nonetheless, challenges remain. Wu et al. (2017) noted that data integration efforts are often hindered by high technological costs, data privacy concerns, and the shortage of skilled analysts. These barriers are especially pronounced in resource-constrained regions like Mandera County. A customised VA framework can help bridge these gaps by automating the

integration and visualisation of multi-source data, making complex information more accessible and actionable even in low-resource settings.

2.7 Challenges in Applying VA in Counterterrorism Efforts in Mandera County

Despite the significant potential of VA frameworks to enhance counterterrorism in high-risk regions, their effective deployment in Mandera County faces several critical challenges. A primary limitation is the County's inadequate infrastructure and limited access to advanced technological resources necessary for real-time data processing, predictive modelling, and high-performance computing (Lopez, 2021). These deficits hinder the operationalisation of VA systems. Moreover, the shortage of trained personnel capable of managing and interpreting large, complex datasets further restricts the practical application of VA. Specialised training and continuous capacity building are required, yet remain underdeveloped in the region.

Institutional factors also undermine the implementation of VA tools. Corruption and inefficiencies within the security apparatus can compromise the accuracy and utility of insights generated by VA systems (Turi, 2021). Even when actionable intelligence is available, it may be misused, ignored, or distorted, ultimately weakening operational responses and eroding public trust in counterterrorism efforts.

Mandera County's geographic and socio-political context further complicates matters. Its proximity to the Somalia border and porous boundary lines make it vulnerable to cross-border insurgencies by groups like AS, who exploit these corridors for recruitment and arms trafficking (Emase et al., 2017). Additionally, internal clan dynamics, historical marginalisation, and limited state presence diminish the effectiveness of conventional intelligence-gathering. A VA framework, however, can provide a structured, data-driven approach by integrating demographic, socio-political, and geospatial data to identify vulnerable

communities and infiltration hotspots. This could enable pre-emptive, localised interventions aimed at reducing the spread of extremist ideologies.

The psychological and social impacts of terrorism on Mandera County's communities are profound. Frequent attacks not only endanger physical safety but also breed fear, mistrust, and societal fragmentation. A VA framework, through its capacity to identify high-risk areas and visualise threat patterns over time, can support more efficient, community-focused interventions. Enabling real-time decision-making, this framework will enhance resource allocation, strengthen incident response, and promote social resilience.

While these challenges are significant, the opportunities for VA remain compelling. The integration of multi-source data offers the potential to generate predictive models and heatmaps that anticipate attack locations or trace terrorist networks. These capabilities can significantly augment traditional counterterrorism approaches, especially in regions like Mandera County where conventional methods have struggled to produce sustained results.

Global terrorism trends continue to evolve, with the 2023 Global Terrorism Index (GTI) reporting increased deaths in the Horn of Africa due to AS operations. Kenya, and Mandera County in particular, witnessed a surge in bombings and armed assaults in 2022. A VA framework could complement existing strategies by revealing tactical patterns such as IED deployment trends or weapons supply routes, helping security agencies disrupt operations before they escalate.

Kenya's shift toward proactive, intelligence-led counterterrorism aligns well with the strengths of VA. Muibu and Çubukçu (2023) note that recent improvements in pre-emptive security operations reflect the benefits of data-driven decision-making. VA frameworks can sharpen this approach by focusing on verified threats rather than relying on broad profiling practices, thereby improving operational efficiency and reducing collateral social harm.

However, the deployment of VA systems raises ethical considerations, particularly regarding privacy and surveillance. The extensive data collection required could be misused without strict legal frameworks and oversight mechanisms. Safeguards must be implemented to prevent mass surveillance, discrimination, or abuse. Furthermore, VA could play a constructive role in addressing socio-economic drivers of radicalisation, such as unemployment and political exclusion, by integrating socio-economic indicators into spatial threat models. This would support holistic counterterrorism strategies that combine security measures with community development and engagement (Mutisya, 2024).

2.8 Pre-Indicators of Terror Activities

Understanding the indicators and pre-attack behaviours of terrorist operations is critical for effective counterterrorism strategies, especially in high-risk regions. Bennett (2017) outlines that terrorists typically follow a series of planning stages, such as target selection, surveillance, and logistical preparation, before executing an attack. Monitoring these stages can reveal observable patterns that offer timely intervention opportunities.

In the target selection phase, terrorists assess factors such as attractiveness, risk, and vulnerability to determine optimal targets. Following this, they conduct intelligence-gathering through overt surveillance and subtle, seemingly harmless interactions designed to expose security weaknesses. A key stage involves testing security measures, where operatives may trigger minor incidents or false alarms to gauge the response of security forces. Intrusion attempts, such as unauthorised entries, are often used to gather further information or pre-position materials.

Acquiring operational supplies, including weapons, explosives, identification documents, vehicles, and financial resources, is a vital step. Suspicious behaviours like impersonation or cross-border movements often surface during this stage and can serve as red flags. Dry runs or

rehearsals are also carried out to ensure preparedness. Finally, asset deployment, where personnel and materials are positioned for the attack, represents the last identifiable stage before execution. VA can help detect these pre-attack indicators by integrating and visualising behavioural and logistical data, thereby enhancing proactive security responses in high-risk zones such as Mandera County, where AS maintains active influence.

In support of these observations, Gill (2020) argues that terrorist attacks result from a convergence of motivated offenders, vulnerable targets, and ineffective guardianship. This 'opportunity model' underscores the value of early detection: terrorists weigh risks, rewards, and environmental conditions when planning attacks. Identifying such spatiotemporal patterns in regions like Mandera can inform targeted interventions, such as increasing surveillance, reinforcing vulnerable sites, and building community resilience.

LaFree and Freilich (2016) further suggest that temporal analysis of terrorist behaviour can reveal group-specific planning cycles based on ideology, operational goals, and size of attack units. Tracking precursor activities, such as the movement or online activity of AS operatives, can refine VA frameworks, strengthen counterterrorism strategy, and reduce the likelihood of successful attacks in vulnerable areas like Mandera County.

2.9 Visual Analytics in Terrorism Research

VA has emerged as a powerful and robust tool in terrorism research, blending human analytical judgment with algorithmic speed and precision. This fusion is particularly valuable in counterterrorism, where quick and accurate interpretation of complex data is essential. According to Cui (2019), VA transforms raw data into intuitive visual formats, such as graphs, charts and maps, streamlining the analytical process and reducing cost and time. Enabling users to efficiently detect patterns, trends, and anomalies, VA supports more informed and timely decision-making.

Guo et al. (2016) highlight the importance of integrating data mining, statistical analysis, and VA to reveal the socio-temporal contexts of terrorist events. Terrorist incidents are embedded within specific spatial and temporal contexts, demanding analytical systems that allow for dynamic, interactive exploration. VA helps uncover key actors, emerging behavioural trends, and geo-temporal correlations critical to effective counterterrorism planning.

A common application of VA in terrorism research is through spatiotemporal thematic maps and statistical charts. These tools visualise the frequency, intensity, and geographic distribution of terrorist activities across time. Events may be displayed as points, paths, or clusters, with temporal trends shown on axes to reveal patterns such as escalation cycles, geographic dispersion, or coordinated attacks. Statistical charts, including line graphs, bar charts, and scatter plots, further enhance VA by showing relationships, fluctuations, and associations within the dataset. Proportional and relational charts, like pie charts, treemaps, and chord diagrams, help map the structure of terrorist networks and their internal dynamics.

Despite the proven effectiveness of VA tools, their application in Kenya, particularly spatiotemporal VA frameworks, remains limited. This presents a missed opportunity in counterterrorism strategy. Implementing VA could transform how data is interpreted and acted

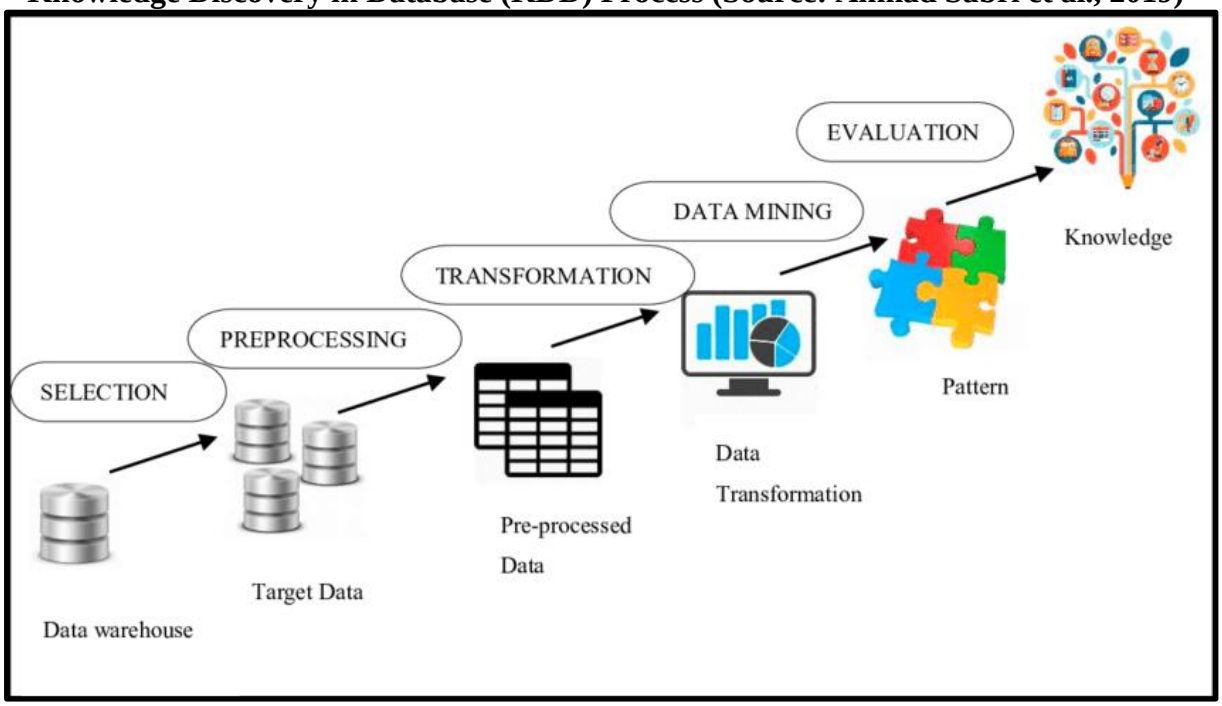
upon, enabling real-time pattern recognition, predictive threat modelling, and targeted deployment of resources. Techniques such as hotspot analysis and buffer zone mapping would help identify high-risk areas and inform both immediate response and long-term planning.

Hegde et al. (2016) developed a VA methodology for terrorism data in India, integrating SNA with data from the GTD, news media, and social platforms. Their approach involved two key phases: data collection and visualisation through charts, maps, and network diagrams. While effective for retrospective analysis, the framework would be significantly enhanced by incorporating predictive modelling to anticipate future threats.

Mansoour (2017) introduced 'Terrorist Watcher,' a VA tool designed to profile individual terrorists rather than entire organisations. This system focuses on demographic and behavioural traits, aiding analysts in identifying early indicators of radicalisation. Such personalised analysis is particularly relevant in localised contexts like Mandera County, where extremist recruitment often targets vulnerable individuals.

Many VA frameworks adopt a modified version of the Knowledge Discovery in Databases (KDD) process, which includes data selection, preprocessing, transformation, mining, and evaluation (Ahmad Sabri et al., 2019). This study applies a similar process, integrating these steps into the development of a tailored VA framework for terrorism monitoring and prediction.

FIGURE 2.2
Knowledge Discovery in Database (KDD) Process (Source: Ahmad Sabri et al., 2019)



VA offers a strategic advantage for counterterrorism, particularly in countries like Kenya that face these complex and evolving threats. Transforming complex data into visual formats, VA enables more effective analysis, informed decision-making, and proactive responses. A VA framework anchored in spatiotemporal analysis could significantly strengthen Kenya's national security infrastructure by enhancing anticipation, prevention, and response to terrorism.

2.10 Knowledge Gaps

Despite significant advances in terrorism research and counterterrorism strategies, notable gaps persist, particularly in integrating advanced technologies for real-time monitoring, analysis and intervention. Most existing studies have focused on static data and retrospective reviews of terrorist events, offering valuable historical insights but falling short in terms of responsiveness to current and emerging threats. These traditional methods often lack the interactivity, adaptability, and predictive capabilities required for timely, effective counterterrorism action. Bridging this gap calls for dynamic, data-driven frameworks such as a VA framework, which can process real-time data and support proactive decision-making in volatile environments.

2.10.1 Underexplored key areas

Current research often overlooks the integration of advanced VA and predictive modelling tools, which have the potential to generate real-time insights into terrorist activity by processing large-scale, multidimensional data. These capabilities are particularly critical in high-risk regions, where traditional static methods often prove inadequate.

Although many existing frameworks build on the KDD process, they do not fully utilise interactive visualisation techniques or integrate real-time data sources. This limits the responsiveness of counterterrorism systems and delays timely, informed decision-making.

The application of spatiotemporal visualisations for analysing and anticipating terrorism trends in Kenya remains underdeveloped. Effective counterterrorism strategies demand a nuanced understanding of spatial and temporal dynamics, an area where current models are insufficient.

Furthermore, Mandera County presents a distinct set of challenges due to its socio-political and geographic complexities. Issues such as cross-border insurgency, local radicalisation, and infrastructural vulnerabilities require a tailored approach that general

counterterrorism frameworks often fail to address. These limitations are summarised in Table 2.1.

TABLE 2.1
Summary of Research Gaps in VA for Counterterrorism

Research Gap	**Description**	**Implications**
Limited Integration of Advanced VA Tools	Underutilisation of advanced VA tools and predictive models for real-time terrorist activity monitoring.	Reduces capacity for timely threat detection and limits pre-emptive response strategies.
Real-Time Interactive Data Integration	Existing frameworks fail to effectively incorporate real-time data and interactive visualisation features.	Delays in generating actionable insights limit timely response to evolving threats.
Lack of Spatiotemporal Visualisation in Terrorism Analysis	Spatiotemporal tools are rarely used to map and analyse terrorist activity across regions and timeframes.	Limits understanding of spatial-temporal patterns, undermining precision-targeted countermeasures.
Context-Specific Framework Limitations	Generic frameworks overlook Kenya's unique socio-political and geographic challenges.	Counterterrorism strategies risk overlooking key local drivers such as cross-border insurgency and marginalisation.

2.11 Conceptual Framework

The conceptual framework presented in this study proposes a robust VA system to improve the monitoring and analysis of terrorism-related data via interactive visualisations. The framework integrates VA principles with the KDD process to enhance counterterrorism efforts through more effective monitoring, prediction, and response strategies.

Central to the framework are visuals that follow Shneiderman's visual information-seeking mantra of 'overview first, zoom and filter, details on demand'. This user-centric approach enables counterterrorism analysts to navigate complex datasets effectively. The 'overview first' presents a dashboard offering a comprehensive view of Mandera County's terrorism landscape, allowing users to grasp overarching trends before focusing on specific details. The zoom and filter functionality enables in-depth exploration of specific attributes of interest, such as region, time period, or incident type, revealing patterns that may not be immediately apparent. Details on demand provide access to granular information as needed, ensuring data remains accessible and actionable throughout the analysis process.

Key components of the framework include data collection and cleaning from established terrorism databases that include the GTD, ACLED, and the CVE Research Hub. This data undergoes thorough cleaning and normalisation, creating a unified dataset with spatial, temporal, and thematic attributes essential for reliable visualisation and analysis. Exploratory Data Analysis (EDA) further investigates pre-attack indicators such as planning activities, surveillance, and security testing. Visualisations through spatiotemporal maps and thematic charts highlight trends and relationships in terrorist activities, with hotspot and buffer analysis identifying high-risk areas and potential escape routes.

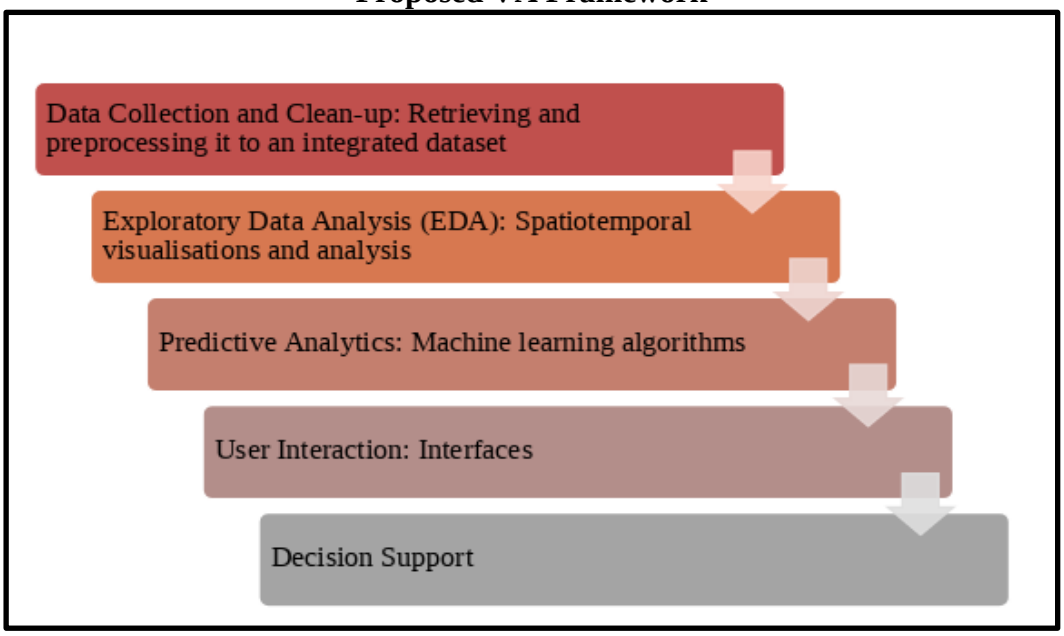
Predictive analytics leverages historical data to build models capable of forecasting future terrorist attacks, incorporating time-series forecasting, risk assessment, and hotspot prediction.

Real-time monitoring tools enhance situational awareness by providing interactive insights into potential trends and areas of concern, allowing for proactive responses rather than reactive ones. Interactive visualisations, such as trend, proportion, and relationship charts, enhance the analysis, with a user-friendly interface that allows for customisation, filtering, and retrieval of specific data details tailored to various analytical needs.

The framework supports the assessment of 'what-if' scenarios to evaluate the impacts of alternative counterterrorism strategies and empowers decision-makers to make informed choices. Through intuitive visualisations that support resource allocation and proactive interventions, the framework provides a comprehensive view of terrorist activities, enabling the identification of patterns and trends that can shape long-term strategies.

The proposed VA framework represents a significant advancement in using VA for counterterrorism. Integrating data collection, exploratory analysis, predictive modelling, and interactive visualisation, the framework guides analysts and researchers in navigating complex terrorism data with precision, supporting evidence-based decisions and proactive measures. This integrated approach enhances evidence-based decision-making and contributes to long-term regional security and stability.

FIGURE 2.3
Proposed VA Framework



2.12 Operationalisation of Variables

This section visually represents the relationships between key variables in the study, emphasising their interrelationships and reciprocal influences. A mind map illustrates the dependencies among variables, while an accompanying table details the operational definitions of each variable. Together, the visuals clarify the study's conceptual framework and its strategy for measuring and analysing these variables. Table 2.2 presents the detailed list of study variables.

2.12.1 Mind map: Dependencies between variables

This mind map illustrates the relationships among key variables in the study, showing how outcomes, such as injuries, fatalities, and property damage, are connected to the time, location, and nature of terrorist incidents.

TABLE 2.2
Operationalisation of Variables (Source: Researcher, 2024)

Variables (Category/Name)	**Indicator**	**Data Type/ Format**
Temporal Variables		
Date	Exact date of the event	Date values (e.g., MM/DD/YYYY)
Geographical Variables		
Latitude	Geographical latitude of the event location	Float (Decimal degrees)
Longitude	Geographical longitude of the event location	Float (Decimal degrees)
Location	Name of the location where the event occurred	Text
Sub-County	Administrative division where the event occurred	Text
Incident Characteristics		

Event Type	Type of event (e.g., bombing, armed assault)	Categorical (Text)
Weapons Type	Type of weapon used in the event	Categorical (Text)
Target Type	General category of the target (e.g., military, civilian)	Categorical (Text)
Target Sub-Type	Specific subtype of the target	Categorical (Text)
Outcome Variables		
Injured	Number of people injured	Integer
Fatalities	Number of people killed	Integer
Abducted	Number of people abducted during the event	Integer
Property Damaged	Binary indicator of property damage during the event	Boolean (Yes/No)

2.13 Summary

Chapter 2 reviews literature on terrorism and counterterrorism strategies, emphasising the role of VA and predictive modelling in enhancing strategic response and operational planning. It explores the specific counterterrorism challenges facing Kenya and highlights the importance of advanced analytical tools in improving responsiveness and decision-making. The chapter further examines early warning indicators, network analysis techniques for identifying key actors, and VA tools for visualising spatiotemporal threat patterns. It also discusses the application of machine learning in forecasting terrorist activity based on historical data to enhance situational awareness and enable proactive interventions.

A major shortcoming in existing studies is the lack of a VA framework that integrates interactive visualisations with predictive analytics tailored for high-risk environments. This chapter provides the theoretical foundation for developing such a framework, aligned with the distinct socio-political and geographical conditions of vulnerable regions like Mandera County. This grounding informs the design and implementation of the VA framework presented in subsequent chapters.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology used to develop and evaluate the VA framework, which aims to enhance counterterrorism efforts. The study adopts a mixed-methods approach, integrating qualitative and quantitative techniques to address the complexity of terrorism data. Data sources include structured and unstructured formats, with detailed processes for data collection, cleaning, and integration. Central to this methodology is the application of spatiotemporal data mining techniques, which identify meaningful patterns and trends, alongside predictive modelling to enhance the framework's ability to anticipate potential terrorist activities. Ethical considerations, particularly those related to data privacy and the ethical handling of sensitive information, are addressed to ensure compliance with established standards. The chapter concludes by outlining the study's limitations and the strategies employed to maintain validity and reliability, thereby laying a solid foundation for the rigorous and adaptable VA framework developed in this study.

