© Journal of Political Science and Policy Studies Vol. 2 No 2 (Feb, 2026)

LEVERAGING SOCIAL MEDIA FOR COUNTER TERRORISM OPERATIONS IN NORTH EAST NIGERIA

IDISIRE JONATHAN TIKON

Nigerian Defence Academy, Kaduna

ABSTRACT

The proliferation of social media has transformed the landscape of terrorism and counter-terrorism globally, providing both opportunities and challenges for security agencies. In North-East Nigeria, terrorist groups such as Boko Haram have extensively leveraged platforms like Facebook, X (formerly Twitter), YouTube, and Telegram to disseminate propaganda, recruit members, and coordinate attacks, undermining conventional military efforts. This study examined the role of social media in enhancing counter-terrorism operations, with a particular focus on Operation Hadin Kai in Borno State. Guided by four objectives, the research explored patterns of terrorist social media use, assessed the extent of social media integration in Operation Hadin Kai, identified technological, institutional, legal, and ethical constraints, and proposed context-specific strategies for optimizing social media utilization. A mixed-methods research design was adopted, combining survey data from security personnel and stakeholders with Key Informant Interviews (KIIs) to provide qualitative depth. Quantitative data were analyzed using descriptive statistics, while qualitative insights were analyzed through content analysis. Findings reveal that terrorists exploit social media for propaganda and recruitment, while Operation Hadin Kai has partially integrated digital tools for intelligence gathering, counter-narratives, and strategic communication. Challenges identified include inadequate personnel training, limited technological capacity, weak inter-agency coordination, legal restrictions, and ethical concerns. The study concludes that strategic, ethically grounded, and context-specific social media measures, including capacity building, technological investment, inter-agency collaboration, ethical guidelines, and community engagement, can significantly enhance non-kinetic counter-terrorism operations. The findings contribute to understanding how social media can complement kinetic strategies, strengthen intelligence-led operations, and foster resilience against radicalization, providing actionable insights for policymakers and practitioners in Nigeria and similar conflict-affected regions.

Keywords: *Social Media, Counter Terrorism, Northeast, Nigeria*

Introduction

Globally, terrorism has evolved into a transnational and technologically mediated security threat, with social media increasingly serving as a critical enabler of extremist activities. The exponential growth in internet penetration and the widespread adoption of interactive digital platforms have transformed the operational landscape of terrorism, enabling groups to radicalize, recruit, fundraise, and disseminate propaganda with unprecedented speed and reach. Social media platforms offer low-cost, accessible, and largely decentralized communication

channels that allow extremist organizations to bypass traditional state controls and engage directly with global audiences (Asongu et al., 2019). Consequently, the digital space has emerged as a central battleground in contemporary counter-terrorism efforts, compelling states and security agencies worldwide to rethink conventional, predominantly kinetic, approaches to combating terrorism.

In Nigeria, terrorism constitutes one of the most persistent and multifaceted threats to national security, social cohesion, and economic development. Although the country has experienced various forms of internal conflict since independence, the contemporary terrorism landscape is largely defined by the Boko Haram insurgency and its splinter faction, the Islamic State West Africa Province (ISWAP), particularly in the North-East geopolitical zone. Since the insurgency escalated in 2009, terrorist violence has resulted in widespread loss of life, large-scale displacement, and a protracted humanitarian crisis affecting millions of civilians (Nyadera et al., 2019). The persistence of terrorism in Nigeria has been linked to structural drivers such as poverty, youth unemployment, political marginalization, corruption, and weak state institutions, which have collectively created fertile conditions for extremist ideologies to flourish (Adesola et al., 2024; Njoku et al., 2025). State incapacity in delivering basic services and justice has further facilitated the radicalization and recruitment of vulnerable populations.

At the same time, Nigerian-based terrorist groups have increasingly mirrored global jihadist movements in their strategic use of social media. Drawing inspiration from organizations such as ISIS and al-Qaeda, Boko Haram and ISWAP have leveraged platforms including YouTube, Facebook, Twitter (now X), Telegram, and WhatsApp to circulate propaganda videos, issue threats, justify violence, and communicate with sympathizers (Schmid, 2021). These platforms enable terrorists to amplify their narratives, shape public discourse, and attract both local and transnational support. The rapid diffusion of extremist content, coupled with the use of encryption and anonymity-enhancing technologies, has significantly constrained the capacity of security agencies to monitor and disrupt online terrorist networks (Jain & Vaidya, 2020; Kumar, 2023).

In response, the Nigerian government has largely prioritized kinetic counter-terrorism measures, including large-scale military operations such as Operation Hadin Kai and regional security collaborations through the Multinational Joint Task Force (MNJTF) (Bappah, 2016). While these interventions have recorded some tactical successes, they have also attracted sustained criticism for their limited effectiveness in addressing the ideological and digital

dimensions of terrorism. Scholars argue that the overreliance on military force, alongside allegations of human rights abuses, has in some instances deepened local grievances, undermined trust in state institutions, and inadvertently reinforced extremist narratives (Nyadera et al., 2019). This has highlighted the limitations of purely kinetic strategies in an era where terrorism is increasingly networked, mediated, and sustained through cyberspace.

The North-East Nigeria case study illustrates the paradoxical role of social media in terrorism and counter-terrorism. On one hand, terrorist groups have exploited the decentralized and relatively unregulated nature of digital platforms to publicize attacks, recruit fighters, raise funds, and coordinate operations across borders (Chukwuere & Onyebukwa, 2018). The global "Bring Back Our Girls" campaign, while mobilizing international advocacy, simultaneously amplified Boko Haram's actions and messaging, demonstrating how online visibility can unintentionally serve terrorist objectives (UNDP, 2019). On the other hand, the same platforms present significant opportunities for counter-terrorism operations, including intelligence gathering, counter-narrative dissemination, community engagement, and early warning mechanisms. Recognizing this duality, governments and national security practitioners globally and within Nigeria have increasingly emphasized the need for non-kinetic, digitally oriented counter-terrorism strategies that leverage social media rather than merely suppress it. However, designing effective social media–based counter-terrorism interventions remains complex, requiring the integration of technological tools, coherent policy frameworks, inter-agency coordination, respect for human rights, and credible leadership (Downing, 2023).

It is against this global, African, national, and regional backdrop that this study examines the role of social media in counter-terrorism operations in North-East Nigeria. By focusing on the strategic use of social media as a counter-terrorism tool, the study seeks to contribute to ongoing scholarly and policy debates on how digital platforms can be harnessed to complement traditional security approaches and enhance the overall effectiveness of counter-terrorism efforts in Nigeria.

Statement of the Research Problem

Terrorist groups operating in Borno State have continued to leverage social media and encrypted platforms to circulate propaganda, intimidate civilian populations, undermine the legitimacy of Operation Hadin Kai, and sustain recruitment despite sustained military pressure. At the same time, encryption and privacy safeguards on widely used platforms constrain

intelligence gathering, creating a strategic dilemma between operational effectiveness and the protection of civil liberties (Kumar, 2023). Furthermore, weak coordination between security agencies, limited digital counter-terrorism capacity, and jurisdictional constraints over foreign-owned social media platforms reduce the ability of Operation Hadin Kai and related agencies to fully exploit social media for intelligence, counter-narratives, and community engagement. The problem is compounded by the rapid spread of misinformation and disinformation, which empirical evidence shows travels significantly faster than verified information online, eroding public trust and weakening civilian cooperation that is critical to population-centric counter-terrorism operations (Vosoughi et al., 2018). In a context where community trust is essential for intelligence-led operations in Borno State, unchallenged extremist narratives and perceptions of state overreach risk undermining the effectiveness of Operation Hadin Kai.

Consequently, despite the centrality of social media to both terrorist operations and everyday communication in North-East Nigeria, there remains a significant gap in coherent, context-specific, and ethically grounded strategies for integrating social media into counter-terrorism operations. This study therefore, addresses the problem of how social media can be systematically leveraged to complement Operation Hadin Kai and broader counter-terrorism efforts in Borno State, enhancing non-kinetic capabilities while safeguarding civil liberties, public trust, and democratic norms.

1.3 Research Questions

The study is guided by the following research questions:

i. How do terrorist groups operating in Borno State utilize social media platforms to propagate propaganda, recruit members, and undermine counter-insurgency efforts such as Operation Hadin Kai?
ii. To what extent has Operation Hadin Kai integrated social media into its counter-terrorism operations for intelligence gathering, strategic communication, and counter-narrative dissemination in Borno State?
iii. What technological, institutional, legal, and ethical challenges limit the effective use of social media in supporting Operation Hadin Kai's counter-terrorism objectives in North-East Nigeria?

iv. How can social media–based strategies be strengthened to complement Operation Hadin Kai by enhancing non-kinetic counter-terrorism operations while maintaining civil liberties and public trust in Borno State?

1.4 Objectives of the Study

The broad objective of this study is to examine how social media can be leveraged to enhance counter-terrorism operations in Borno State, with specific reference to Operation Hadin Kai. The specific objectives are to:

i. Examine the patterns and methods through which terrorist groups in Borno State utilize social media platforms for propaganda dissemination, recruitment, and the undermining of Operation Hadin Kai.
ii. Assess the extent to which Operation Hadin Kai integrates social media into its counter-terrorism operations for intelligence gathering, strategic communication, and counter-narrative dissemination.
iii. Identify the technological, institutional, legal, and ethical challenges constraining the effective use of social media in supporting Operation Hadin Kai's counter-terrorism objectives in Borno State.
iv. Propose context-specific and ethically grounded social media strategies capable of strengthening non-kinetic counter-terrorism operations and complementing Operation Hadin Kai in Borno State.