3.2 Target Group

This study primarily focuses on the residents of Mandera County, an area significantly impacted by the persistent threat of terrorism. This study aims to assess the impact of terror attacks on the local population's daily lives, livelihoods, and social dynamics. Particular emphasis is placed on vulnerable groups such as women, children, and youth, who are disproportionately affected by ongoing violence. In addition to the residents, the study engages key stakeholders who play a critical role in the region's security and development. These include local government officials, security personnel, community leaders, educators, and healthcare providers. Engaging these stakeholders enables the study to gain insights into the region's security challenges and explore potential mitigation strategies.

The study group also includes civil society organisations and non-governmental organisations (NGOs) in the region, which offer unique insights into the County's socio-economic conditions and play an instrumental role in implementing grassroots initiatives to counter radicalisation and promote peace. Incorporating these perspectives allows the study to present a comprehensive view of the impact of terrorism on Mandera County. This inclusive approach ensures that the findings and recommendations reflect the lived experiences of those most affected by the conflict and the practical realities faced by those working to address the region's security challenges.

3.3 Research Design

This study adopted a case study approach to examine the complexities of terrorism within Mandera County, Kenya, a region severely impacted by threats from the AS terror group. This method provided a structured framework to examine the multifaceted issues faced in real-world settings (Hancock 2021). Mandera County was purposefully selected due to its persistent exposure to terrorism, with reports from local authorities emphasising the extensive influence of AS in the region (Otsialo, 2023), thus highlighting the urgent need for a deeper understanding of terrorism dynamics in this context.

The research design combined exploratory and descriptive approaches. The exploratory aspect was appropriate due to the absence of VA frameworks tailored to Kenya's terrorism landscape, facilitating the identification of novel areas of inquiry and emerging insights. The descriptive component provided a comprehensive account of the current state of terrorism and counterterrorism responses in Mandera County (Alotaibi, 2017), forming the empirical foundation for developing the proposed VA framework.

Focusing on the spatiotemporal aspects of terrorist activities, this case study approach facilitated an in-depth analysis of the interrelationships between various contributing factors.

It supported the identification of patterns, trends, and underlying mechanisms essential for advancing a data-driven, context-specific counterterrorism strategy. The findings contribute to the creation of a robust VA framework designed to address Kenya's unique counterterrorism challenges.

3.4 The Data Needed

The development and implementation of a comprehensive VA framework for counterterrorism requires a diverse and extensive dataset. The study utilised key data sources, including historical records on terrorist incidents, covering locations, dates, and attack types, to identify patterns and trends over time. Additionally, demographic and socio-economic data, such as population distribution, employment rates, education levels, and political dynamics, were essential for understanding the underlying drivers of terrorism.

A purposive sampling technique was employed to ensure that the data analysed accurately reflected observed trends during the review period. The dataset was developed from existing comprehensive sources and covered multiple years, with particular focus on the escalation and spatial concentration of attacks across Mandera County's Sub-Counties. This approach allowed for the targeted analysis of the frequency, nature, and geographic distribution of terrorist activities.

Spatiotemporal data capturing the distribution of attacks over time and space were critical for generating accurate visualisations and predictive models. Real-time data, such as current security reports, intelligence bulletins, and relevant social media activity, further enriched the dataset by providing timely insights into emerging threats and tactics. Collectively, these data sources enabled a comprehensive analysis of terrorism dynamics in Mandera County, enabling the development of a robust, context-sensitive counterterrorism framework.

Various data collection instruments were used to capture the spatial and temporal dimensions, including geospatial mapping tools and statistical software. This rigorous and integrated data collection approach underpinned the analytical methods and outcomes presented in this study.

3.3.1 The study population

The study examines terrorist activities within Mandera County, utilising data spanning from 2013 to 2023. The research population comprises all documented terrorist events recorded during this period, including details on incident types, targeted groups, geographic locations, and the impacts on both security installations and civilian populations. This broad scope enables the study to capture the multifaceted nature of terrorism in the region, offering a comprehensive understanding of its patterns, actors, and consequences.

3.3.2 Data collection and analysis techniques

Mazhar (2021) emphasises the importance of data collection in research, asserting that without it, research efforts cannot progress. This study adopted a comprehensive approach to data collection, drawing on multiple secondary sources to compile a robust dataset for the development of a VA framework to monitor terrorism. The integration of diverse data sources facilitated a holistic understanding of terrorism-related patterns and dynamics in Mandera County.

The data were sourced from both structured and unstructured sources. Structured data was obtained from established databases, including the GTD, ACLED, and the CVE Research Hub. These databases provided detailed information on terrorist incidents, such as perpetrators, targets, methods, and outcomes. Introduced in 2007, the GTD is one of the largest and most comprehensive databases available (Hermann, 2023). It is an open-source resource that covers over 200,000 terrorist events from 1970 to 2021, including details such as the date, location,

weapons used, targets, casualties, and responsible parties. This database is maintained by the Study of Terrorism and Responses to Terrorism (START) to support academic research and inform counterterrorism initiatives (START, 2021).

Although the GTD covers worldwide terrorist events, this study focused specifically on those orchestrated by the AS terror group that affected Mandera County. The GTD comprises 107 column attributes, and key variables for this study included the GTD ID (Year, Month, Day), Incident Information (Incident Summary), Incident Location (Country, Region, Province/State, City, Location Details, Latitude, Longitude), Attack Information (Attack Type), Weapon Information (Weapon Type), Target/Victim Type (Target/Victim Subtype), Perpetrator Information (Perpetrator Group Name), and Casualties and Consequences (Total Number of Fatalities, Property Damage, Total Number of Hostages/Kidnapping Victims) (START, 2021). The data was downloaded as a Microsoft Excel Worksheet (.xlsx) and filtered using the Incident Location variables, with the Region set to Sub-Saharan Africa, Country to Kenya, and Provstate to Mandera. This filtering yielded 184 event records from Mandera County between 2013 and 2021.

The ACLED dataset compiles global political disorder events, covering political violence, protests and other forms of unrest. It monitors various conflict actors and types of unrest through a researcher-led data collection process incorporating local-language media, conflict observatories, and situation reports, thus reducing reliance on international news agencies (Carboni & Raleigh, 2024). The Global Terrorism Index (GTI, 2023) emphasises that violent conflicts are a primary driver of terrorism, with over 88% of attacks and 98% of terrorism deaths in 2022 occurring in conflict-affected countries. The ACLED Data Export tool was used to download a dataset covering the past three years (2020–2023). The data were

filtered to focus on Kenya, specifically using the keyword ‘Al-Shabaab’, resulting in 149 records with 32 variables spanning the period from 2020 to 2023.

The CVE database offered localised insights into terror attacks in Mandera County, as it was compiled locally within Kenya. The CVE Research Hub, hosted by the Centre for Human Rights and Policy Studies (CHRIPS), includes the Terror Attacks and Arrests Observatory, which compiles disaggregated data on terror-related incidents and arrests in Kenya, drawing on local partners and media sources. This observatory provided a rich dataset for analysing trends and informing policy (CVE Kenya, 2023). The data, spanning from 2017 to 2020, included 32 variables and was downloaded in .xlsx format. Using the ‘County’ attribute, the events were filtered to focus on Mandera County, resulting in 61 records.

Document reviews were employed as a secondary data collection technique, involving the systematic examination of terrorism-related reports, academic studies, and other authoritative publications (Taherdoost, 2021). This included analysing terror reports, academic studies, and other authoritative documents on terrorism in Mandera County. This process helped establish historical context, identify prevailing trends, and corroborate data.

3.5 Data Processing and Analysis

3.5.1 Data reduction, cleaning, and integration

Data cleaning involved detecting and correcting or removing incorrect, incomplete, or irrelevant records. Data reduction minimised the dataset size, enabling more efficient analysis. Data integration combined multiple sources into a unified dataset for comprehensive interpretation (Maharana et al., 2022). Cleaning structured data from sources such as GTD, ACLED, and the CVE Research Hub addressed typical data quality issues, including duplicate records and missing values. Duplicate entries were eliminated, and missing data were supplemented using credible online sources.

Data reduction applied to the GTD and ACLED datasets enhanced manageability (Ur Rehman, 2016). Irrelevant columns were dropped using Python, reducing the GTD dataset columns to 20 and the ACLED dataset columns to 16. Dates in the ACLED dataset were split into iyear, imonth, and iday to align with GTD's format, ensuring consistency and facilitating integration.

Database integration was crucial to merging these diverse sources into a cohesive dataset (Naeem, 2019). Using Python's pd.concat() function, the GTD and ACLED datasets were combined into the gtd_acled dataset, which was then sorted chronologically and geographically to support pattern analysis. The CVE dataset's date format was standardised to match the GTD and ACLED format and subsequently merged with gtd_acled, forming the gtd_acled_cve dataset. Further processing involved creating unified variables by merging columns with similar attributes, such as event_location (from 'city' and 'LOCATION') and event_fatalities (from 'fatalities' and 'FATALITIES'). This ensured consistency across all datasets. Temporal alignment of timestamps provided a coherent timeline, and data fusion integrated structured and unstructured sources into a comprehensive dataset for analysing terrorism in Mandera County.

3.5.2 Data transformation

The dataset underwent extensive geospatial transformation to enable spatial analysis of terrorist events. A GeoDataFrame was generated by converting the longitude and latitude columns into geometric points using the WGS 84 (EPSG:4326) coordinate reference system (CRS). The dataset was then exported into GeoJSON format to facilitate mapping. GeoJSON files containing administrative boundary data for Mandera County and its Sub-Counties were imported, and a spatial join was performed to link each incident to the correct Sub-County. The total number of incidents per Sub-County was computed and joined to the boundary

GeoDataFrame. This transformation provided the spatial structure required for a comprehensive geospatial analysis of terrorism patterns across Mandera County.

Analysis revealed inconsistencies in area names across the datasets, posing a challenge, as identical locations were listed differently. For instance, a location in Kotulo Sub-County appeared as ‘Daba Siti’ in the ACLED dataset and ‘Dabasiti’ in the GTD dataset. These discrepancies were resolved by creating a standardised reference list to unify variations of the same location under a consistent name. A manual review and correction of the data was also undertaken due to the complex and overlapping settlement names common in Mandera County. This involved realigning location coordinates to ensure the location was accurately placed within the correct coordinates and Sub-Counties. The outcome was a harmonised dataset containing 20 attributes and 335 event entries spanning 2013 to 2023. A preview of the final data is shown below in Table 3.1:

TABLE 3.1
A snippet of the standardised dataset utilised in the study

ID	Year	Month	Day	Date	Day_Txt	Summary	Latitude	Longitude
0	2016	12	2	02/12/2016	Friday	Three people are injured in Mandera after thei...	2.4607	40.6644
1	2014	8	4	04/08/2014	Monday	08/04/2014: Assailants fired rocket-propelled ...	3.934	41.8558
2	2014	10	15	15/10/2014	Wednesday	10/15/2014: An explosive device detonated targ...	3.9387	41.8447
3	2015	3	13	13/03/2015	Friday	03/13/2015: Assailants fired a rocket-propelle...	3.6359	41.5605
4	2019	7	15	15/07/2019	Monday	07/15/2019: An explosive device detonated agai...	3.6424	41.0164
...	...	...	...	...	...	...	...	...
330	2023	8	8	08/08/2023	Tuesday	Movement of forces: On 8 August 2023, suspecte...	3.9208	41.2192
331	2015	12	26	26/12/2015	Saturday	12/26/2015: An explosive device detonated as i...	2.809	40.9274
332	2020	7	13	13/07/2020	Monday	Detonation: On 13 July 2020, a man, suspected...	3.9538	41.8846
333	2021	12	11	11/12/2021	Saturday	Detonation: On 11 December 2021, three Al Shab...	3.1597	41.3256
334	2021	7	31	31/07/2021	Saturday	On 31 July 2021, Al Shabaab militants attacke...	3.3911	41.4184

3.6 Data Analysis Methodology

EDA was a central aspect of the methodology, supporting the understanding of terrorism dynamics in Mandera County. The study employed a range of visualisation and analytical techniques to interpret the data, detect patterns, and present the findings effectively. Python programming libraries were used for these purposes, including 'Pandas' for data management, 'Geopandas' for processing spatial data, 'Folium' for generating interactive maps, 'Matplotlib' for statistical visualisations, and 'Scikit-learn' for implementing machine learning models.

3.6.1 Geographic data visualisation and analysis

Geographic visualisation played a pivotal role in analysing the spatial distribution of terrorism incidents within Mandera County. In this study, spatial analysis was conducted using geospatial datasets and mapping tools to highlight the locations and frequencies of terror-related events across the various Sub-Counties.

The mapping process began by initiating an interactive 'Folium map', centred on the coordinates of specific incidents within Mandera County. This base map served as a foundation for layering additional visual elements. 'GeoJSON' files containing administrative boundary data for Mandera County and its Sub-Counties were imported into GeoDataFrames. A spatial join was then carried out to associate each recorded incident with its corresponding Sub-County boundary.

The number of incidents per Sub-County was computed and incorporated into the County-level 'GeoDataFrame'. The incident data was converted to 'GeoJSON' format and added to the map as point markers, represented by customised icons symbolising terrorist events. County boundaries were overlaid with 'tooltips' offering contextual details such as incident counts and population density. The map's extent was configured to display all layers

effectively, ensuring a comprehensive and interactive visualisation of terrorism patterns across Mandera County (Folium, 2021).

Subsequently, both static and animated heat maps were developed to depict incident density and temporal progression. Interactive 'tooltips' enriched each Sub-County's display by revealing incident counts and locality names. The heatmap layer was generated using latitude and longitude coordinates to visualise event concentration, with higher-density areas rendered in brighter shades. To enhance this representation, an animated heatmap was created to illustrate the evolution of incidents over time. This involved defining a function to generate timestamp strings based on the year, month, and day variables. The 'GeoDataFrame' was chronologically sorted, and at each interval, incidents up to that point were visualised, resulting in a dynamic temporal map (Huang et al., 2017).

The 'HeatMapWithTime' plugin was employed to integrate the animated layer, enabling observers to track the spatial and temporal progression of terrorist incidents across Mandera County. This dual-layer visualisation offered critical insights into both the intensity and timing of attacks, supporting policymakers and security agencies in prioritising their interventions effectively (Folium, 2021)

3.6.2 Statistical data visualisation and analysis

This study utilised statistical data visualisation to reveal patterns, distributions, and inter-variable relationships within the terrorism-related data from Mandera County. The process began with generating descriptive statistics, offering an overview of key variables such as fatalities, attack types, target categories, and weapons deployed. Measures of central tendency, including the mean, median, and mode, alongside standard deviation, were calculated to assess data variability and general characteristics (Taherdoost, 2021).

Temporal analysis was performed to explore trends in terrorist activity over time. Time series plots were created to visualise the number of incidents occurring each year, with the data aggregated by year and month to identify seasonal or annual patterns. Line charts highlighted periods of increased or decreased activity, helping to pinpoint significant events or shifts in terrorist behaviour over the study period from 2013 to 2023. This temporal analysis was critical for understanding how terrorism in Mandera County evolved (Hermann, 2023).

Categorical data analysis was another important component of the statistical visualisation process. Bar charts and histograms were used to compare the frequency of different variables such as attack types, target types, and weapons used. For example, bar charts effectively displayed the distribution of attack types (e.g., armed assault, bombing/explosion) and target types (e.g., government institutions, civilians), making it easy to identify the most common forms of attacks and the most frequently targeted entities. Pie charts were utilised to summarise the proportions of different variables, such as the distribution of weapon types, providing a concise visual overview of the categorical variables.

Correlation analysis was conducted to explore relationships between various variables in the dataset. Correlation matrices were generated and visualised using heatmaps, where the colour intensity indicated the strength of the correlation between variables, such as the number of incidents, fatalities, and population density. This analysis was instrumental in identifying significant relationships that offered deeper insights into the factors influencing terrorism in the region. Understanding these correlations helped elucidate the interplay between different aspects of the data.

Finally, exploratory analysis was performed using scatter plots and box plots. Scatter plots were used to examine the relationship between continuous variables, such as the correlation between the number of incidents and population density, offering a visual

representation of potential associations or trends. Box plots displayed the distribution and outliers in variables such as fatalities across different attack types, helping to identify anomalies or variations within the data. These graphical tools were essential in making the data more interpretable and accessible, supporting the study's objective of understanding terrorism dynamics in Mandera County.

3.7 Operationalisation of Research Objectives

This study employed a mixed-methods approach to fulfil its objectives, with a focus on spatiotemporal visualisations and predictive analytics to analyse terrorism patterns. The following section details how each objective was systematically addressed:

3.7.1 Objective 1 (Challenges and Early Warning Indicators)

To establish the foundation for the study, the research began by identifying the challenges impeding counterterrorism efforts in Kenya, alongside potential indicators and early warning signs of terrorist attacks. This was accomplished through a systematic review of literature, in-depth analysis of structured datasets (such as GTD, ACLED, and CVE), and the examination of unstructured data from social media and news sources. This process revealed recurring themes such as fragmented data sources, limited use of geospatial tools, underutilisation of historic data and the need for more robust early warning systems. These insights directly informed the design and focus of the subsequent framework.

3.7.2 Objective 2 (VA Framework Development)

Based on the findings from the first objective, a comprehensive VA framework was developed. This framework was designed to address the specific challenges identified and to utilise the early warning indicators uncovered during the initial phase. It integrates interactive visualisations, such as heat maps and dashboards, with predictive models to support the

forecasting of high-risk areas and periods. The architecture of the framework ensures that insights from the preliminary analysis are embedded within its core functionality.

3.7.3 Objective 3 (Validation and Refinement)

To ensure the framework was both practical and actionable, feedback was sought through stakeholder engagement and expert-led usability testing. Their input led to several refinements, particularly in the dashboard's design and the relevance of the outputs. The methodologies were interconnected throughout the process: for example, clustering results from the data analysis phase informed the predictive models, and both were seamlessly integrated into the framework's visualisations.

3.7.4 Objective 4 (Intervention Strategy Development)

Finally, an intervention strategy was developed that leverages the validated VA framework to enhance counterterrorism efforts in Kenya. This strategy is grounded in the real-world needs and challenges identified at the outset, ensuring that the framework is not just a technical solution but a practical tool for decision-makers and security agencies.

3.8 Event Prediction

Event prediction employed statistical models, machine learning algorithms, and data analytics to forecast the likelihood of future terrorist incidents. Historical data from a unified, standardised dataset was utilised to identify patterns and trends in terrorist activities within Mandera County. Analysing variables such as timing, location, and attack methods facilitated the development of predictive models to estimate the probability of future incidents in specific areas.

Predictive models commonly employ machine learning techniques such as logistic regression, decision trees, and random forests, alongside advanced approaches like neural networks. These models were trained on historical data to identify the conditions most likely

to precede terrorist activities. The modelling process revealed correlations between socio-political events and spikes in terrorism, supporting the anticipation of future incidents under similar circumstances.

Furthermore, GIS tools were integrated with the predictive models to conduct spatial analysis. This enabled the identification of potential hotspots within Mandera County where future attacks were most likely to occur. Mapping these high-risk areas allowed security forces and policymakers to allocate resources and plan interventions more effectively, thereby enhancing their ability to prevent or mitigate the impact of terrorist attacks.

3.9 Decision Making

Decision-making in this context involved utilising insights from event prediction models to inform strategic planning and operational responses. The goal was to translate predictive analytics into actionable intelligence to guide resource allocation, the deployment of security forces, and the formulation of policies that could prevent terrorist activities.

In this study, the decision-making process was informed by a comprehensive analysis of both statistical and geographic data. Understanding patterns and trends in terrorist activities, alongside the socio-economic and demographic factors influencing them, better equips decision-makers to implement targeted interventions. For instance, if predictive models indicated a high likelihood of attacks in a particular Sub-County, security responses such as increased surveillance, additional personnel deployment, or community engagement to raise awareness and preparedness could be intensified in the area (Johnson, 2021).

Moreover, decision-making extended beyond immediate tactical responses and encompassed long-term strategic planning. Insights from event prediction models shaped broader counterterrorism strategies, including funding community resilience programmes,

enhancing infrastructure to support security efforts, and developing policies to address the underlying causes of terrorism (Anderson, 2020).

Ultimately, integrating event prediction with decision-making ensured a proactive approach to terrorism. Anticipating threats and making informed decisions enabled authorities to safeguard vulnerable populations, reduce the frequency and severity of attacks, and strengthen the overall security landscape of Mandera County.

3.10 Testing and Validation

Ensuring the effectiveness and reliability of the VA framework was of paramount importance. This process was systematically executed to assess the usability, functionality, performance, and alignment of the framework with real-world counterterrorism scenarios. It began with rigorous data validation to guarantee the quality of data integrated from multiple sources, including the GTD, ACLED, and the CVE Research Hub Observatory. Validation encompassed accuracy, completeness, and consistency checks, removing duplicates, correcting inconsistencies, and standardising location names to ensure the dataset accurately reflected conditions in Mandera County.

In addition to data validation, the predictive models embedded in the framework were extensively tested for robustness and generalisability. Techniques such as k-fold cross-validation were employed to evaluate model performance across data subsets, providing a reliable assessment of their predictive capacity. Models were assessed using metrics including accuracy, precision, recall, F1-score, and area under the curve (AUC). The evaluation process also involved hyperparameter tuning, followed by re-evaluation to optimise model performance.