Literature Review

Concept of Social Media

Social media refers to internet-based platforms and applications that enable users to create, share, and interact with content in real time, facilitating communication, collaboration, and information exchange across local, national, and global networks (Kaplan & Haenlein, 2010). These platforms, which include Facebook, X (formerly Twitter), YouTube, WhatsApp, Telegram, and Instagram, are characterised by their interactive nature, accessibility, and capacity for rapid dissemination of information. Beyond personal and commercial use, social media has emerged as a critical arena for political communication, advocacy, and public discourse.

In the context of security studies, social media assumes a dual role. On one hand, it serves as a powerful tool for state actors and civil society to enhance public awareness, mobilize communities, and support counter-terrorism initiatives through intelligence gathering, strategic communication, and counter-narratives (Chukwuere & Onyebukwa, 2018). On the other hand, social media provides terrorist organisations with unprecedented opportunities to propagate extremist ideologies, recruit members, fundraise, and coordinate operations across borders with minimal oversight (Schmid, 2021). The decentralised and largely unregulated nature of these platforms allows rapid spread of content, including misinformation and radicalising narratives, making social media both a resource and a challenge for contemporary counter-terrorism efforts. In North-East Nigeria, the strategic use of social media by Boko Haram and ISWAP has amplified the threat landscape, facilitating online radicalization, psychological warfare, and undermining of operations such as Operation Hadin Kai. Understanding social media's characteristics, potentials, and limitations is therefore essential to designing effective and ethically grounded strategies for leveraging these platforms in counter-terrorism operations.

Kapoor et al. (2018) conceptualise social media as a constellation of digital technologies designed to enable the exchange of ideas, opinions, and multimedia content across virtual communities. These platforms empower users not only to consume but also to create and disseminate content, thus promoting dialogic, interactive communication in contrast to the traditional monologic, one-directional transmission of information (Kent & Taylor, 2021). The scale of social media adoption is unprecedented; over 5 billion people representing approximately 62% of the global population are active users of platforms such as Facebook, X (formerly Twitter), Instagram, and YouTube (Kapoor et al., 2018). This digital expansion has precipitated a marked shift in information consumption patterns, with a growing number of individuals obtaining news and current affairs updates from social media rather than from traditional media outlets (Walker & Masta, 2021).

The versatility of social media is reflected in its wide-ranging applications, which include personal communication, professional networking, political activism, business marketing, and customer engagement. For commercial entities, social media offers cost-effective tools for brand visibility, consumer interaction, and strategic advertising. As De Oliveira Santini et al. (2020) observe, social media platforms have come to represent a substantial share of global advertising expenditure, highlighting their economic and communicative significance. However, the growth of social media has also introduced complex challenges. Scholars such

as Adeeb and Mirhoseini (2023) have identified various negative externalities, including the proliferation of misinformation, breaches of personal privacy, and adverse psychological effects, particularly among adolescents and young adults. These concerns have prompted increased scrutiny from policymakers, technology firms, and civil society actors, all of whom recognise the urgency of fostering a safer and more accountable digital environment.

Concept of Counterterrorism

Counterterrorism refers to the broad spectrum of policies, strategies, and operational measures undertaken by state and non-state actors such as governments, military forces, law enforcement agencies, and intelligence services to prevent, disrupt, and respond to acts of terrorism (Byman, 2019). Modern counterterrorism encompasses both reactive and proactive approaches. While reactive measures aim to disrupt ongoing or imminent terrorist activities, proactive strategies focus on preventing radicalisation, enhancing community resilience, and addressing the root causes of extremism (Schmid et al., 2021). An essential pillar of current counterterrorism efforts is community engagement. As Hartley (2023) observes, effective counterterrorism extends beyond state-centric security frameworks to involve grassroots participation. Local communities play a crucial role in early detection of radicalisation and in countering extremist ideologies through inclusive narratives, education, and dialogue. By building trust between law enforcement and civil society, this approach enhances social cohesion and strengthens societal resilience against violent extremism.

Similarly, technology companies are becoming key stakeholders in counterterrorism operations. Through collaborations with governments and regulatory bodies, major platforms such as Meta, Google, and X have developed algorithms and content moderation policies aimed at identifying and removing extremist material. Legislative instruments, such as the European Union's Digital Services Act, have imposed binding obligations on digital service providers to monitor, report, and eliminate illegal content, including terrorist propaganda (Wilson Sonsini, 2022). Nevertheless, formidable challenges persist, threat actors increasingly exploit encrypted messaging services and the dark web to evade surveillance and coordinate operations clandestinely (Malik, 2018). Moreover, structural drivers of radicalisation such as socioeconomic inequality, political marginalisation, state repression, and ideological polarization remain largely unaddressed. These root causes fuel grievances that violent extremist groups manipulate to recruit adherents and justify their actions.