Geographic components of the framework were validated to ensure spatial accuracy and reliability in geospatial analysis. Geographic coordinates were cross-referenced against official

boundary maps, while spatial joins and transformations were checked for consistency. These outputs were further verified by comparison with historical records and literature, ensuring that the spatial distribution of incidents was accurately captured.

Usability testing, targeting key end-users such as security personnel, policymakers, and analysts, was undertaken to evaluate the clarity of visualisations, navigability, and overall user experience. Feedback gathered during task-specific usability sessions, such as hotspot identification and trend analysis, was used to refine and enhance the interface.

Scenario-based testing was conducted to examine the framework's performance under simulated conditions modelled on historical and plausible future events. This process tested the framework's ability to deliver timely predictions and decision support, while also revealing areas that require further refinement.

Finally, the framework was validated against established ground truth data and expert interpretations. Discrepancies were analysed and addressed through iterative updates to the underlying algorithms and processing pipelines, thereby ensuring maximum possible accuracy and reliability.

Through this comprehensive validation approach, the study ensured the framework serves as a robust and dependable instrument for terrorism analysis in Mandera County, enhancing security operations and supporting informed decision-making in Kenya's counterterrorism strategy.

3.11 Ethical Considerations

Ethical considerations were paramount in this research due to the sensitive nature of terrorism-related data. The study prioritised the responsible handling of information, ensuring privacy protection and minimising potential harm to individuals and communities. Personal identifying information (PII) was anonymised or excluded where possible, in strict adherence to data protection regulations. Only data from reputable sources that complied with ethical standards for collection and sharing were utilised. For participants involved in primary data collection, informed consent was obtained following comprehensive briefings. Participants were made aware of the study's aims, their rights, and their right to withdraw at any time without penalty or negative consequences.

Efforts were undertaken to minimise potential harms, including the risk of stigmatisation or the unfair targeting of specific groups or regions. The analysis and presentation of findings were conducted responsibly to avoid inciting fear, discrimination, or other unintended outcomes. The study avoided speculative conclusions or predictions that could be misused or misinterpreted in harmful ways. This approach ensured that findings upheld the integrity of the data and were framed with sensitivity to their implications for policy and practice.

Transparency and research integrity were central throughout the research process. Methodologies, data sources, and analytical procedures were comprehensively documented to enable replication and verification by other researchers. The study acknowledged its limitations and potential biases to support accurate interpretation of the results. It adhered to institutional and ethical guidelines, received formal approval before data collection, and maintained ethical oversight throughout the project. These measures ensured the research was conducted with academic rigour and a strong commitment to ethical responsibility and societal well-being.

3.12 Limitations

Diligent acknowledgement and mitigation of potential limitations are essential in any research endeavour to safeguard the validity, generalisability, and interpretive strength of a study's outcomes. While this study offers valuable insights into the dynamics of terrorism in Mandera County and introduces a robust VA framework, several limitations may have affected the scope, precision, and overall reliability of its findings. These limitations also identify avenues for future research enhancement.

One of the primary limitations concerned the availability and quality of data. Although datasets such as GTD, ACLED, and the CVE Research Hub were relatively comprehensive, they exhibited limitations in granularity and completeness. Some incidents may have been underreported or lacked critical detail, owing to the inherent challenges of data collection in conflict-affected regions. Furthermore, reliance on secondary sources introduced dependency on the accuracy and integrity of third-party data, potentially resulting in biases or errors beyond the researchers' control.

The geospatial analysis encountered challenges relating to the precision of geographic coordinates and administrative boundary data. Discrepancies in place names and inconsistencies in coordinates complicated the mapping of events. Despite efforts to standardise spatial data, inaccuracies may have affected the precision of visualisations and the reliability of the insights derived from spatial patterns.

Temporal constraints also affected the study. Although the dataset spanned the period from 2013 to 2023, providing a decadal overview, it did not capture longer-term historical trends and may lack the depth necessary for broader temporal generalisations. In addition, the temporal resolution, often limited to annual or monthly intervals, may have obscured short-term fluctuations and event clustering.

The predictive modelling was based on historical data, operating under the assumption that past patterns are indicative of future occurrences. However, terrorism is a multifaceted phenomenon influenced by dynamic political, social, and economic conditions that can shift rapidly and unpredictably. As such, the predictive accuracy of the models may be constrained. There also exists a risk of overfitting, where the models perform well on existing data but generalise poorly to novel or evolving scenarios.

Ethical and practical considerations further shaped the scope of the study. Ethical responsibilities related to privacy protection and harm prevention restrict in-depth data collection in sensitive domains. Practical constraints, such as limited academic time and institutional resources, also impacted the breadth and depth of analysis.

Lastly, the analytical framework relied heavily on specific technologies, including Python, Jupyter Notebook, and Folium. While these tools enabled complex visualisation and modelling, they also introduced limitations related to computational resources and software capabilities. The effective use of these tools required a high level of technical expertise, which may have affected the efficiency and scalability of the analysis process.

Despite these limitations, the study makes a meaningful contribution to understanding terrorism in Mandera County and introduces a practical VA framework with potential for future application. However, it is essential to consider these constraints when evaluating the study's findings. Future research should seek to address these gaps by integrating more granular and diverse datasets, broadening both the temporal and geographical scope, and enhancing predictive models to more accurately capture the complexity and volatility characteristic of terrorism dynamics.

3.13 Summary

Chapter 3 outlined the methodological approach employed to analyse terrorism in Mandera County, encompassing data pre-processing, exploratory analysis, predictive modelling, decision support, and validation. The process commenced with data cleaning, dimensionality reduction, and the integration of datasets from established sources, which include the GTD, ACLED, and the CVE Research Hub. This resulted in a unified dataset comprising 335 recorded incidents spanning the period from 2013 to 2023. Geospatial transformation enabled visualisation of incident distributions across Mandera's Sub-Counties, while EDA used various visualisations to reveal spatial and temporal patterns. Predictive models, including logistic regression and random forests, were applied to forecast future attacks, shifting the approach from reactive to predictive. These insights informed counterterrorism decision-making, including the strategic allocation of resources and the development of community-based intervention strategies. Validation procedures were conducted to assess the reliability and robustness of the proposed framework, with particular emphasis on predictive accuracy and practical applicability.

CHAPTER FOUR

FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents the analysis and findings derived from the novel VA Framework designed to monitor and predict terrorist activities, with Mandera County serving as a case study. The framework was developed to uncover spatial and temporal patterns in terrorism-related data by integrating multiple analytical techniques, including outlier detection, clustering, association rule mining, and predictive modelling. Together, these methods enable a comprehensive analysis of terrorism data by identifying hotspots, revealing underlying trends, detecting anomalies, and forecasting potential threats. This chapter demonstrates how each component of the framework contributes to a deeper understanding of terrorism-related incidents and explains how these insights can be used to inform and enhance counterterrorism strategies.

4.2 Data Collection and Clean-up

The process of data collection involved a multifaceted approach, integrating information from both structured and unstructured sources. These sources included established datasets such as the GTD, ACLED and CVE Research Hub, complemented with unstructured data obtained from social media platforms and various online repositories. While gathering data from diverse sources enhances the overall accuracy, consistency, and reliability of the dataset, it also underscores the importance of having a unified schema, a structured dataset blueprint, that facilitates the effective merging and analysis of disparate data based on specific analytical requirements.

Given that databases such as GTD and ACLED often classify and label their data using different conventions, the unified schema played a critical role in reconciling these discrepancies. It did so by mapping diverse terminologies, formats, and structures into consistent fields and values. This standardisation allowed for the integration of multiple sources

into a single, coherent dataset while preserving the integrity and contextual richness of the original information. In the context of this study, a unified schema will enable the seamless incorporation of terrorism-related data from a variety of sources, supporting a comprehensive analysis of terrorism patterns of interest to experts. Furthermore, the schema improved the efficiency of data exchange and collaboration among relevant organisations and security agencies in Kenya, aligning the dataset with the needs of analysts working on counterterrorism efforts.

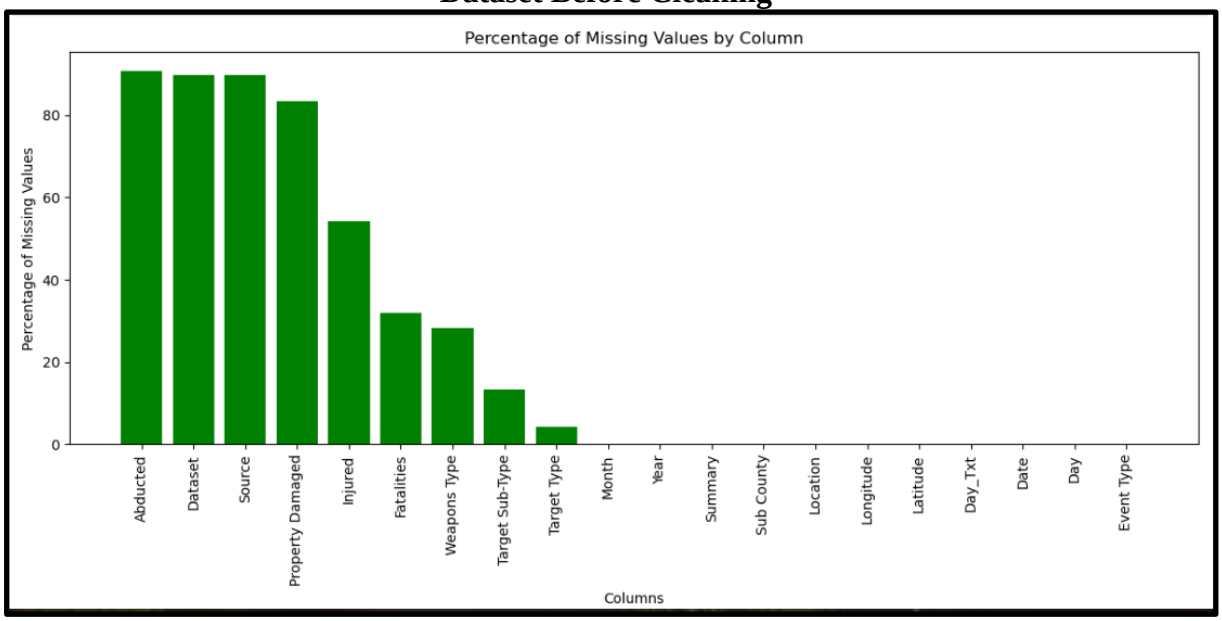
FIGURE 4.1
General Information of the Dataset after Collection

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 335 entries, 0 to 334
Data columns (total 20 columns):
 #   Column            Non-Null Count  Dtype
---  ------            --------------  -----
 0   Year              335 non-null    int64
 1   Month             335 non-null    int64
 2   Day               335 non-null    int64
 3   Date              335 non-null    object
 4   Day_Txt           335 non-null    object
 5   Latitude          335 non-null    float64
 6   Longitude         335 non-null    float64
 7   Location          335 non-null    object
 8   Sub County        335 non-null    object
 9   Summary           335 non-null    object
 10  Event Type        335 non-null    object
 11  Weapons Type      240 non-null    object
 12  Target Type       321 non-null    object
 13  Target Sub-Type   290 non-null    object
 14  Injured           153 non-null    object
 15  Fatalities        228 non-null    object
 16  Abducted          31 non-null     float64
 17  Property Damaged  56 non-null     object
 18  Source            34 non-null     object
 19  Dataset           34 non-null     object
dtypes: float64(3), int64(3), object(14)
memory usage: 52.5+ KB
```

Data cleaning was essential to ensure the reliability and analytical readiness of the integrated dataset. Rigorous cleaning procedures were applied to address common inconsistencies, including duplicate entries, missing values, and variations in location names referring to the same geographic areas. For example, discrepancies in how locations were recorded, such as ‘Mandera East County’ in one source and ‘Mandera E County’ in another,

were resolved through careful standardisation. This step was crucial in preventing errors and analytical biases that could distort results. The data cleaning process thus enhanced the validity and consistency of the findings generated through the VA framework. This phase allows diverse, real-world data to be integrated under a unified schema, enriching the analysis of terrorism and expanding the scope of the study, enabling deeper and more comprehensive insights into terrorism dynamics.

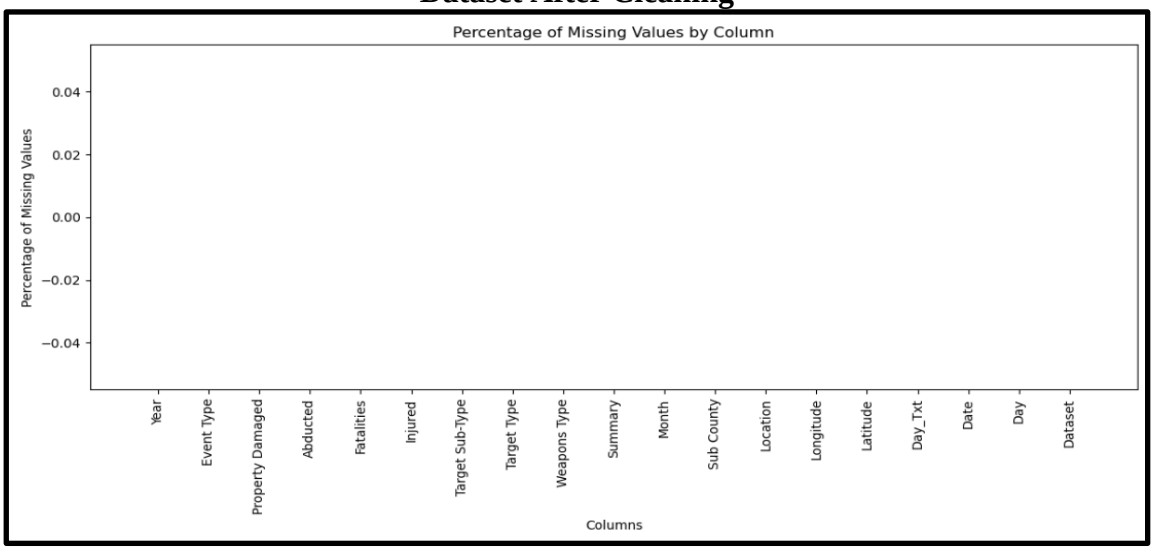
FIGURE 4.2
Dataset Before Cleaning



Missing values posed a significant challenge, primarily caused by incomplete reporting across various sources and the general scarcity of comprehensive terrorism datasets in Kenya. The study addressed these gaps using additional sources such as online news reports, social networks, primarily X (formerly Twitter), and security bulletins. When no supplementary data were available, a careful strategy was employed to maintain the integrity and analytical value of the dataset. For categorical fields such as ‘Weapons Type’, ‘Target Type’, and ‘Target Sub-Type’, missing values were labelled as ‘Unknown’, thereby signalling data gaps while preserving context. This method supported data standardisation and enhanced manageability for subsequent analysis.

In cases where the ‘Property Damaged’ field had missing values, the label ‘No’ was used as a substitute, indicating that no damage was captured. These data handling strategies made it possible to construct a consistent and coherent dataset, even in the presence of missing or incomplete information. This approach enhances the accuracy and reliability of the data, ensuring that the VA framework can deliver meaningful insights. This strategy was essential to the study, allowing for the use of real-world, often imperfect data while still producing reliable analyses of terrorism dynamics in Mandera County. Thoughtful management of missing values was essential to preserving the analytical utility of the dataset and ensuring the generation of findings that can support more effective and informed counterterrorism measures.

FIGURE 4.3
Dataset After Cleaning



4.3 Exploratory Data Analytics (EDA)

EDA was pivotal in establishing a foundation for understanding the dataset's structure, distribution, and internal relationships. It enabled analysis of the dataset, revealing underlying patterns and trends, and generating insights essential for informed decision-making (Jebb et al., 2017). In this study, EDA was applied to terrorism-related data from Mandera County, spanning the period from 2013 to 2023, to examine the dynamics of terrorist activity in the region. The ten-year dataset provided a robust basis for analysis, capturing periods of heightened activity, temporal fluctuations, and changes in the methods and tactics employed in terrorist incidents.

4.3.1 Descriptive statistics and temporal trends

A comprehensive descriptive analysis was conducted to examine the patterns and impacts of terrorist attacks in Mandera County. The analysis aimed to uncover key insights into the frequency, distribution, and severity of incidents. Descriptive statistics offered an overview of critical variables, such as fatalities, injuries, and abductions, revealing significant variability in the scale and consequences of individual events. Analysing the frequency of event types, weapons used, and targeted locations provided a clearer understanding of the predominant forms of violence and their most common targets. Correlation analysis of impact metrics, such as fatalities and injuries, highlighted relationships between variables and offered deeper insight into the nature and intensity of attacks.

The descriptive findings revealed a complex and volatile security environment in Mandera County, characterised by significant variation in the frequency, impact, and geographic spread of terrorist incidents. While many events resulted in no casualties, others led to severe consequences, underscoring the unpredictable nature of the threat. Although the average number of fatalities per event was relatively low (2.32), some incidents resulted in as many as 38 deaths, reflecting the high-risk context. Similarly, injuries and abductions followed

a comparable pattern, with most attacks causing limited harm, but a few high-impact incidents resulting in up to 11 injuries and 22 abductions in a single event. This variability in outcomes underscores the need for adaptable counterterrorism measures that can effectively address both low and high-impact scenarios.

TABLE 4.1
Descriptive Statistics

	count	mean	std	min	25%	50%	75%	max
Fatalities	74.0	2.324324	5.898939	0.0000	0.0000	0.0000	2.0000	38.0000
Injured	74.0	0.918919	2.032319	0.0000	0.0000	0.0000	1.0000	11.0000
Abducted	74.0	0.337838	2.565723	0.0000	0.0000	0.0000	0.0000	22.0000
Latitude	74.0	3.922076	0.093943	3.1508	3.9357	3.9357	3.9387	3.9661
Longitude	74.0	41.839042	0.081200	41.1862	41.8447	41.8542	41.8542	41.8945

The analysis of temporal trends provides essential context for understanding how terrorism dynamics have changed over the past decade. The dataset illustrates a fluctuating pattern of terrorist activity between 2013 and 2023, with certain years exhibiting pronounced spikes in violence.

FIGURE 4.4
Temporal Trends of Terror Attacks

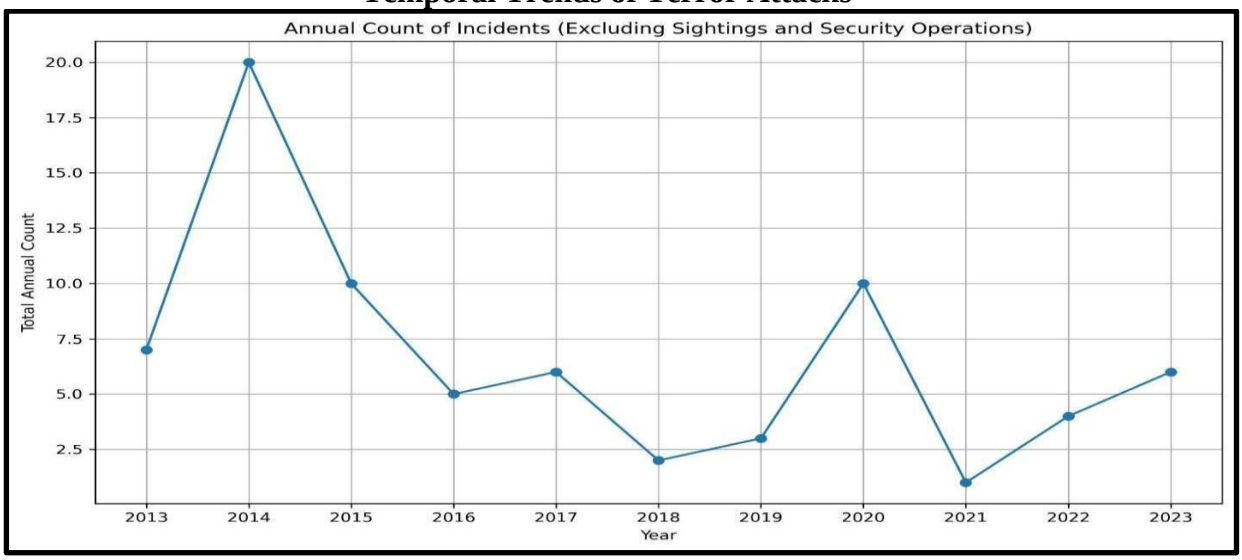
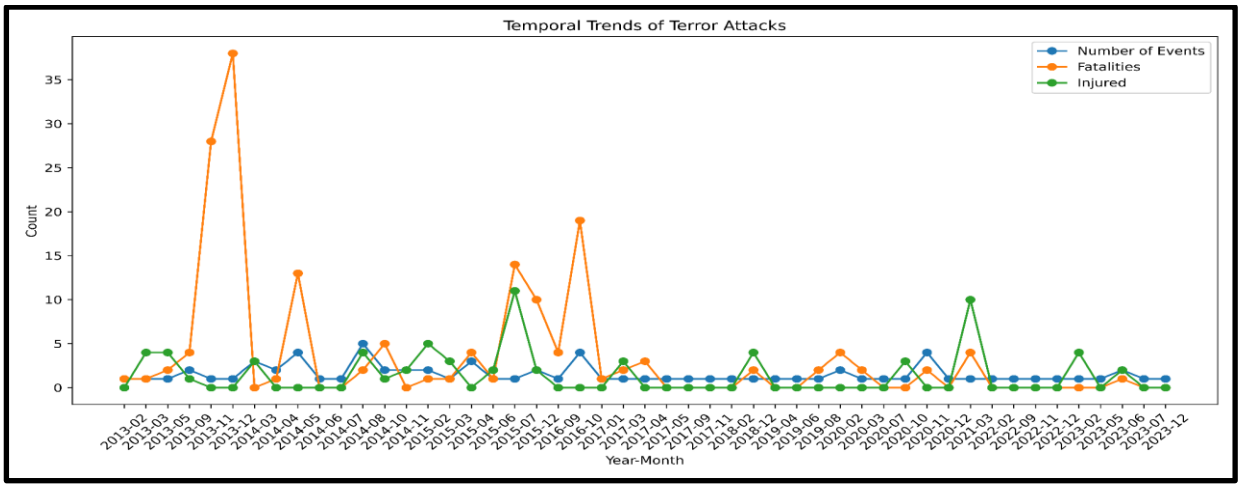


FIGURE 4.5
Annual Trend of Terror Attacks



Annual incident counts show a sharp peak in attacks occurred in 2014, with 20 recorded attacks, a period likely influenced by broader regional instability, including cross-border terrorism and the activities of extremist groups in neighbouring Somalia. This was followed by a decline in incidents between 2015 and 2017, potentially reflecting the effects of intensified counterterrorism interventions. However, a resurgence occurred in 2020, coinciding with global disruptions caused by the COVID-19 pandemic, which may have weakened law enforcement operations and created opportunities for terrorist activity. Around 2021 and 2023, a gradual rise in attacks was observed, potentially linked to political uncertainty surrounding the 2022 general elections.

Beyond overall attack frequency, temporal patterns in casualties provide a more nuanced picture. In December 2013, for example, over 35 fatalities were recorded in a single month, likely due to a particularly lethal incident. While the median number of deaths from attacks across the dataset is zero, indicating that most incidents do not result in fatalities, a significant minority involve multiple casualties. Injuries follow a similar pattern, with most incidents resulting in no harm, yet a small subset causing significant physical damage.

Abductions were rare in most cases, as confirmed by 25th, 50th, and 75th percentiles all registering zero, yet outliers involved up to 22 individuals abducted in a single event.

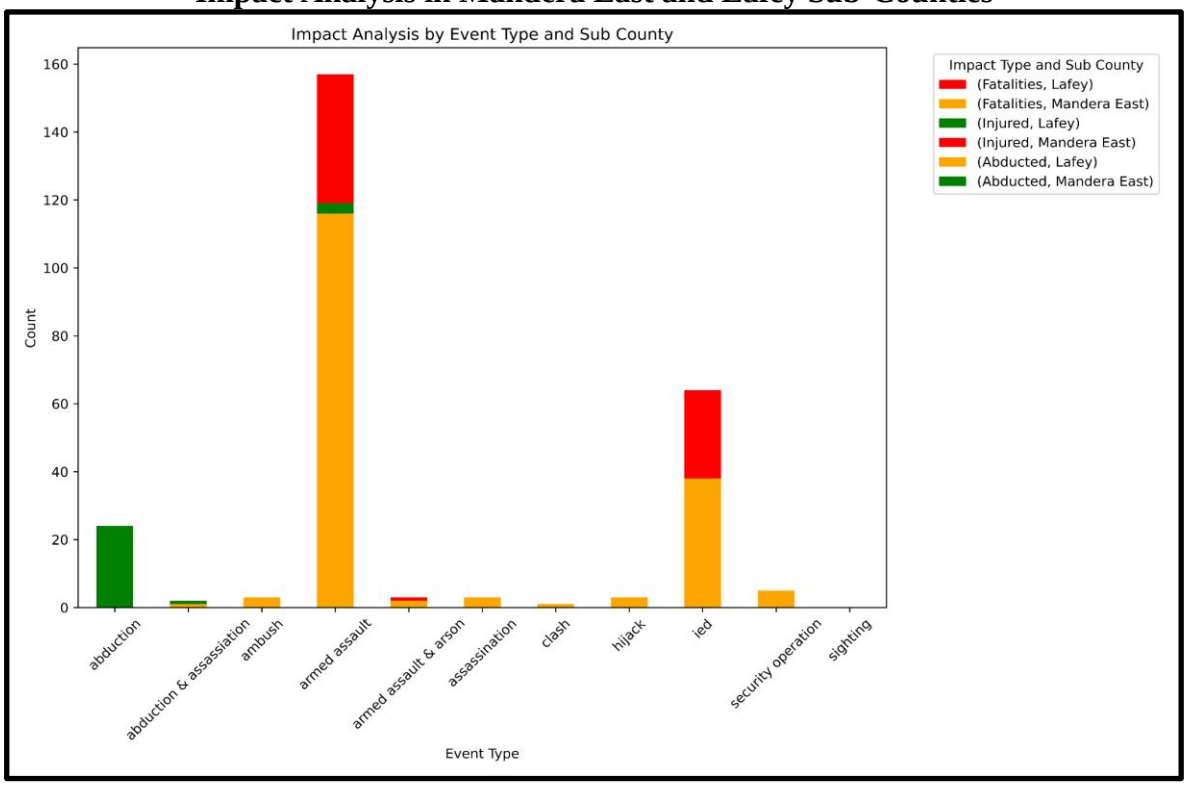
Spatial analysis further supports these insights. The geospatial data showed a narrow range of latitude and longitude values, indicating that incidents were geographically concentrated in specific areas of Mandera County. These clusters, particularly near the Somalia border and around Mandera town, align with historically high-risk zones. The relatively small standard deviations for both coordinates reinforce this spatial concentration and justify the prioritisation of security resources in these zones. Although summary statistics do not fully capture temporal volatility, the observed patterns suggest fluctuating activity across time, highlighting the importance of understanding when and where risks intensify.

In conclusion, the descriptive and temporal analyses, supported by insights from the literature review, provide a strong foundation for developing a VA framework tailored to the unique counterterrorism challenges in Mandera County. Capturing the variability, spatial concentration, and temporal shifts of terrorist activity enables the framework to generate precise and timely insights, supporting more effective evidence-based interventions and policy decisions.

4.3.2 Impact analysis

Mandera East and Lafey Sub-Counties recorded the highest number of terrorist incidents in Mandera County, with 116 and 64 events, respectively. These figures establish them as significant hotspots for AS activities. However, the nature and intensity of violence differ markedly between the two areas, reflecting divergent operational strategies by armed groups. Mandera East Sub-County experienced significantly higher intensity across various categories of attacks, while Lafey Sub-County displays a more targeted form of insecurity. This disparity, illustrated in Figure 4.6, has profound implications for local communities, influencing both physical safety and long-term socio-economic development.

FIGURE 4.6
Impact Analysis in Mandera East and Lafey Sub-Counties



In Mandera East Sub-County, the severity of violence is particularly pronounced, especially through armed assaults and improvised IED attacks. Armed assaults alone resulted in over 140 fatalities and 48 injuries, making them the deadliest form of attack in the region. IED incidents have also contributed substantially, with 60 fatalities and 78 injuries recorded.

These attacks have inflicted considerable human suffering, causing trauma and grief among affected families while exposing the broader community to a persistent threat. The sustained danger contributes to long-term psychological consequences, including chronic stress, fear, and diminished community well-being.

The frequent occurrence of such violent incidents has disrupted social cohesion and severely impeded economic activity in Mandera East Sub-County. Local businesses are often destroyed, leading to the loss of livelihoods, and the displacement of families is common due to the instability. The pervasive insecurity deters investment and development efforts, reinforcing cycles of poverty and underdevelopment. Public services, including education and healthcare, as well as critical infrastructure, are frequently interrupted, further exacerbating the Sub-County's vulnerability.

The high volume of violent events also places considerable strain on already overstretched local security and emergency response systems. The frequency and unpredictability of attacks undermine consistent service delivery and contribute to a persistent sense of vulnerability among residents. This situation erodes public trust in governmental and security institutions, weakening the overall stability of the region.

In contrast, Lafey Sub-County presents a different pattern of violence. While it experiences relatively fewer incidents of armed assaults and IED attacks, it has recorded 24 abduction cases, compared to none in Mandera East Sub-County. This indicates a distinct security challenge in Lafey Sub-County, where abductions appear to be a tactic preferred by AS operatives.

The prevalence of abductions in Lafey Sub-County suggests a targeted approach, often aimed at extracting ransom or exerting control over the local population. Although the total number of fatalities and injuries is lower than in Mandera East Sub-County, the psychological

and social repercussions are considerable. Abductions instil a pervasive sense of fear and insecurity, disrupt daily life, and reduce the population's sense of safety.

Families of abducted individuals suffer significant emotional trauma, long-term anxiety, and financial hardship. Social isolation is common, as community members withdraw from public activities out of fear. The persistent threat of abductions undermines community trust and weakens social networks. The lack of timely and effective security responses further compounds this fear, leaving residents feeling exposed and unsupported. While Lafey Sub-County experienced lower levels of direct violence, the strategic use of abductions remains a serious security concern.

The clear contrast between demonstrates that AS adapts its tactics to local conditions. In Mandera East Sub-County, they prioritise high-impact, high-fatality attacks, while in Lafey Sub-County, they employ abductions as a form of psychological warfare. These distinct threat profiles demand tailored, context-specific security interventions. For instance, Mandera East Sub-County requires strengthened rapid response mechanisms, improved intelligence gathering, and the deployment of counter-IED capabilities. In Lafey Sub-County, the focus should be on community-based surveillance, abduction-prevention strategies, and resilience-building programmes to restore public trust and cohesion.

4.3.3 Comparative analysis

A comparison of violent incidents in Mandera East and Lafey Sub-Counties underscores the varying security dynamics within Mandera County. Mandera East Sub-County faces a broader range of violent incidents, such as armed assaults and IED attacks, which severely impact community safety, infrastructure, and essential public services. In contrast, Lafey Sub-County, while experiencing fewer forms of violence overall, struggles with a high prevalence of abductions. This creates unique challenges for local security operations and community well-being, as abductions foster widespread fear and weaken social bonds.

The scale and nature of violence in each Sub-County have profound implications for the local population. In Mandera East Sub-County, the high casualty rates and frequent disruptions displace families, destabilise local economies, and stretch emergency services to their limits. Meanwhile, in Lafey Sub-County, targeted abductions, while resulting in fewer casualties, inflict deep psychological harm, contribute to social isolation, and undermine community trust.

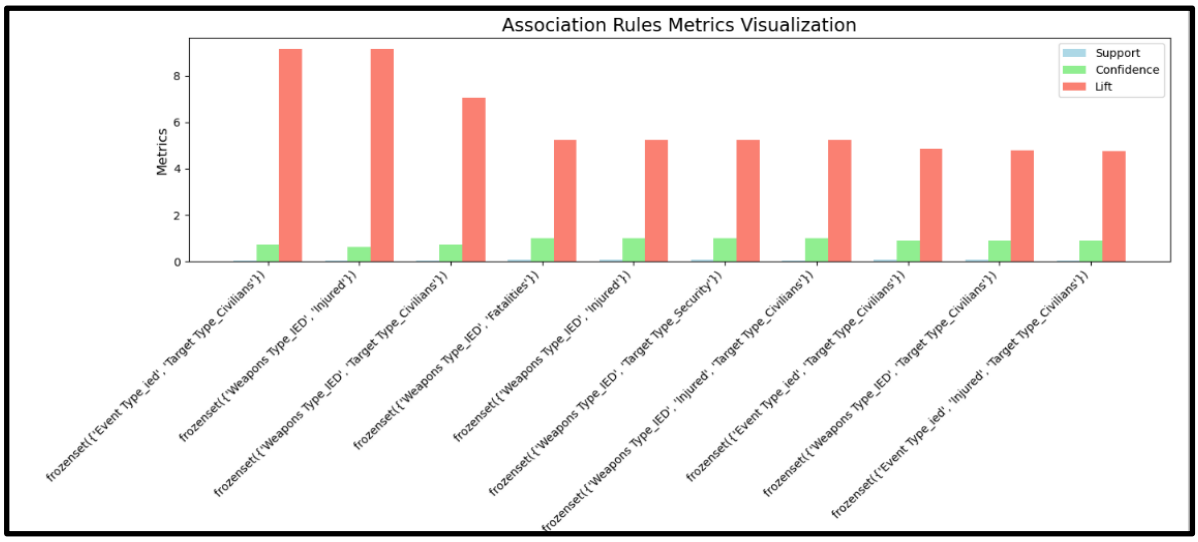
The EDA process revealed several critical insights into the nature of AS activities in Mandera County. Terrorist activities were not uniformly distributed over time but were concentrated around specific periods, often coinciding with political events or periods of heightened socio-economic stress. Spatial analysis reveals that certain locations are consistently targeted, suggesting operational or logistical advantages for militant groups. Furthermore, the link between socioeconomic factors, particularly poverty and unemployment, and increased vulnerability to radicalisation in these areas demonstrates the importance of addressing these root causes alongside robust security measures. These findings highlight the importance of adopting an integrated counterterrorism approach that not only reinforces

security operations but also tackles the root socio-economic conditions contributing to instability, to promote sustained resilience within Mandera County.

4.3.4 Association analysis

This study employed association analysis to reveal significant relationships among event types, weapon usage, and target categories in terrorist incidents within Mandera County. Using the Apriori algorithm, the analysis generated association rules that expose key patterns in how attacks unfold, who they target, and the expected consequences. These findings deepen understanding of the factors driving terror-related incidents and guide strategic decisions to improve prevention and response. The support, confidence, and lift metrics quantify these associations, providing a clear measure of their strength and relevance. Figure 4.7 visualises these metrics, enabling a clear comparison of the relationships uncovered by the analysis.

FIGURE 4.7
Visualisation of Association Rules Metrics



The association rules revealed several notable findings. One of the most significant observations is the strong correlation between IED attacks targeting civilians and the likelihood of injuries. The confidence level for this rule is 73.9%, with a high lift value of 9.17, indicating that such attacks are not only prevalent but are also highly likely to result in injuries. The high lift value suggests that this relationship is far stronger than would be expected by random

chance, underscoring the need for targeted interventions to mitigate the risks posed by these attacks.

Moreover, the analysis revealed a strong association between IED attacks and fatalities, particularly when civilians are the primary targets. The confidence and lift metrics for this association highlight the deadly nature of such attacks, with fatalities being a frequent outcome of these incidents. Similarly, rules linking IEDs to fatalities and IED attacks aimed at security forces also display notable lift values above 5, underscoring the consistent lethality of IEDs regardless of the target. These elevated lift values make clear that IEDs pose an outsized threat whenever deployed, and therefore demand targeted countermeasures.

The patterns identified through association analysis demonstrate the critical importance of focusing security efforts on areas prone to IED attacks, especially those targeting civilians. These insights suggest that focused intervention strategies are essential. Raising community awareness, expanding early warning systems, and improving local reporting mechanisms are all crucial steps to lowering civilian exposure. Meanwhile, investments in counter-IED capabilities, especially in high-risk civilian zones, can reduce the likelihood of both injuries and fatalities.

Association analysis, which quantifies the links between event types, weapons, and targets, provides critical evidence to guide security priorities and resource allocation. In Mandera County, where IED attacks continue to pose a major threat, these insights should inform tactical deployments, community awareness, and policy measures to better safeguard vulnerable populations.

4.4 Objective One Results

Counterterrorism efforts in Kenya, and especially in regions like Mandera County, continue to face complex obstacles that limit their effectiveness. As an area frequently targeted by the AS terrorist organisation, it is essential to identify and address these barriers to strengthen security and stability in the County.

This study conducted a systematic analysis of the main challenges that hinder the success of counterterrorism initiatives. An extensive review of existing data, including government reports, NGO case studies, scholarly research, and credible media sources, provided a clear picture of the scale and persistence of terrorism-related threats in Kenya.

In particular, secondary data drawn from key sources such as the GTD, Africa Center for Strategic Studies (ACSS), and ACLED offered valuable insights into the frequency, nature, and geographic patterns of terrorist incidents. These sources consistently highlight how persistent insecurity, porous borders, limited local intelligence networks, and community-level socio-economic vulnerabilities continue to undermine counterterrorism operations in high-risk regions like Mandera County. Together, this evidence establishes a clear understanding of the factors that limit the effectiveness of current counterterrorism measures, emphasising the need for targeted, locally relevant interventions to address Mandera County's unique security challenges

4.4.1 Distribution of terror events

FIGURE 4.8
Distribution of Terror Events by Type

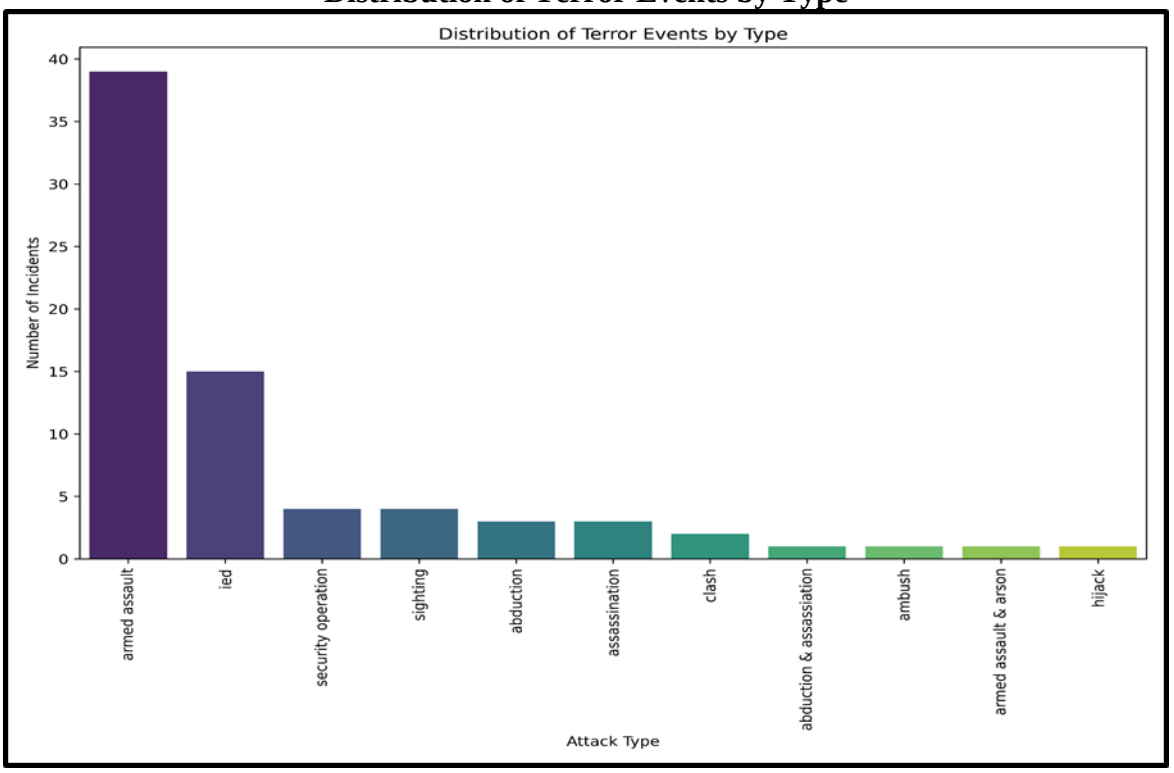


Figure 4.8 illustrates the distribution of terror events by type in Mandera County. Armed assaults are the most prevalent attack type, accounting for approximately 39 incidents, followed by IED attacks with around 15 incidents. Other types of events, including abductions, assassinations, ambushes, and hijackings, occur less frequently but still pose significant threats within Mandera County's broader security environment. The concentration of armed assaults and IED attacks demonstrates the tactical preference of terrorist groups operating in the region for high-casualty, high-impact methods designed to instil fear, disrupt civilian life, and undermine government authority.

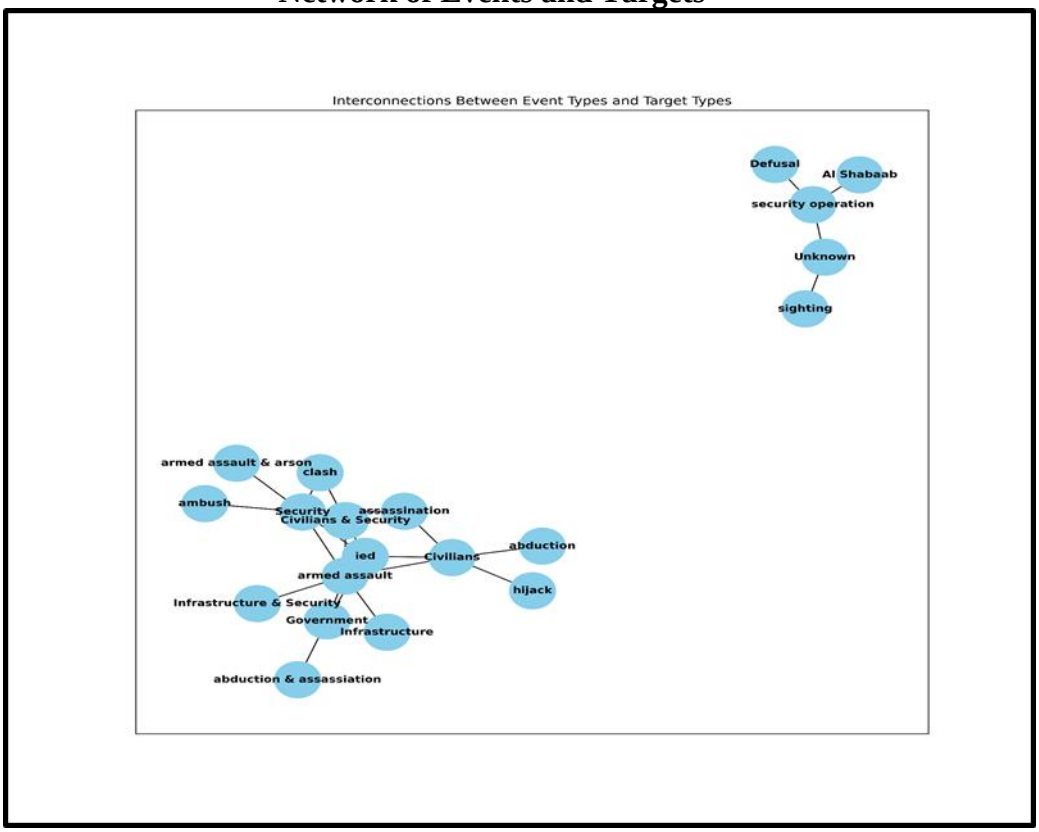
Notably, the chart also shows lower reported frequencies for sightings and security operations, which may not accurately reflect the true scale of these activities. As highlighted in Chapter Two, sightings of AS operatives are a known precursor to terror attacks, while security operations indicate progress in countering AS in the County. Such events are often

under-reported due to limited local surveillance, fear of reprisals, and logistical challenges in data collection in remote areas. This under-reporting can hinder early warning systems and reduce the responsiveness of counterterrorism interventions that rely on timely intelligence.

Additionally, AS frequently compounds and coordinates attacks in Mandera County. In practice, IED explosions are often combined with armed ambushes targeting first responders or security convoys, amplifying the impact of a single event. Such layered tactics increase casualties and strain already limited security resources. This represents a key barrier to effective counterterrorism highlighted by this study. Overall, Figure 4.8 demonstrates that understanding the distribution of different attack types and recognising the under-reporting of critical precursor activities is vital for designing effective early warning systems and intelligence-led counterterrorism responses.

4.4.2 Network diagram of event types and target types

FIGURE 4.9
Network of Events and Targets



The above figure illustrates the interconnections between various event types and target types associated with terrorist activities in Mandera County. It provides a clearer visual summary of how different tactics and targets are interrelated, reflecting the operational strategies of AS in the region.

The diagram highlights that abductions continue to be a significant threat, especially targeting civilians and occasionally government personnel. These incidents, common in Mandera East Sub-County and other remote areas, underscore the vulnerability of border communities where security infrastructure is limited. Such abductions are designed to instil fear, disrupt daily life, and undermine public confidence in government protection.

Another key observation from the network diagram is the link between assassinations and government targets, demonstrating AS's ongoing strategy to destabilise local governance by eliminating officials and eroding state authority. This tactic deepens instability and hampers service delivery, leaving communities more isolated and insecure.

The frequent use of ambushes against security forces and armed assaults against civilians, security installations, and infrastructure points to AS's multipronged approach to weaken state presence. These attacks exploit difficult terrain and limited security patrols, enabling repeated strikes that drain security resources and morale.

The diagram also shows that arson attacks are closely associated with infrastructure attacks. The deliberate destruction of roads, communication lines, and facilities prolongs recovery efforts and disrupts the local economy, creating conditions that allow AS to maintain influence.

The use of IEDs, which often have unknown or mixed targets, adds further complexity. IEDs pose constant danger to both civilians and security forces, with their unpredictability

heightening fear and complicating counterterrorism efforts. The diagram also reflects proactive measures, with security operations linked to IED defusal, showing the critical role of bomb disposal and surveillance in preventing casualties.

Sightings of AS operatives, mapped here as linked to both AS and security operations, reveal a persistent militant presence and provide indicators of potential attacks. Although sightings do not always result in immediate violence, they might signal active cells in the area and justify continued counterinsurgency actions.

The hijacking of vehicles and goods, often with unspecified or opportunistic targets, further disrupts regional transport and supply chains, compounding the economic and security challenges faced by communities.

Overall, Figure 4.9 illustrates that the terrorist threat in Mandera County is sustained through a network of interlinked tactics, from abductions and assassinations to IEDs and hijackings, each exploiting vulnerability in civilian life, governance, and infrastructure. Addressing this threat requires not only robust security operations but also targeted efforts to strengthen community resilience, rebuild damaged infrastructure, and address socio-economic conditions that allow AS to operate.

4.4.3 Challenges impeding counterterrorism efforts in Kenya

A significant challenge impeding counterterrorism efforts in Kenya, particularly in Mandera County, is the limited allocation of resources. The frequency of armed assaults underscores the urgent need for a stronger security infrastructure. Despite the severity of these attacks, local law enforcement agencies remain under-resourced, lacking sufficient personnel, equipment, and protective gear, which limits their capacity to respond effectively. This shortage leaves both security forces and local communities exposed to repeated attacks by AS.

This problem is compounded by the County's vast and rugged terrain, which poses considerable logistical challenges in establishing and maintaining security outposts and government facilities. Poor transport and communication networks hinder swift responses to incidents, giving AS a tactical advantage as security forces are often forced into reactive strategies, dealing with the aftermath of attacks rather than preventing them. Additionally, the absence of paved roads facilitates the planting of IEDs, which terrorists exploit with relative impunity. The combination of challenging terrain and inadequate infrastructure intensifies the threat of IED attacks, underscoring the urgent need for enhanced security strategies and more effective resource allocation.

Intelligence gathering and analysis also present significant obstacles. The frequent occurrence of IED attacks illustrates the challenges of detecting and neutralising these types of threats before they materialise. IEDs have been noted to be employed in public areas, especially along unpaved roads in Mandera County, requiring advanced intelligence and surveillance capabilities to detect and disarm them safely. However, the intelligence apparatus in Kenya, particularly in remote counties such as Mandera, faces critical limitations, including a lack of real-time information and weak inter-agency communication.

Cultural factors further complicate intelligence efforts, as local populations may be hesitant to report suspicious activity due to fear of retaliation or a lack of trust in the

authorities. This creates critical security gaps that make it harder to prevent attacks. Moreover, the complexity of terrorist networks operating in the region, often linked to transnational organisations such as AQ and IS, adds another layer of difficulty, complicating efforts to predict and counter AS operations.

Poor coordination between security and intelligence agencies presents another serious challenge. The diversity of target types and tactics demands cooperation among multiple agencies, including the military, police, intelligence, financial and religious agencies. However, bureaucratic inefficiencies, overlapping mandates, and competition for resources often lead to fragmented efforts where vital information is not shared promptly or operations are poorly synchronised. During operations aimed at neutralising terrorist cells, poor coordination can result in missed opportunities or even incidents of friendly fire. The absence of a unified command structure and integrated communication systems exacerbates these weaknesses, reducing operational efficiency and undermining the overall effectiveness of counterterrorism efforts.

Building trust between security forces and local communities remains a persistent challenge in Mandera County. Events such as abductions and hijackings often involve local informants or collaborators who may be coerced or persuaded by terrorists. These incidents highlight the strained relationship between authorities and communities, where years of neglect, heavy-handed security operations, and perceived injustices have eroded public trust. Effective community engagement is crucial for gathering intelligence, preventing radicalisation, and building resilience against terrorism. Rebuilding this trust requires a sustained effort to improve the conduct of security operations and to address underlying socio-economic grievances. Community programmes providing education,

healthcare, and economic opportunities could help bridge the gap between the state and residents, fostering greater cooperation in counterterrorism efforts.

The legal and judicial systems in Kenya also present significant obstacles. Arresting and prosecuting suspected terrorists often involves numerous challenges, including insufficient evidence, procedural flaws, and delays within the judicial process. This is particularly problematic in complex cases such as armed assaults combined with arson or IED attacks linked to ambushes, where multiple charges and jurisdictions may be involved. Although Kenya's counterterrorism legal framework is robust in principle, its practical implementation has faced repeated criticism. Allegations of extrajudicial killings, unlawful detentions, and torture undermine the legitimacy of counterterrorism operations and risk further radicalising affected communities. An efficient and fair legal system that upholds human rights while ensuring swift justice for terrorists is vital to maintaining public confidence and support.

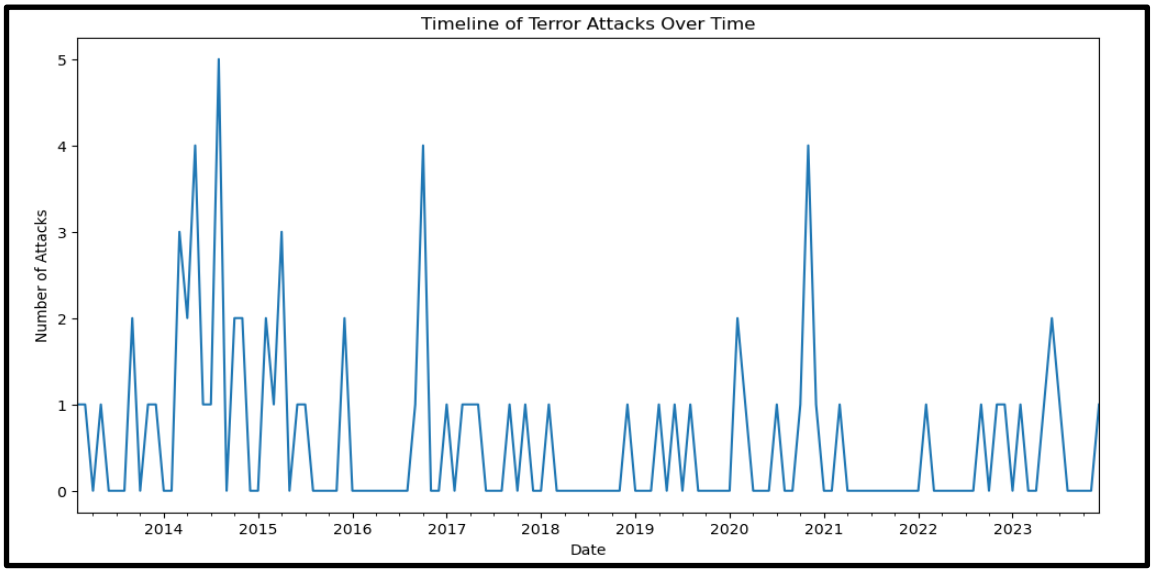
The network diagram reveals the interconnections within the Mandera County dataset, revealing how various events and targets are interwoven to create a complex security landscape that cannot be addressed in isolation. This underlines the need for a more integrated approach to counterterrorism, recognising the interrelated nature of these challenges and addressing them through coordinated action across sectors and stakeholders.

The evidence from Mandera County illustrates that the obstacles facing counterterrorism efforts in Kenya are multifaceted and deeply entrenched. Effectively addressing them requires a holistic approach that goes beyond military interventions. It demands strategic resource allocation, enhanced intelligence capabilities, stronger inter-agency coordination, meaningful community engagement, and a legal system that is both

fair and efficient. Kenya can strengthen its strategies to combat terrorism and better ensure the safety and security of its people by acknowledging and effectively managing these challenges.

4.5 Potential Indicators

FIGURE 4.10
Timeline of Attacks over Time



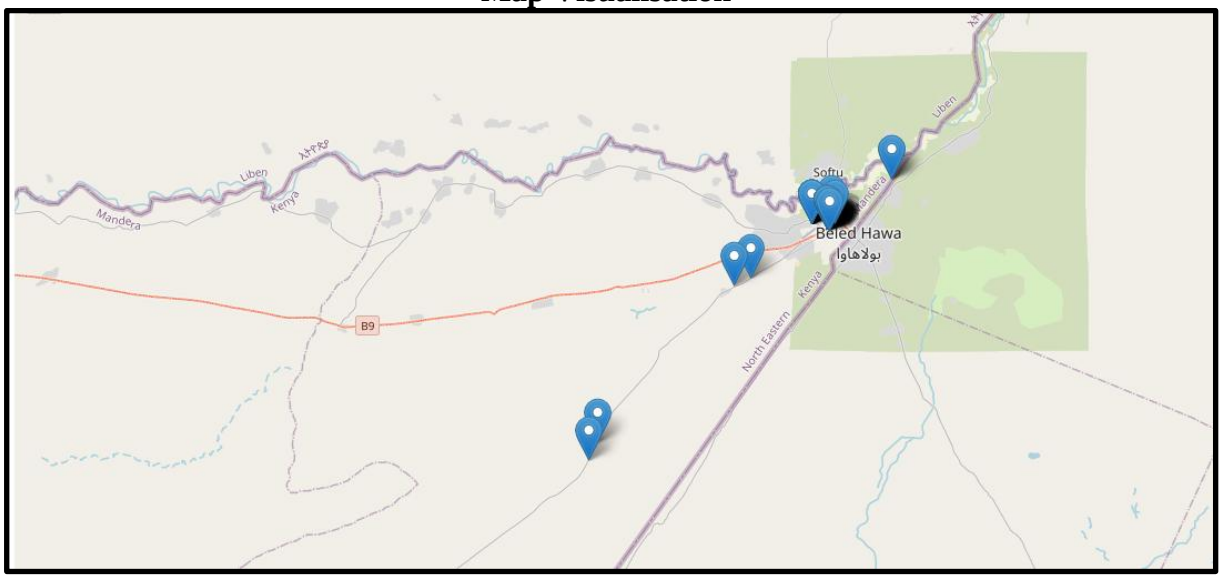
The temporal fluctuations illustrated in Figure 4.10 serve as a critical indicator of terrorist activity trends in Mandera County and can inform early-warning systems. The timeline reveals discernible peaks in attack frequency, most notably in mid-2014 and early 2015, suggesting periods of heightened operational momentum by AS, likely influenced by broader regional instability or strategic intent. These spikes offer insight into the group's mobilisation cycles and can be viewed as reactive or opportunistic responses to shifts in local governance, military deployments, or cross-border dynamics.

A secondary surge in late 2020 to early 2021 highlights another significant period of elevated threat, potentially driven by changing tactics or increased regional volatility. In contrast, the prolonged decline in attacks observed from mid-2017 through 2019, and again in parts of 2022, may reflect the temporary success of counterterrorism interventions or adaptive withdrawal by AS.

These alternating periods of escalation and decline can serve as valuable indicators when correlated with other data such as militant sightings, border activity, or political developments. A resurgence in attacks toward the end of 2023 further reinforces the utility of trend analysis in forecasting future threats. These upticks may signal the reorganisation of militant networks, a breakdown in local security measures, or renewed external support for insurgent operations.

Identifying and analysing these temporal shifts as early warning signals enables security agencies to anticipate emerging threats, allocate resources more efficiently, and implement preventive strategies. Therefore, the attack timeline is not only a record of historical events but also a forward-looking diagnostic tool, essential for proactive counterterrorism planning in Mandera County.

FIGURE 4.11
Map Visualisation



Map visualisations offer essential geographical insight into the distribution of terror events across Mandera County. The visual representation of attack locations enables the identification of spatial patterns, clearly pinpointing hotspots where terrorist activities are concentrated, particularly along the porous Kenya-Somalia border. These areas are especially vulnerable due to their proximity to known AS bases, which facilitate cross-border incursions.

The map also highlights zones that are repeatedly targeted by specific types of attacks, such as armed assaults or abductions. Over time, the spread of attack locations deeper into the County suggests an expansion of AS's operational reach, potentially exacerbated by surveillance gaps or lapses in security patrols. Recognising these hotspots is crucial for guiding the strategic allocation of security resources, ensuring that attention is directed to the most vulnerable regions. This type of spatial analysis is indispensable for understanding attack dynamics, supporting the implementation of proactive security strategies aimed at mitigating risks and protecting local populations.

FIGURE 4.12
Density Plot

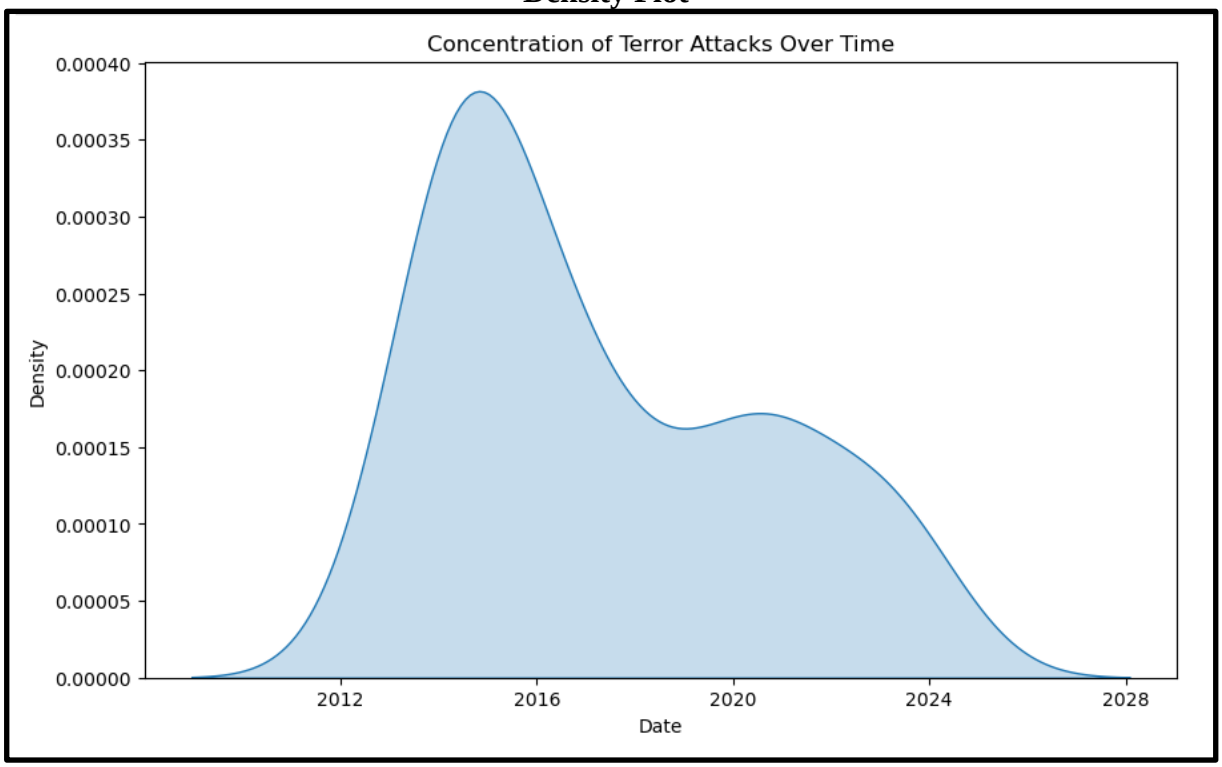


Figure 4.12 illustrates the temporal density of terror attacks in Mandera County, highlighting periods of heightened activity. The density curve highlights a pronounced peak between 2014 and 2016, indicating a period of sustained and intense terrorist operations, consistent with the timeline and map analyses. This high-density phase may reflect increased operational freedom by AS or gaps in security infrastructure during that period.

A secondary, less intense rise is observed around 2020-2021, signalling a resurgence of activity, potentially tied to renewed political instability or shifts in regional counterterrorism dynamics. The curve's tapering in recent years may suggest a decline in recorded attacks, although the uptick toward 2023 in earlier figures signals that the threat remains active and evolving.

This density-based visualisation complements the raw timeline by smoothing short-term fluctuations and revealing broader temporal patterns. It offers valuable insight for forecasting, strategic planning, and the optimisation of surveillance and response mechanisms during periods of elevated risk.

4.6 Aspects of Prediction in the Context of Terrorism Analysis

Prediction is a critical component of this study's analytical framework, enabling the anticipation of future terrorist activity. In high-risk regions such as Mandera County, where terrorism is a recurrent threat, forecasting when and where attacks may occur provides significant strategic advantages. It enhances the ability of decision-makers to allocate resources efficiently and implement preventive measures in a timely and targeted manner. This section outlines the key predictive approaches employed in this research, with a focus on the Random Forest Classifier, the AutoRegressive Integrated Moving Average (ARIMA) model, and other tools used to anticipate future incidents.

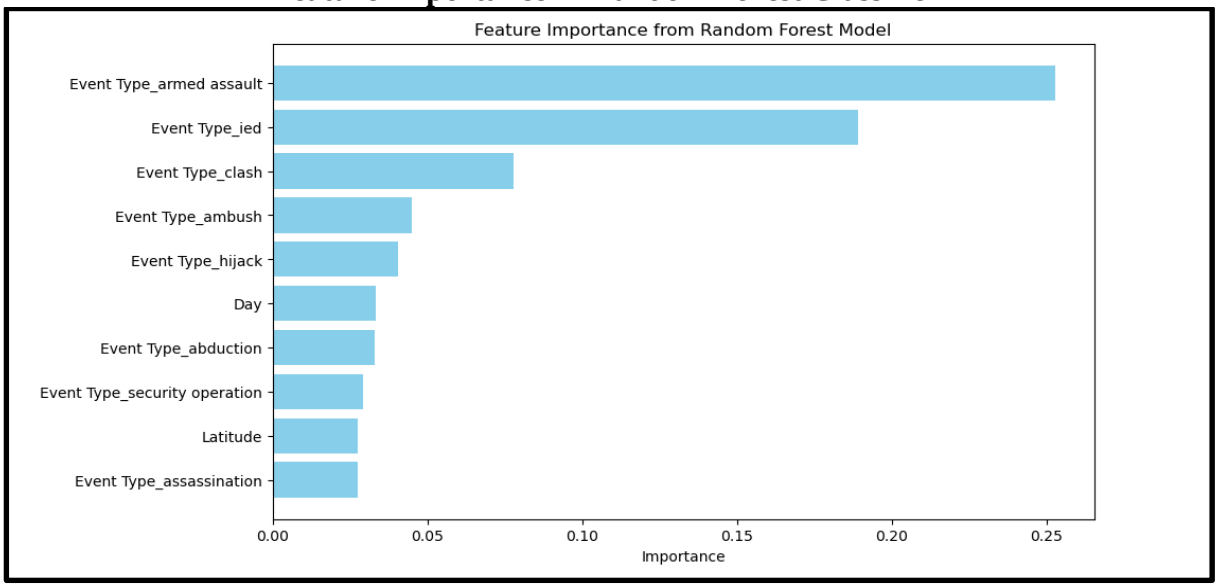
The Random Forest Classifier was employed to forecast both the location and type of terrorist attacks based on historical patterns. This ensemble method constructs multiple decision trees and aggregates their outputs to generate stable predictions. Its capacity to handle complex, non-linear relationships makes it particularly suitable for analysing terrorism-related data. Within this study, event types such as armed assaults and IED attacks emerged as strong predictors. The model successfully recognised patterns from past incidents, which informed its

estimations regarding the likelihood of specific types of events occurring under similar conditions.

Geospatial variables, including coordinates and Sub-County identifiers, played an essential role in enabling the model to identify spatial trends in attack distribution. The results showed that terrorist incidents tend to cluster around particular hotspots, especially near the Kenya-Somalia border and along critical transit routes. These identifiable concentrations enable the estimation of high-risk zones and support a more strategic deployment of security forces.

Temporal features also proved valuable in identifying periods of elevated risk. Variables such as the day of the month revealed recurring trends in attack frequency. Notably, certain periods, such as national elections or religious holidays, showed increased levels of terrorist activity. These findings contribute to the development of forecasts that highlight high-alert windows, enhancing operational readiness and resource optimisation.

FIGURE 4.13
Feature Importance in Random Forest Classifier



Feature importance analysis, illustrated in Figure 4.13, highlights which variables contributed most significantly to accurate predictions. Armed assaults and IED-related events were found to be the most influential features, underscoring the relevance of historical patterns

in understanding future risks. Temporal variables such as ‘day of month’, alongside spatial elements like latitude, also ranked highly in terms of predictive power.

These findings emphasise the necessity of incorporating both time and location dimensions into counterterrorism models. The Random Forest Classifier enables decision-makers to isolate critical factors associated with heightened risk, helping to inform more proactive and data-driven interventions. Focused resource deployment becomes more achievable when informed by predictive insights into both when and where attacks are most likely to occur.

4.7 Objective Two Results

The VA framework was developed to address core challenges identified in counterterrorism efforts, including fragmented integrated data systems, the absence of reliable predictive tools, and the demand for operationally actionable insights. The framework’s visuals were informed by Shneiderman’s Visual Information-Seeking Mantra: ‘overview first, zoom and filter, details on demand’. It integrates structured data collection, spatiotemporal analysis, and dynamic visualisation techniques to enhance situational awareness and support timely, data-driven decision-making in counterterrorism contexts.

4.7.1 Framework components

The data collection and integration layer serves as the foundational stage of the framework, aggregating inputs from both structured and unstructured sources to provide a comprehensive dataset. Structured sources include reliable, standardised datasets such as the GTD, the ACLED, and the CVE Research Hub Observatory. These datasets are recognised for their methodological rigour and consistent formatting.

In contrast, unstructured data sources encompass social media feeds (primarily X), news articles, and community-level incident reports. To ensure consistency and analytical validity, all data undergo pre-processing steps that standardise temporal, spatial, and

categorical attributes. Missing values are either imputed using appropriate statistical methods or categorised explicitly as ‘unknown’. Further, data was validated from multiple sources to ensure accuracy and consistency. Once cleansed, the datasets are merged into a unified schema that resolves inconsistencies, eliminates redundancies, and harmonises varied data structures. This integration process enables seamless cross-source querying, supporting robust analytics, accurate pattern detection, and evidence-based counterterrorism decision-making.

The Analytics Layer applies advanced computational methods to derive actionable insights from the integrated dataset. Spatiotemporal analysis, underpinned by GIS techniques, enables the visualisation of attack density and geographic clustering. Tools such as heatmaps and clustering algorithms (e.g. Density-Based Spatial Clustering of Applications with Noise (DBSCAN)) are used to identify high-risk zones and assess regional vulnerability patterns.

Predictive modelling techniques are employed to anticipate both the type and location of future attacks. The Random Forest algorithm facilitates classification of likely event types, while ARIMA models forecast temporal trends and anticipate potential surges in incident frequency. In addition, anomaly detection methods are used to highlight unusual patterns or the emergence of threats in previously low-risk areas. Together, these methodologies create a robust analytical foundation for risk forecasting and operational planning.

The Decision Support Layer translates analytical outputs into practical strategies for enhancing security response. This component is designed to optimise the allocation of limited resources, prioritise high-risk locations, and manage peak threat periods. Scenario planning is supported through ‘what-if’ simulations, which evaluate the probable outcomes of alternative counterterrorism strategies under varied conditions.

Furthermore, this layer encourages public engagement by using data visualisations to inform local communities about threat-prone areas and to raise awareness of preventive actions.

This dual emphasis on strategic policy planning and community participation contributes to improved resilience and more responsive preparedness at both institutional and grassroots levels.

The Monitoring and Validation Layer ensures that the framework remains adaptive, accurate, and aligned with operational needs over time. Regular feedback loops involving end-users, such as security personnel, analysts, and policymakers, support usability testing and inform iterative system refinement. Performance metrics, including accuracy, precision, and recall, are continuously evaluated to monitor the effectiveness of predictive models.

The framework adopts a dynamic update mechanism, integrating new data as it becomes available and refining algorithms in response to emerging threats and changing operational environments. This ongoing cycle of evaluation and adaptation ensures that the system remains robust, responsive, and aligned with evolving counterterrorism priorities.

4.7.2 Key features and benefits

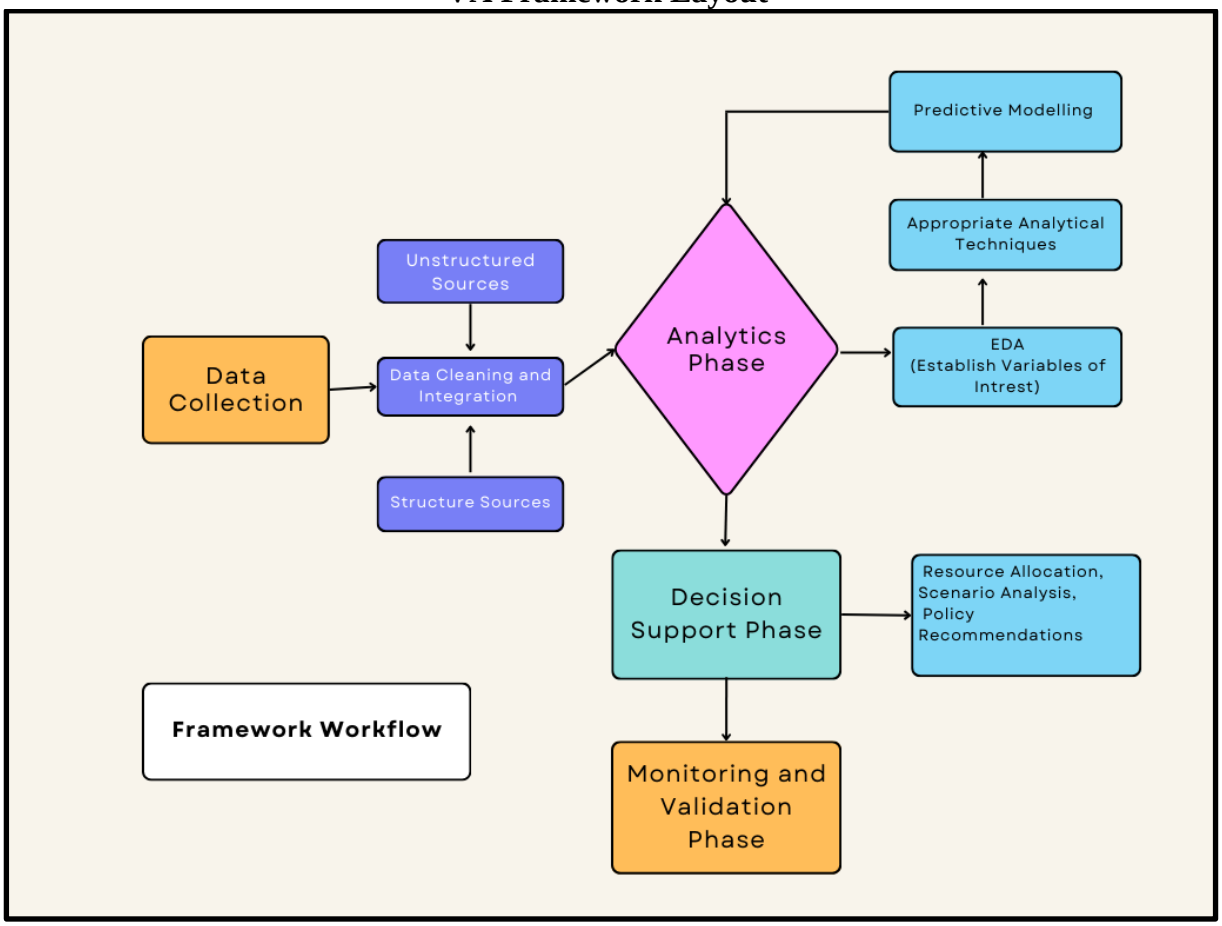
The framework incorporates several advanced features that support adaptability, operational relevance, and cross-regional scalability. Its scalable design allows implementation across different geographical areas experiencing similar threat patterns. Emphasising a proactive approach, the framework seeks to anticipate and prevent attacks, rather than relying solely on reactive responses.

Through the integration of both structured and unstructured data sources, it enables in-depth analysis of spatial, temporal, and behavioural trends, facilitating a more nuanced understanding of terrorist threats. The user-oriented design ensures that outputs are accessible, interpretable, and usable by both security agencies and policymakers, thereby supporting timely and informed decision-making.

Moreover, the framework encourages institutional collaboration by supporting corresponding data sharing and strategic alignment across agencies. These capabilities collectively enhance preparedness, strengthen inter-agency response mechanisms, and improve the overall capacity to mitigate evolving security challenges**.**

4.7.3 Framework workflow

FIGURE 4.14
VA Framework Layout



The development of the VA framework followed a systematic, multi-phase process designed to ensure both analytical rigour, contextual adaptability, and decision-making utility. Each component of the workflow addressed distinct objectives through specific methodologies, forming a cohesive architecture for counterterrorism analysis and strategic planning

The process begins with the Data Collection and Integration Phase. Diverse datasets from both structured and unstructured sources are acquired, ranging from government reports to social media feeds and local news reports. A robust data cleaning, validation, and harmonisation process standardises variables across spatial, temporal, and categorical dimensions, resolving inconsistencies and integrating datasets into a unified, coherent schema. This foundational step enables consistent analysis and reliable data-driven insights.

Subsequently, the Analytics Phase transforms raw data into actionable intelligence. EDA is performed to isolate key variables and identify temporal, spatial, and behavioural patterns. Advanced methods such as clustering (e.g. DBSCAN) help in identifying high-risk zones, while association analysis reveals linkages between attack modalities and targets. Predictive modelling techniques, including Random Forest for classification and ARIMA for temporal forecasting, provide anticipatory insights to inform operational readiness.

Although not explicitly illustrated as a distinct phase, visualisation is embedded within the analytics and decision-support stages. Graphical outputs such as heatmaps, density plots, and network diagrams communicate findings intuitively. These visual tools enhance interpretability and foster shared understanding among analysts, policymakers, and operational stakeholders

The Decision Support Phase applies the analytical outputs to guide operational planning. Security resources are directed to high-risk locations, and simulations are conducted to explore potential outcomes under different strategic scenarios. This phase further underpins evidence-based policymaking and supports sustainable security planning.

Finally, the Monitoring and Validation Phase ensures a continuous system relevance and robustness. Predictive model performance is assessed using metrics such as accuracy, precision, recall, and F1-score. Feedback loops involving practitioners and analysts support

iterative improvements to both model logic and dashboard functionality. As new data becomes available, models are retrained to reflect changing patterns, enabling adaptive responses to evolving threats.

Collectively, this workflow provides a scalable, intelligence-driven framework for counterterrorism that integrates real-time analysis with long-term strategy, enhancing both tactical responsiveness and institutional resilience.

FIGURE 4.15
Visualisation of the data

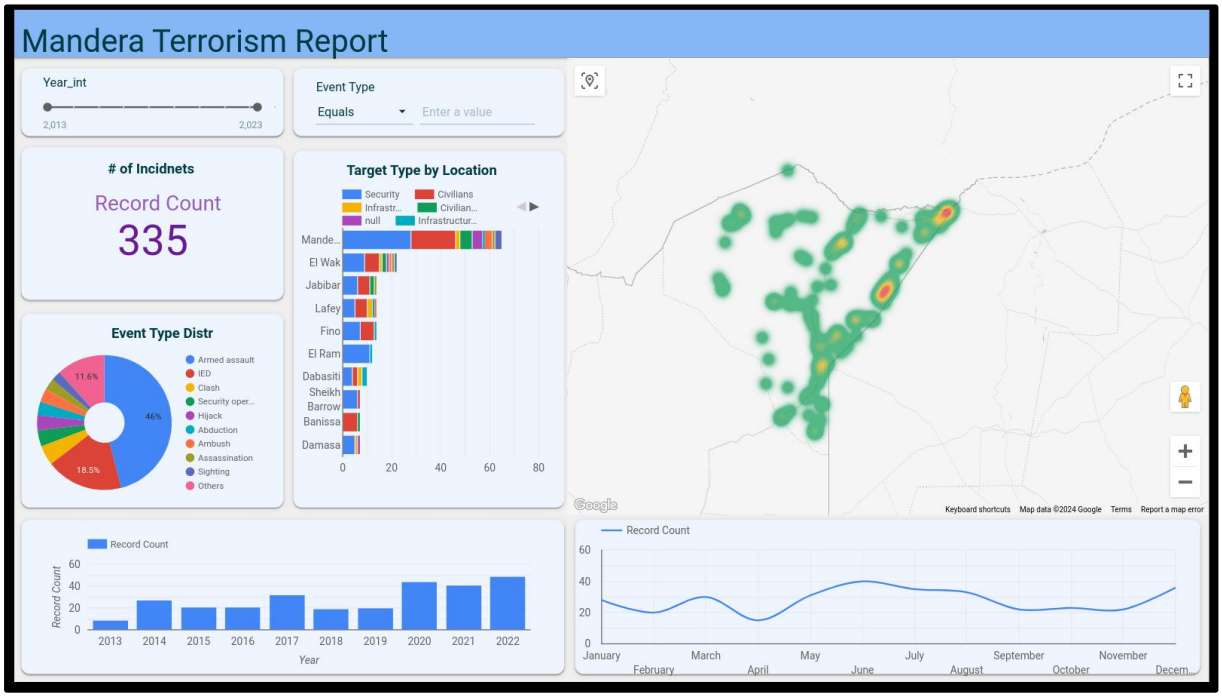
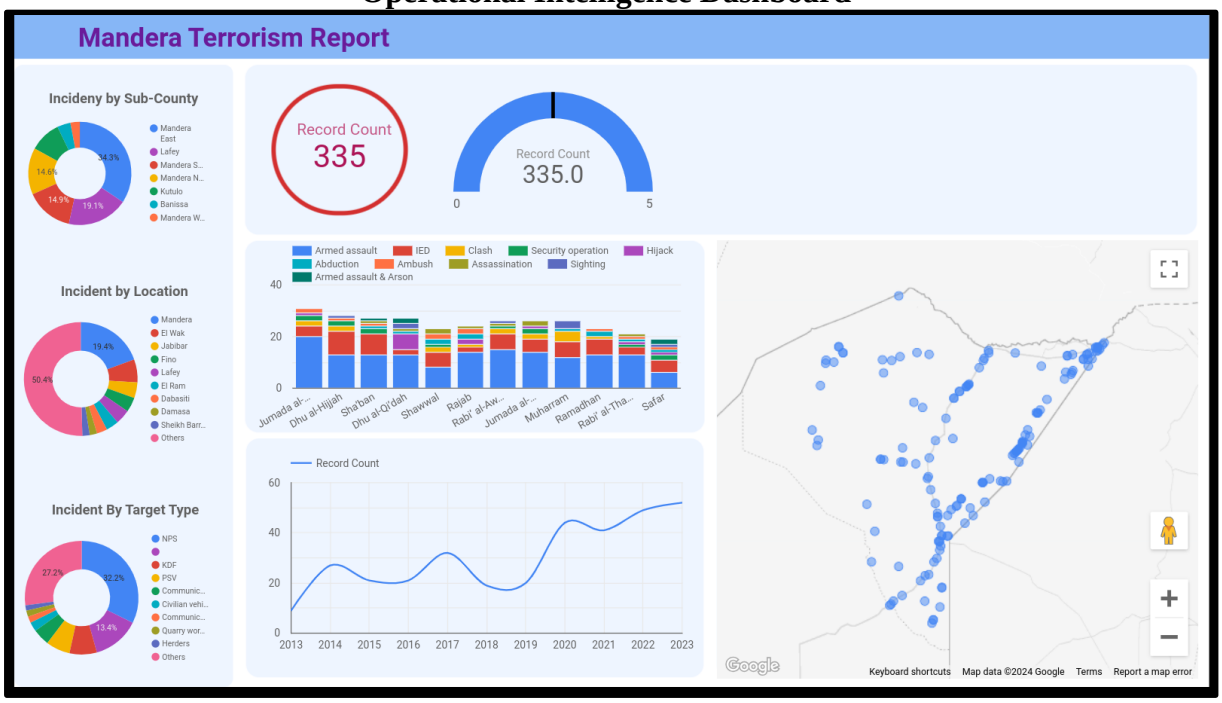


FIGURE 4.16
Operational Intelligence Dashboard



4.8 Findings

4.8.1 Spatial patterns

The geospatial analysis of AS events across Mandera County uncovered distinct and alarming spatial patterns. These non-random patterns reflect deeper socio-political and geographical dynamics that shape the region's vulnerability to terrorist activity. A key finding is the identification of several prominent hotspots, particularly along the volatile Kenya-Somalia border, where incidents are disproportionately concentrated. This border area is marked by weak formal state control and the significant influence of non-state actors, including terrorist groups. Its proximity to Somalia, plagued by chronic instability and the presence of AS, further exacerbates security vulnerabilities in Mandera County

The analysis reveals that specific attack methods are strategically deployed in different locations. Border hotspots, for example, experience more frequent use of IEDs and armed assaults, likely chosen for their high impact and the region's limited capacity for rapid security

response. In contrast, areas with fewer incidents tend to exhibit varied or less intensive forms of violence. This suggests a deliberate targeting strategy, with attack methods tailored to exploit local vulnerabilities.

The socio-economic conditions in these hotspots, characterised by poverty, unemployment, and limited education, render the population, especially youth, vulnerable to radicalisation. Extremist groups exploit these grievances, offering financial incentives and a sense of belonging. These findings underscore the need for a comprehensive counterterrorism strategy that combines strengthened security measures, such as improved border controls, with targeted initiatives to address underlying socio-economic disparities. Greater cooperation between Kenyan and Somali authorities is also essential to managing cross-border threats. Understanding the spatial and temporal dimensions of terrorist activity is crucial to shaping effective and sustainable security responses for Mandera County and the broader region.

4.8.2 Temporal patterns

The temporal analysis of terrorist activity in Mandera County reveals a clear correlation between the timing of attacks and broader socio-political events. These acts of violence are not random but follow discernible patterns, with periodic surges that suggest a deliberate strategy by AS to capitalise on moments of instability or unrest.

A notable observation is the increase in AS activity during election seasons and periods of political uncertainty. During such times, heightened political rhetoric, public demonstrations, and occasional violent clashes create an atmosphere of instability. Terrorist groups appear to exploit this turbulence to erode public confidence in the government's capacity to ensure security and order.

Surges in AS activity also tend to follow large-scale security operations. These increases may arise from several factors: terrorist groups might launch retaliatory attacks to

demonstrate their resilience and challenge state authority, while the operations themselves can disrupt local communities. Displacement, temporary disruptions to daily life, and sometimes heavy-handed enforcement tactics can alienate the local population, conditions that extremist groups often leverage for recruitment and radicalisation.

These temporal patterns underscore the complex interplay between socio-political dynamics and terrorist violence, emphasising the need for a nuanced counterterrorism approach. Such an approach must go beyond immediate tactical responses to include efforts to stabilise the political environment, mitigate the collateral impact of security operations on communities, and address root causes of extremism. A deep understanding of the temporal dynamics of terrorist behaviour enables policymakers and security agencies to anticipate surges in violence and respond with targeted, proactive measures, ultimately contributing to long-term regional stability.

4.8.3 Outlier analysis

Outlier analysis played a vital role in identifying anomalies within the dataset, revealing cases where incident patterns diverged significantly from expected norms. These anomalies often represent rare but high-impact events that can be overlooked in aggregate trend analyses. A particularly notable example was the spike in attacks during the post-election period of 2021, especially in Sub-Counties that had historically experienced low levels of violence. This surge served as an early warning, underscoring the need for heightened security measures during politically sensitive periods and suggesting that AS may be expanding its operations into previously unaffected areas. The detection of such outliers reinforces the importance of tracking atypical patterns, as these may signal emerging threats and shifts in the operational strategies of terrorist groups.

4.8.4 Attack and target types

In Mandera County, terrorist attack patterns are characterised by a predominance of armed assaults and bombings, the primary tactics employed by militant groups in the area. These attacks are deliberately orchestrated to maximise psychological and physical impact, aiming to disrupt daily life and instil widespread fear within local communities. Armed assaults typically involve direct engagements with security personnel or attacks on civilians, frequently resulting in substantial casualties. Bombings, by contrast, are used to inflict extensive damage, targeting symbolic and strategic locations such as markets, government buildings, and vital transport and communication infrastructure.

The selection of targets further illustrates the calculated nature of such violence. Civilians often bear the brunt of attacks designed to destabilise communities and erode public morale. Security forces are also consistently targeted, especially in areas where law enforcement presence disrupts militant activities. These attacks serve a dual purpose: they weaken the government's operational capacity and symbolically challenge state authority.

Analysis of these incidents suggests a sustained presence of AS militants, a group notorious for its prolonged and deadly insurgency in the region. Their operational strategies in Mandera County mirror broader trends observed across the border in Somalia, where AS continues to resist local and international efforts to restore governance and regional stability.

4.8.5 Data fusion insights and multi-agency coordination

The application of data fusion techniques has significantly enhanced the understanding of terrorism dynamics in Mandera County by integrating structured and unstructured data. Structured data, typically sourced from official reports and databases, provides a solid foundation for analysing long-term patterns. In contrast, unstructured data, particularly from social media platforms such as X (formerly Twitter), offers real-time, context-rich insights that

may be absent from traditional sources. These updates, including eyewitness accounts, help corroborate official records and improve the accuracy of incident verification.

Integrating data from multiple agencies further enriches the analytical process. Different organisations often collect distinct types of information, ranging from incident reports and threat assessments to socio-political indicators. Consolidating these datasets into a unified framework produces a more holistic view of the threat environment. This multi-agency approach fosters coordination and strategic alignment, allowing stakeholders to operate with a shared understanding.

Collaborative insights drawn from law enforcement, intelligence bodies, local authorities, and financial institutions help reveal emerging trends and public reactions. For instance, spikes in social media activity following an attack may expose underlying community sentiment or broader political ramifications. The fusion of multi-source data from various agencies bridges critical information gaps and supports more agile, data-driven counterterrorism strategies. Ultimately, this approach strengthens institutional cohesion and enhances the national response to terrorism.

4.8.6 Clustering

Clustering techniques were employed to group similar terrorist attacks based on shared characteristics, including location, timing, and method of execution. Using K-Means clustering, Sub-Counties were categorised by similarities in attack frequency, target profiles, and weapon types.

The analysis identified three primary clusters: High-Risk Areas, comprising border Sub-Counties with frequent and severe attacks; Moderate-Risk Areas, where attacks were sporadic but often impactful; and Low-Risk Areas, typically more inland regions experiencing occasional attacks, primarily against civilians.

These clusters provide a strategic framework for prioritising resource allocation. Border areas, consistently identified as high-risk, require sustained capacity building in surveillance, intelligence, and defence operations. This data-driven clustering approach enables the GoK to allocate resources more efficiently and target interventions toward the most vulnerable regions. It also facilitates a more focused response to the distinct threat profiles present across the County, helping to address both immediate risks and long-term vulnerabilities.

4.8.7 Key features in random forest prediction

In the Random Forest predictive model, key features such as event subtypes, notably Armed Assaults and IED attacks, exerted the greatest influence on predictive performance. Other important variables, including the day of occurrence and geographical coordinates, underscored the significance of temporal and spatial dimensions in forecasting future incidents.

The model's results suggest that counterterrorism strategies should prioritise the prevention of Armed Assaults and IED attacks, as these pose the most critical threats based on feature importance rankings. This calls for concentrated efforts to strengthen defences in high-risk areas and to pursue intelligence-led operations aimed at pre-empting such events.

Monitoring high-risk days and locations is essential, given the strong predictive value of temporal and spatial indicators. Targeting these patterns enables more efficient resource allocation and improved risk mitigation. The model also highlighted the predictive relevance of less frequent, yet high-impact events, such as abductions, hijackings, and assassinations, signalling the need for tailored operational responses.

The predictive accuracy of the Random Forest Classifier was evaluated by comparing its forecasts against actual outcomes in a test dataset. Results demonstrated robust performance, particularly in identifying high-risk zones and event types. As such, the model offers a valuable

decision-support tool for future counterterrorism planning, enabling more precise and proactive resource deployment to address emerging threats.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This concluding chapter synthesises the findings and key insights derived from the proposed VA framework, discusses its contributions to counterterrorism efforts, and outlines avenues for future research. The framework demonstrates strong potential to support the tracking, analysis, and prediction of terrorism patterns, thereby strengthening strategic planning and operational responses. Building on its emphasis on spatiotemporal analysis and predictive modelling, the framework offers a robust methodology for monitoring and anticipating terrorism dynamics. Additionally, it provides recommendations for future research into contextual and systemic factors that may influence the occurrence and escalation of terrorist attacks.

5.2 Summary of Findings

The research objectives were systematically addressed through the application of the VA framework, using a case study of terrorism trends in Mandera County. Objectives I and II, which focused on analysing spatiotemporal patterns of terrorist activity and identifying critical predictors of attacks, were particularly instrumental in shaping the design of the framework. The spatial analysis revealed distinct concentrations of AS operations in Sub-Counties adjacent to the Kenya-Somalia border, while the temporal analysis established clear correlations between spikes in terrorist activity and socio-political events, especially election cycles and intensified security operations.

Building on these insights, predictive modelling tools such as the Random Forest Classifier and the ARIMA model were integrated into the framework's architecture to forecast attack trends and identify high-risk periods and locations. The results underscored the influence of geographic and temporal features in driving the occurrence of terrorist incidents. Embedding

these patterns and predictors into the VA framework enabled the creation of a decision-support tool capable of generating data-driven insights that strengthen early warning systems, optimise resource allocation, and guide targeted interventions in high-risk areas.

Objectives III and IV extended this foundation, with Objective III validating the framework's effectiveness in real-world contexts. At the same time, Objective IV produced practical recommendations for scaling and adapting it to other high-risk regions. Together, the four objectives form a coherent progression, from analysis and design to validation and application, ensuring that the framework is both theoretically robust and practically relevant.

5.2.1 Role of predictive analytics in achieving the research objectives

A central objective of this study was to incorporate the prediction of terrorist incidents into the VA framework, thereby equipping decision-makers to anticipate and prevent future attacks. To realise this, predictive analytics tools, specifically the Random Forest Classifier and the ARIMA model, were applied to generate reliable forecasts on the timing and location of potential incidents.

The Random Forest model played a key role in identifying high-risk areas. Analysis of features such as event type, geographic coordinates, and day of occurrence enabled the model to generate spatial insights into regions and attack types with a higher likelihood of recurrence. The analysis revealed that certain Sub-Counties, especially those situated along the Kenya-Somalia border and along major transport corridors within Mandera County, exhibited heightened vulnerability to armed assaults and IED attacks, underscoring the County's exposure to cross-border militant activity. These predictive insights inform more effective resource allocation, ensuring that security measures are prioritised in the most at-risk areas to deter and prevent future attacks.

ARIMA modelling was instrumental in forecasting temporal patterns by uncovering seasonal and historical trends in terrorist activity. The model revealed recurring spikes in attacks during politically sensitive periods, notably national election cycles, and during major religious observances such as Ramadan, demonstrating that terrorist activity in Mandera County follows probable, event-driven patterns. These temporal forecasts provide critical support for the development of proactive counterterrorism strategies, particularly the reinforcement of security operations, the enhancement of surveillance, and the dynamic reallocation of resources during high-risk periods to pre-empt militant activity.

In addition to forward-looking prediction, anomaly detection techniques were applied to identify outliers, unusual surges in terrorist incidents that deviated from established trends. These anomalies often coincided with the emergence of new threats or shifts in militant strategy, particularly in areas previously considered low-risk. Detecting and interpreting such deviations provides valuable tactical insights, enabling security forces to adapt their operations, deploy investigative teams, and respond swiftly to evolving threats. This capacity for dynamic responsiveness is critical in preventing both the geographical spread and the operational escalation of terrorist activity. Prediction was built into the VA framework because anticipating attacks allows security agencies to act early, allocate resources efficiently, and prevent threats before they escalate.

5.2.2 Impact of feature importance on decision-making

An essential component of the Random Forest Classifier was the feature importance assessment, which identified the most influential variables associated with future terrorist incidents. Although the dataset was insufficient to achieve highly accurate predictions, the ranking of features nonetheless provided critical direction by revealing the key drivers of terrorist activity. This insight ensured that even in data-scarce environments, the VA

framework could still generate actionable intelligence to guide operational planning and decision-making.

A key finding was that the ‘Armed Assault’ event type emerged as the most significant predictor of future attacks. This insight directly informs resource allocation strategies, as the prevalence and severity of armed assaults necessitate targeted preventive measures. Such measures include deploying armed patrol units in high-risk areas, establishing checkpoints on frequently attacked roads, and strengthening intelligence operations in historically affected regions to disrupt plots before they escalate. The finding also highlights the need for further research into the types of attacks employed by terrorist organisations, to deepen understanding and strengthen anticipatory counterterrorism strategies.

Geographic variables, particularly coordinates and the Sub-County classifications, also ranked highly, underscoring the importance of spatial context in anticipating attack locations. This information enables security planners to prioritise resources in high-risk border regions and major transportation corridors, where the likelihood of cross-border infiltration is greatest. In addition to deploying enhanced surveillance and road monitoring technologies in these areas, it is equally important to study the terrain to understand why terrorist groups favour specific locations for their operations. The analysis further indicates that most IED attacks occurred on untarmacked roads, suggesting that infrastructural improvements, such as the tarmacking of frequently targeted routes, could significantly reduce the prevalence and effectiveness of such attacks, while simultaneously improving mobility for security forces.

Temporal features, such as the ‘Day’ variable, also emerged as significant predictors, emphasising the importance of aligning operational planning with days of elevated risk. These findings suggest that security agencies should adapt deployments to temporal patterns of terrorist activity by rotating shifts to ensure full coverage, establishing temporary checkpoints

on high-risk days, and intensifying patrols during periods of heightened vulnerability, such as market days, religious gatherings, or political rallies. Adjusting security operations to these temporal rhythms not only reduces the likelihood of successful attacks but also ensures that limited resources are utilised more strategically in anticipation of predictable surges in threat levels.

Understanding the relative weight of these features, the VA framework demonstrated that predictive modelling can provide meaningful strategic and tactical guidance even when comprehensive datasets are unavailable. Feature importance thus serves as a bridge between limited data environments and predictive insight, giving decision-makers direction on where and when to intervene. The inclusion of prediction in the framework remains vital, as it enables the transition from reactive responses to proactive counterterrorism by anticipating threats, informing resource allocation, and supporting early interventions that strengthen overall security posture

5.2.3 Challenges impeding counterterrorism efforts in Kenya

The study identified several key challenges impeding counterterrorism efforts in Kenya, which directly informed the design and relevance of the VA framework. Chief among these is the interconnected nature of terrorist activities, ranging from armed assaults and IED attacks to abductions that target civilians, security personnel, and critical infrastructure, thereby sustaining persistent insecurity across affected regions. The use of visuals within the framework directly addresses this complexity by enabling analysts to map and interpret the relationships between different attack types, timelines, and locations. This capacity to visualise interdependencies transforms fragmented incident data into coherent patterns, allowing security agencies to better understand how one form of attack may reinforce or escalate another, and to design more integrated and anticipatory counterterrorism strategies.

The geographical dispersion of these incidents, particularly in remote and underserved areas with minimal state presence, severely constrains timely security responses. Limited infrastructure and resource shortages further compound the challenge, making it difficult for overstretched security forces to maintain consistent coverage and creating opportunities for militant groups to operate with relative freedom. The VA framework responds to this challenge by integrating multi-source data into visual, real-time maps that highlight emerging hotspots and priority zones. This enables decision-makers to optimise scarce resources, direct security operations to the most vulnerable areas, and overcome the spatial and logistical barriers that have historically undermined counterterrorism in such regions.

Findings further underscore the need for a coordinated and holistic counterterrorism strategy. Terrorist incidents should not be treated as discrete, isolated events but rather as interrelated components of a complex and evolving threat landscape. Effective strategies must therefore address both immediate operational risks and the deeper structural conditions that sustain terrorism. In Kenya, the government already employs a multi-agency approach to counterterrorism, bringing together intelligence, law enforcement, military, and local administrative actors. The VA framework enhances this approach through a shared, data-driven platform that enables agencies to visualise attack patterns, anticipate risks, and coordinate more effectively. Enhanced inter-agency collaboration, combined with more strategic resource allocation, transforms fragmented responses into resilient, adaptive, and integrated interventions that reflect the systemic nature of terrorism in the region.

5.2.4 Potential indicators and early warning signs of terror attacks

The study identified several critical precursors to terrorist attacks, including increased arms trafficking, irregular patterns of movement, and the sudden emergence of new armed groups. These indicators exhibited strong correlations with the frequency and timing of attacks, particularly in high-risk and border-adjacent regions. Recognising such patterns is fundamental to anticipating the spatial and temporal dynamics of terrorist activity, and their integration into the VA framework was central to its design.

One key insight from the research is the potential of these indicators to form the backbone of an early warning system that provides a strategic advantage to security agencies. Continuous monitoring of such precursors allows for pre-emptive action and disrupts attacks before they materialise. For example, a surge in arms trafficking within a specific area may indicate operational preparations, offering authorities the opportunity to intercept weapons supplies and neutralise threats in advance. Similarly, the detection of suspicious movements or the sudden mobilisation of new armed groups provides actionable intelligence that often signals the planning or staging of an attack.

The VA framework integrates these early warning indicators within its visual and predictive layers, equipping decision-makers to pinpoint hotspots, detect anomalies, and implement interventions with greater speed, accuracy, and operational precision. This integration transforms fragmented signals into coherent, actionable insights that inform surveillance operations, guide intelligence deployment, and support timely security interventions during the preparatory phases of terrorist activity.

In regions facing elevated threat levels, such as Mandera County, the ability to detect and act upon these indicators is especially critical. A focused monitoring strategy, supported by swift intelligence-led interventions, reduces the potential for loss of life and infrastructure

damage while enhancing long-term stability in vulnerable areas. The framework, therefore, demonstrates the importance of embedding predictive indicators into a comprehensive early warning system, advancing preventative, intelligence-driven counterterrorism strategies grounded in anticipation rather than reaction.

5.2.5 A VA framework for monitoring terrorist attacks

The development of the VA framework marks a significant advancement in the monitoring and strategic response to terrorist activity. Unlike conventional approaches that rely on fragmented and delayed data, the framework was purposefully designed to support analysts, researchers, and policymakers through a holistic interrogation of multidimensional terror-related data, thereby addressing the persistent gaps in Kenya's counterterrorism capacity. Its structure accommodates operational, tactical, and academic priorities, ensuring both practical utility and research relevance.

The integration of multi-source datasets combined with advanced visualisation techniques enables the VA framework to deliver a real-time, coherent depiction of an evolving threat environment. This dynamic capacity is particularly vital in regions such as Mandera County, where delayed detection and weak data integration have historically undermined effective responses. Within Kenya's multi-agency counterterrorism framework, the VA system offers a shared platform through which intelligence, law enforcement, military, and administrative agencies can access, interpret, and act upon the same evidence base. Such integration not only reduces duplication and information silos but also enhances inter-agency coordination, ensuring that interventions are timely, well-targeted, and strategically aligned to the evolving threat landscape.

A strength of the framework lies in its ability to represent spatial and temporal dimensions simultaneously. This capability illuminates trends and correlations that would

remain hidden in tabular or text-based formats, such as the clustering of bombings, kidnappings, or armed assaults, and their correlation with shifting variables like militant group movements or arms trafficking routes. In doing so, the framework provides evidence-based clarity on the interdependencies between attack types, targets, and enabling conditions.

The visual approach enhances both interpretability and operational relevance. Security agencies can identify concentrations of suspicious activity, prioritise at-risk areas, and deploy resources pre-emptively to prevent escalation. This justification for the framework's design rests on its capacity to transform fragmented signals into actionable intelligence, enabling more agile, data-driven, and targeted interventions.

Ultimately, the VA framework does more than offer a technological enhancement; it constitutes a strategic evolution toward intelligence-led, proactive security planning. Its capacity to anticipate risks, strengthen early warning systems, and inform the timely allocation of resources significantly increases the potential to prevent attacks and save lives. This validates its role as a critical tool for counterterrorism, particularly in resource-constrained and high-risk contexts where conventional systems have proven inadequate.

5.2.6 Testing and validating the VA framework

The validation phase of the developed VA framework demonstrated its practical utility in advancing more strategic and timely counterterrorism responses. When applied to terrorism data from other Counties, such as Wajir, the framework consistently revealed spatial hotspots of militant activity. Temporal validation also confirmed recurring spikes in attacks during politically sensitive periods, including election cycles and major religious observances, thereby illustrating the framework's capacity to detect seasonality and event-driven surges in terrorist activity.

These outputs, spatial clustering, temporal forecasting, and anomaly detection, demonstrated the framework's effectiveness in generating actionable insights for decision-makers. Security agencies can use hotspot maps to prioritise deployments, temporal forecasts to plan heightened surveillance during high-risk periods, and anomaly detection to investigate irregular activity in areas previously considered low-risk. The validation exercise confirmed that the framework transforms raw data into actionable intelligence, providing decision-makers with a practical basis for proactive counterterrorism planning.

The outcomes affirm that the VA framework developed in this study is a valuable decision-support tool for enhancing the efficiency of counterterrorism initiatives in Kenya. Its integration of multi-source datasets with predictive and visual analytics enables not only the anticipation of threats but also the identification of priority zones and timelines for intervention. Validation within Mandera demonstrates the framework's relevance to Kenya's counterterrorism environment, while also underscoring its potential for adaptation in other high-risk regions facing similar challenges.

5.2.7 Intervention strategy utilising the VA framework

The intervention strategy informed by the VA framework represents a transformative model for the deployment of security resources, particularly in regions most vulnerable to terrorist activity. It facilitates the optimal allocation of personnel, technological assets, and logistical support by directing efforts toward high-risk areas and event types identified through predictive analysis. This approach enhances the operational impact of deployed resources and enables a more responsive and informed counterterrorism strategy.

Findings from this study demonstrate that targeted interventions can significantly reduce the frequency and severity of terrorist incidents. Concentrating efforts on areas and

attack types with the highest likelihood of occurrence enables authorities to neutralise threats at an early stage, thereby promoting greater public safety and regional stability

This data-driven approach improves both the efficiency and effectiveness of counterterrorism operations. Real-time prioritisation empowers security agencies to stay ahead of potential threats, reduce response times, and mitigate the scale of attacks. The successful application of this strategy in Mandera County suggests its potential as a scalable model for other high-risk regions, providing a robust framework for proactive, evidence-based security interventions.

5.3 Conclusions

This study aimed to develop a VA framework for monitoring terrorist activity, using Mandera County, Kenya, as a case study to address persistent counterterrorism challenges in the region. The research demonstrated that the VA approach significantly enhances the detection, analysis, and forecasting of terrorist threats by offering a comprehensive, multi-dimensional view of spatiotemporal and thematic data.

Through the application of cluster analysis, association analysis, and outlier detection, the framework uncovered critical patterns and underlying trends that inform both tactical and strategic decision-making. These conclusions are grounded in the empirical results generated by the framework's application and affirm its potential as a valuable tool in guiding future counterterrorism efforts in Kenya and beyond.

5.3.1 Achievement of objectives

This study successfully developed and validated a VA framework for monitoring and forecasting terrorist activities. The framework supports improved decision-making and strategic resource allocation by addressing critical limitations in existing counterterrorism practices, including fragmented data systems and reactive threat responses. Its tailored design facilitates a proactive posture in anticipating and responding to emerging security threats.

Main deliverable. The core output of the study, the VA framework, integrates both structured and unstructured data sources, applying spatiotemporal analytics and predictive modelling to identify attack hotspots and forecast future threat patterns. Through a user-friendly visualisation interface, the framework enables real-time situational awareness and facilitates evidence-based planning for counterterrorism interventions.

Key insights. The framework addresses critical challenges such as data fragmentation and limited analytical capacity by enabling the integration and interpretation of complex datasets within a unified analytical system. Through this capability, the framework uncovers meaningful patterns and actionable indicators of terrorist activity, including correlations between attack types and specific targets, for instance, the tendency of armed assaults to be directed at communication infrastructure. It also identifies seasonal and event-driven trends, such as heightened attack frequency during Ramadan, which are often overlooked in conventional analyses. The framework highlighted elevated threat levels in Lafey Sub-County during peak periods, such as national election cycles and major religious observances like Ramadan. This capacity to draw attention to high-risk windows demonstrates its value in guiding resource allocation and enabling anticipatory security responses.

Significance. The VA framework represents a scalable and transferable solution for enhancing counterterrorism efforts in Mandera County and similarly affected regions. Its integration of

advanced analytical techniques with an intuitive user interface ensures that complex data can be transformed into operational intelligence, supporting more agile, informed, and effective security interventions.

5.4 Contributions

5.4.1 Theoretical contributions: Advancing counterterrorism and VA research

This study advances and extends existing theories in counterterrorism and visual analytics by introducing the following innovations.

Localised application of SIT in radicalisation. While SIT has been widely applied to explain radicalisation (McCauley & Moskalenko, 2017), this study operationalises the theory within Mandera's unique socio-cultural setting through the developed VA framework. The framework can incorporate clan dynamics and economic grievances to identify potential al-AS recruitment hotspots, showing how localised identity factors, such as marginalisation and inter-clan tensions, intersect with terrorist propaganda to fuel radicalisation. The integration of these socio-cultural dimensions into the VA framework yields a context-specific model of radicalisation, providing a more nuanced and empirically grounded alternative to generic, Western-centric approaches. Furthermore, the model demonstrates potential for adaptation in other terrorism-prone regions of Kenya, particularly counties with comparable socio-cultural complexities such as Wajir and Garissa Counties, thereby broadening its relevance to national counterterrorism efforts.

Bridging the gap between VA and counterterrorism. Existing VA research has largely focused on retrospective analysis (Hegde, 2016) or generic threat detection (Mansoour, 2017). This study advances the field through the development of a proactive, predictive VA framework specifically designed for low-resource, high-threat environments such as Kenya's border counties. Unlike prior work, the framework integrates real-time data fusion, community

validation mechanisms, and adaptive resource allocation strategies, enabling it to function not only as an analytical tool but as an operational asset in counterterrorism. The framework's context-sensitive design ensures its scalability within Kenya and other regions, demonstrating how VA can transition from abstract academic models into practical, field-ready systems that directly enhance national counterterrorism capacity.

Spatiotemporal analysis of border security. Traditional border security theories often emphasise physical barriers and surveillance (Buzan & Hansen, 2020). This study, through the developed VA framework, introduces a data-driven approach to monitoring cross-border militant movements along fragile frontiers such as the Kenya-Somalia border. The analysis of geospatial patterns, including AS infiltration routes, and temporal dynamics, such as election-related surges, produces empirical evidence that supports predictive and adaptive border security strategies. The framework also demonstrates strong potential for regional collaboration, enabling Kenya, Somalia, and Ethiopia to merge transnational datasets, share intelligence on infiltration routes, and coordinate cross-border interventions. The framework also allows for the processing of data from technical tools, such as drones, satellite imagery, and border monitoring systems, and integrating these inputs with other datasets to generate a comprehensive and dynamic picture of emerging threats.. Through this approach, the VA framework advances border security thinking beyond static surveillance, establishing a proactive, intelligence-led model that reflects both the transnational and technologically complex nature of AS operations.

The role of technology in asymmetric conflicts. This study challenges the prevailing assumption that advanced counterterrorism technologies, such as AI and predictive policing, are only applicable in high-resource environments (Chen, 2019). Through the development and application of the VA framework in Mandera County, a resource-constrained and data-scarce

setting, the research demonstrates that context-adapted technology can deliver superior outcomes compared to traditional methods. The framework's ability to integrate multi-source datasets, apply predictive analytics, and provide actionable visual intelligence illustrates how technological innovations, when designed for local realities, can enhance counterterrorism effectiveness even in environments with limited infrastructure

5.4.2 Methodological Contributions: A new paradigm for terrorism analytics

The research introduces innovative methodological advancements that transform how terrorism data is collected, analysed, and translated into operational practice.

Hybrid data fusion model. Unlike prior studies that rely on single-source datasets, the developed VA framework allows for the unification of multiple datasets within a comprehensive analytical schema. This multi-source fusion enhances the accuracy and reliability of threat detection while reducing the biases and blind spots typically associated with isolated datasets. Through this design, the framework ensures that counterterrorism decision-making is informed by a richer, more balanced evidence base, thereby strengthening both predictive capacity and operational relevance.

Predictive disruption modelling. The study pioneers a Predictive Disruption Model that applies machine learning not only to forecast potential terrorist attacks but also to design corresponding countermeasures. This dual capability shifts counterterrorism from a reactive posture of defence to a proactive strategy of offence, enabling security actors to anticipate and pre-empt threats before they materialise. In doing so, the framework represents a methodological advancement beyond conventional predictive policing models, offering a context-adapted approach that directly informs operational planning in high-risk regions.

Community-validated threat intelligence. The framework integrates AI-generated alerts with intelligence from local informant networks, creating a hybrid human-machine validation system. This innovation overcomes a critical limitation in existing VA tools, which are prone to false positives arising from the lack of ground-truth verification. Embedding community validation within the analytical process enhances the credibility of alerts, fosters trust between security agencies and local populations, and ensures that counterterrorism responses remain both accurate and context-sensitive.

Dynamic resource allocation algorithms. Within the developed VA framework, real-time heat maps facilitate the adaptive deployment of security assets, ensuring that limited resources are directed to areas of greatest need. This capability moves beyond static, rule-based allocations by enabling flexible, data-driven adjustments that reflect shifting threat landscapes. The approach offers a scalable and context-appropriate solution for regions like Mandera County, where security operations must operate effectively under constrained budgets and volatile conditions.

Cross-Border threat fusion cells. The study proposes the establishment of joint Kenya-Somalia analytics hubs designed to integrate transnational datasets with locally observed attack patterns. Such cross-border fusion enables the detection of infiltration routes, coordinated monitoring of militant activity, and shared validation of early warning indicators across jurisdictions. This form of integration is unprecedented in VA-based counterterrorism research and directly addresses the transnational character of AS operations, providing a foundation for regional intelligence collaboration and coordinated security responses.

5.4.3 Practical contributions: From theory to action

The VA framework provides tangible, empirically validated solutions that strengthen operational effectiveness in counterterrorism and demonstrate adaptability for application in other high-risk regions.

Real-time early warning system. The developed VA framework encompasses predictive analytics that significantly reduce response times, enabling security forces to pre-empt rather than merely react to attacks. This advancement marks a clear improvement over existing early warning systems, which often rely on delayed, fragmented, or incomplete intelligence, limiting their effectiveness in high-risk contexts such as Mandera County.

Cost-effective counterterrorism. The framework optimises patrol routes, checkpoint placements, and the deployment of other resources such as surveillance drones, enabling security agencies to lower operational costs while simultaneously improving threat interception rates. Validation within the study confirmed that hotspot detection and temporal analysis guided smarter deployments in high-risk Sub-Counties, ensuring that resources were channelled where they were most needed. These outcomes demonstrate that data-driven strategies can deliver greater impact with fewer resources, a critical advantage for regions operating under persistent budgetary and logistical constraints.

Community-centric security. Validation of information by the community embedded within the developed VA framework strengthens trust between local communities and security forces while minimising false alarms that often undermine operational credibility. This socio-technical integration, though rare in counterterrorism practice, addresses the intelligence-action gap in high-risk regions. Its importance is evident in Somalia-border counties, where cross-border clan affiliations shape trust and recruitment dynamics. Embedding these realities within the VA framework ensures strategies that are both technologically robust and socially

grounded. The approach also responds to the historical victimisation of Somali and broader Muslim communities in Kenya's counterterrorism efforts, which has fuelled mistrust and alienation. Embedding community validation into intelligence processes reduces the risk of wrongful targeting, enhances cooperation with affected populations, and provides a platform for regional collaboration, as cross-border clan linkages can strengthen transnational intelligence-sharing and coordinated interventions.

Scalable pilot programs. The framework's successful application in Mandera County demonstrates its adaptability to other regions facing comparable security challenges. Pilot results highlighted measurable gains in threat detection, resource efficiency, and community resilience, providing a replicable blueprint for deployment in similar high-risk environments. Given the shared dynamics of Kenya's northern frontier, including Mandera, Wajir, Garissa and Lamu Counties, the framework holds strong potential for wider implementation across these counties to strengthen counterterrorism efforts along the border region.

Policy and legislative support. The study provides empirical evidence to inform policy decisions on budget reallocation, intelligence-sharing reform, and investment in local capacity-building. While consistent with the objectives of Kenya's National Counterterrorism Strategy, the developed VA framework enhances implementation through data-driven precision, ensuring that counter-terrorism interventions are both targeted and evidence-based.

5.4.4 *Contribution to stakeholders: Who benefits and how*?

The VA framework delivers targeted, actionable benefits across diverse stakeholder groups, reinforcing its practical relevance and real-world impact.

TABLE 5.1
Contribution to Stakeholders

Stakeholder	**Contribution**	**Impact**
Security Agencies	Real-time threat maps, predictive disruption tactics, and optimised resource deployment.	Faster response times, improved cost efficiency, and higher interception of threats.
Local Communities	Community-validated alerts, youth empowerment tools, and trust-building mechanisms.	Fewer false alarms, reduced radicalisation risks, and strengthened trust with security forces.
Policymakers	Data-driven insights for legislation, budget allocation, and cross-border collaborations.	Evidence-based policy formulation and enhanced inter-agency coordination.
Academic Researchers	Access to a rich dataset, analytical framework, and case study for terrorism research.	Expanded avenues for spatiotemporal and VA-based research in conflict zones.
International Partners	Scalable model for cross-border security collaboration (e.g., Kenya-Somalia initiatives).	Stronger regional security cooperation and more effective threat intelligence sharing.

5.4.5 Broader Implications for Counterterrorism and VA Research

This study extends the boundaries of counterterrorism and visual analytics through the VA framework in several key ways.

Proving VA's viability in low-resource settings. The framework demonstrates that advanced analytics can function effectively in data-scarce, infrastructure-poor environments, challenging the perception that such tools are limited to high-income nations.

Shifting from reaction to proactive. The research advances counterterrorism practice from post-incident analysis to proactive, pre-emptive action, establishing a new benchmark for predictive security strategies.

Human-centric technology. The integration of AI-driven analytics with community validation shows how technology and local trust can complement one another, addressing ethical concerns about excessive reliance on automation in security operations.

Cross-disciplinary fusion. The framework bridges computer science (VA, machine learning), social sciences (SIT, radicalisation), and security studies, offering a holistic and interdisciplinary model for future research.

A blueprint for asymmetric conflicts. The study provides a scalable and adaptable framework that can be applied to other regions confronting non-state armed groups, from insurgencies in the Sahel to urban terrorism in fragile cities.

5.4 Research Limitations

While this study has yielded valuable insights, several limitations must be acknowledged. First, data availability and quality presented a challenge. The analysis depended on existing secondary sources, and the accuracy of findings was inherently linked to the quality and completeness of these reports, which may have introduced biases or omitted critical incidents. Moreover, the availability of locally assembled datasets on terrorist activities within Kenya was limited, highlighting the need for more systematic and standardised data collection frameworks to support robust counterterrorism research.

Second, the geographic scope of the study was restricted to Mandera County, which may limit the generalisability of the findings to other regions with different socio-political characteristics. Although Mandera County was selected as a representative case study, further application of the VA framework across diverse regional contexts is necessary to validate its scalability and adaptability.

Third, resource constraints, including limited access to advanced analytical software and computing infrastructure, affected the depth of modelling and hindered more rigorous validation procedures. Future studies could benefit from enhanced technical resources to strengthen analytical robustness.

Despite these limitations, the study lays a solid foundation for future investigations and contributes actionable insights that can inform the development of more effective counterterrorism strategies.

5.6 Recommendations for Future Research

Terrorism in Mandera County requires context-specific and adaptive solutions that extend beyond conventional counterterrorism measures. This study advances three innovative approaches, each operationalised through the developed VA framework, to address Mandera County's distinct challenges of porous borders, clan dynamics, and resource constraints. In contrast to generic strategies, these approaches integrate predictive analytics, community collaboration, and dynamic resource management to proactively disrupt AS operations.

5.6.1 Predictive disruption model: Turning data into offensive tactics

The study pioneers a Predictive Disruption Model that transforms the VA framework's forecasts into offensive counterterrorism tools. Through the analysis of historical attack sequences (e.g., IEDs followed by armed assaults), the model can be used to predict not only where but also how AS is likely to strike next. Security forces can then deploy tactical decoys, such as fake convoys or simulated checkpoints, to lure militants into controlled engagements. This approach compels AS operatives to expend resources or fall into ambushes, shifting the operational advantage to defenders. Pilot applications in Mandera confirmed the model's potential to disrupt militant patterns of operation, demonstrating how proactive strategies can turn the region's terrain into a liability for insurgents.

5.6.2 Community-validated threat intelligence: Bridging tech and trust

To address misinformation and delays in intelligence-sharing, the study introduces a Community-Validated Threat Intelligence system within the VA framework. In this model, VA-generated alerts are cross-checked through trusted local networks, such as vetted elders, traders, and other community actors, via a secure mobile platform. The hybrid approach integrates social trust with AI predictions, minimising false positives and accelerating response times. In practice, community feedback was instrumental in validating suspicious gatherings flagged by the VA system, helping to intercept an AS recruitment drive. This innovation closes

a critical gap in existing counterterrorism tools, demonstrating how local knowledge can enhance technological accuracy and ensure threats are acted upon both swiftly and reliably.

5.6.3 Dynamic resource redistribution: Real-time adaptability

The VA framework's real-time heat maps support Dynamic Resource Redistribution, enabling security assets such as drones and patrols to be reallocated in response to live threat assessments. The system tracks patterns of activity, including election-related violence and militant movements along trade routes, ensuring that limited resources are directed where they have the greatest impact. Validation in Mandera County demonstrated that this adaptive approach improved interception effectiveness compared to static deployments, which AS frequently exploits through predictable routines. The method illustrates that even in resource-constrained environments, smart allocation informed by data can outmanoeuvre militant strategies and strengthen operational resilience.

REFERENCES

Ahmad Sabri, I. A., Man, M., Abu Bakar, W. A. W., & Mohd Rose, A. N. (2019). *Web data extraction approach for deep web using WEIDJ*. Procedia Computer Science, 163, 417–426.

Aleroud, A., Abu-Al Sheeh, N., & Al-Shawakfa, E. (2020). *A graph proximity feature augmentation approach for identifying accounts of terrorists on Twitter*. Computers & Security, 99, 102056.

Alexander, E., Eppler, M. J., & Comi, A. (2021). *Data Integration: A Real-Time, Participant-Driven, and Visually Supported Method*. Journal of Mixed Methods Research, 15(1), 87–113. https://doi.org/10.1177/1558689820902294

Alotaibi, M. (2017). *Applying visual analytics in threat detection*. Security Informatics, 9(3), 301–317.

Al Jazeera. (2023). *Counter-terrorism experts say Africa is the world's terrorism hotspot with half of 2022's victims*. Al Jazeera.

Andrienko, G., Andrienko, N., Fuchs, G., & Rinzivillo, S. (2017). *Detecting hidden traffic problems with visual analytics of geospatial data*. Transportation Research Procedia, 27, 349–356.

Aning, K., & Abdallah, M. (2016). *Countering violent extremism in Africa: The role of media and civil society*. South African Journal of International Affairs, 23(4), 521-536.

Bergen, P. L. (2024). *September 11 attacks*. Encyclopedia Britannica.

Bowie, N. G. (2024). *40 terrorism databases and data sets*. Journal of Security Studies, 15(2).

Brennan, T. (2017). *Analyzing the spread of terrorism: A case study approach*. Journal of Terrorism Studies, 34(2), 45-67.

Buil-Gil, D., & Langton, S. H. (2020). *GIS and geovisual analysis*. In GIS and Geovisual Analysis. SAGE Publications Ltd.

Campbell, J. (2021). *The changing dynamics of terrorism in Africa*. African Security Review, 30(1), 98-114.

Carboni, A., & Raleigh, C. (2024). *Collecting conflict data worldwide: ACLED's contribution*. In H. Wilson, O. Samuel, & D. Plesch (Eds.), Security science and technology (Vol. 4, pp. 171–187). WORLD SCIENTIFIC.

Cui, W. (2019). *Visual analytics: A comprehensive overview*. IEEE Access, 7, 81555–81573.

CVE Kenya. (2023). *Home—Countering violent extremism (CVE) research hub Kenya*.

Emase, P., Kenia, & Interpeace (Eds.). (2017). *Voices of the people: Challenges to peace in Mandera County*. National Cohesion and Intergration Commission Kenya.

Epstein, H.-A. B. (2020). *Logos and signatures: An important element of outreach*. Journal of Hospital Librarianship, 20(1), 72–77.

Gathara, P. (2021). *The Westgate Mall attack and Kenya's national amnesia*. The Standard.

Ghalleb, A. E. K., & Amara, N. E. B. (2020). *Terrorist act prediction based on machine learning: Case study of Tunisia*. In 2020 17th International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 398–403).

Gill, P., Marchment, Z., Corner, E., & Bouhana, N. (2020). *Terrorist decision making in the context of risk, attack planning, and attack commission*. Studies in Conflict & Terrorism, 43(2), 145–160.

Hancock, D. R., Algozzine, R., & Lim, J. H. (2021). *Doing case study research: A practical guide for beginning researchers (4th ed*.). Teachers College Press.

Hao, M., Jiang, D., Ding, F., Fu, J., & Chen, S. (2019). *Simulating spatio-temporal patterns of terrorism incidents on the Indochina Peninsula with GIS and the random forest method*. ISPRS International Journal of Geo-Information, 8(3), 133.

Hermann, Z. (2023). *15 years of analysing the Global Terrorism Database: An overview*. Scientia et Securitas, 4(1), 51–58.

Institute for Economics & Peace. (2023). *Global terrorism index 2023: Measuring the impact of terrorism*. Institute for Economics & Peace.

Islam, J., Anslow, C., Xu, K., Wong, W., & Zhang, L. (2016). *Towards Analytical Provenance Visualization for Criminal Intelligence Analysis*. In C. Turkay & T. R. Wan (Eds.), EG UK Computer Graphics & Visual Computing (2016). Eurographics Association. https://doi.org/10.2312/cgvc.20161234

Jenkins, J. P. (2023). *Terrorism*. Encyclopedia Britannica.

Kejriwal, M., Doan, A., & Shah, A. (2017). *Visual analytics for understanding terrorist behavior in social media*. Information Visualization, 14(2), 175-188.

Kirwa, A. K & Handa, S. (2025). *Determinants of Successful Implementation of Interagency Counterterrorism Strategies in Lamu County, Kenya*. Journal of African Interdisciplinary Studies, 9(6), 103 – 114

Lederer, E. M. (2023). *Counter-terrorism experts say Africa is the world's terrorism hotspot with half of 2022's victims*. Encyclopedia Britannica.

Lopez, G. (2021). *Mandera Municipality Diagnostics Report*. Sustainable Urban Development (SUED).

Maharana, K., Mondal, S., & Nemade, B. (2022). *A review: Data pre-processing and data augmentation techniques*. Global Transitions Proceedings, 3(1), 91–99.

Mazhar, S. A., Anjum, R., Anwar, A. I., & Khan, A. A. (2021). *Methods of data collection: A fundamental tool of research*. Journal of Integrated Community Health, 10(1), 6–10.

Mugwang'a, M. (2023). *Multi-agency approach is best bet in war on terror*. Nation Africa.

Muibu, D., & Cubukcu, S. (2023). *Assessing the impact of terrorism and counter-terrorism on public perceptions among ethnic minorities in Kenya*. Journal of Policing, Intelligence and Counter Terrorism, 18(1), 43–71.

Nasir, N. M., Latiff, K. A., & Arshad, H. (2020). *Temporal analysis of terrorist attacks in Africa using GIS technology*. ISPRS International Journal of Geo-Information, 9(11), 634.

Nacos, B. L. (2016). *Mass-mediated terrorism: Mainstream and digital media in terrorism and counterterrorism (3rd ed*.). Rowman & Littlefield.

Otsialo, S. (2023). *Governor's report on AS control in Mandera*. Nation Africa.

Phiri, C. (2024). *Examining Kenya's counter-terrorism strategies in the wake of evolving threats*. Journal of Contemporary African Studies, 39(2).

Pate, A. M., & Yates, E. (2023). *Counter-terrorism and public health: Challenges and innovations*. Journal of Public Health Policy and Practice, 34(1), 109–126.

Raleigh, C., & Dowd, C. (2017). *Armed conflict location and event data project (ACLED)*. Journal of Peace Research, 52(4), 496–509.

Sang, P. (2023). *Kenyans are still reeling from 2019 DusitD2 terror attack*. All Africa.

Strindberg, A. (2020). *Social Identity Theory and the Study of Terrorism and Violent Extremism*.

Taherdoost, H. (2021). *Data collection and analysis in scientific research*. Procedia Computer Science, 186, 2–10.

Turi, G. C. (2021). *Winning community trust can help rid Kenya of al-Shabaab*. Institute for Security Studies. https://issafrica.org/iss-today/winning-community-trust-can-help-rid-kenya-of-al-shabaab

UNHCR. (2021). *Addressing displacement due to terrorism in Sub-Saharan Africa*. UN Refugee Agency.

U.S. Department of Homeland Security. (2022). *National terrorism advisory system*. Department of Homeland Security. https://www.dhs.gov/topics/national-terrorism-advisory-system

Wang, Z. (2022). *Developing effective counter-terrorism measures in East Africa*. Journal of Terrorism Studies, 29(4), 312–329.

Williams, P. (2020). *Counterterrorism efforts in sub-Saharan Africa: Strategies and challenges*. Journal of African Studies, 48(3), 293-310.

Wright, L. (2023). *The looming tower: Al-Qaeda and the road to 9/11 (3rd ed*.). Vintage.

Yates, R., & Freeman, L. (2023). *Kenya's counter-terrorism journey: Challenges and future directions*. African Security Review, 32(2), 139–157.

Yohannes, K. (2020). *Understanding the roots of terrorism in Africa*. Macmillan Press.

Zahra, S., & Ali, S. (2022). *Mapping terrorism in East Africa: A spatiotemporal analysis*. International Journal of Geographic Information Science, 36(7), 1390–1412.

Zhang, Y., & Prakash, S. (2022). *Countering terrorism with machine learning*. International Journal of Computer Science & Network Security, 22(3), 55–66.

Zhou, M., & Mears, W. (2023). *Enhancing situational awareness in counter-terrorism efforts*. Journal of Strategic Studies, 25(3), 167–188.

APPENDICES

APPENDIX I: Project Schedule

2025/2026	AUG	SEPT	OCT	NOV	DEC	JAN	FEB	MARCH	APRIL	MAY	JUNE	JULY
Ideation												
Draft Research Questions												
Writing Research Proposal												
Review of Literature												
Proposal Presentation												
Data Collection												
Framework Formulation												
Data Analysis												
Framework Validation												
Compiling the work												
Final defense												
Document submission												

APPENDIX II: Project Budget

No.	Item	Unit	Price	Total
1	Computer / Laptop	1	70,000	70,000
2	Internet connection for conducting research, software downloads, and other purposes.	8	2,500	20,000
3	Travel cost	30	2,500	75,000
4	Data Collection and Cleaning	1	20,000	20,000
5	Conferences cost	4	10,000	40,000
6	Flash Disk	1	1,000	1,000
7	Proposal preparation (i.e., printing, binding, etc.)	500	20 per page	10,000
8	Publishing	1	20,000	20,000
9	Miscellaneous expenses	1		25,600
	Total			281,600