To respond effectively to these evolving threats, counterterrorism strategies must adopt a comprehensive and forward-looking orientation. This includes investing in advanced technologies, strengthening international partnerships, promoting human rights, and addressing the social, political, and economic conditions conducive to radicalisation. A robust counterterrorism framework must balance kinetic mechanisms with proactive, preventative initiatives to sustainably mitigate the threat of terrorism. In line with this study, counterterrorism is defined as the coordinated use of legal, military, intelligence, technological, and socio-political measures by state and non-state actors aimed at preventing, disrupting, and responding to terrorism, with the overarching objective of ensuring public safety and national security.

The Relationship between Social Media and Terrorism

The relationship between social media and terrorism has been extensively explored in contemporary security studies, highlighting the transformative role of digital platforms in modern extremist operations. Social media platforms provide terrorists with cost-effective, accessible, and far-reaching tools to disseminate propaganda, recruit followers, raise funds, and coordinate activities across local, national, and transnational networks (Schmid, 2021). Unlike traditional media, social media offers interactivity, anonymity, and global reach, which extremist groups exploit to influence public perception, instil fear, and legitimize their ideological narratives.

Empirical studies indicate that terrorist groups such as ISIS, al-Qaeda, and Boko Haram have developed sophisticated digital strategies that capitalize on social media's unique affordances. For instance, ISIS is known for producing high-quality videos, online magazines, and messaging campaigns that target vulnerable individuals worldwide, resulting in significant foreign fighter mobilization (Conway et al., 2019). Similarly, Boko Haram and ISWAP in North-East Nigeria have leveraged platforms such as WhatsApp, Facebook, X (formerly Twitter), and Telegram to recruit youth, coordinate attacks, and undermine government counter-terrorism efforts, particularly Operation Hadin Kai (UNDP, 2019). The insurgents' use of regional languages, encrypted communication channels, and culturally resonant messaging has further enhanced the effectiveness of their online campaigns, making detection and intervention challenging for security agencies.

According to Risius et al. (2023), the rapid dissemination of extremist propaganda on social media can create an information cascade, whereby repeated exposure to such content can lead

individuals to perceive extremist narratives as mainstream, thereby lowering the psychological barriers to radicalization. The abduction of the Chibok schoolgirls videos shared online provided incontrovertible evidence of the kidnappings, that amplified the global reach of their actions (Okeowo, 2014). The persuasive tactics employed by terrorist organizations indicates that their digital content frequently utilizes cultural and religious symbolism that resonates with specific target groups. This strategic use of symbolism enhances the appeal of recruitment efforts and deepens ideological commitment among potential recruits (Braddock, 2020).

Ogbondah and Agbese (2018) observe that radical groups and extremist organizations, such as ISIS, al-Qaeda, Hamas, Boko Haram, and the Islamic State West Africa Province (ISWAP), exhibit a sophisticated understanding of the unique characteristics of social media, which they leverage to influence public opinion and secure resources. This phenomenon is consistent with Benson's (2016) argument that social media provides extremist groups with virtual sanctuaries, enabling them to transcend geographic boundaries, establish transnational networks, and mobilize support and coordinate actions with minimal reliance on physical infrastructure. Since 2010,

Despite the recognized threat, social media also presents opportunities for counter-terrorism. Governments, security agencies, and civil society can utilize these platforms for intelligence gathering, dissemination of counter-narratives, early warning, and community engagement. However, scholars note that the effective use of social media for counter-terrorism is constrained by technological, legal, and ethical considerations, including encryption, privacy rights, and the risk of overreach that may alienate communities (Downing, 2023; Kumar, 2023). In summary, the literature reveals a complex, bidirectional relationship between social media and terrorism. While terrorist groups exploit digital platforms to advance operational and ideological objectives, the same platforms can be harnessed by state and non-state actors to disrupt extremism, provided that counter-terrorism strategies are contextually grounded, technologically adept, and ethically sound. In the North-East Nigerian context, understanding this dynamic is particularly crucial for enhancing the effectiveness of Operation Hadin Kai and other complementary non-kinetic measures.

Counter-Terrorism and Military Operations in the Digital Age

The digital age has fundamentally transformed the landscape of counter-terrorism, creating both opportunities and challenges for military operations worldwide. Traditional kinetic approaches, which rely primarily on physical force and territorial control, are increasingly

insufficient to address the complex, ideologically driven, and networked nature of modern terrorist organizations. Social media and other digital technologies have become central to both terrorist operations and counter-terrorism strategies, requiring military and security agencies to adopt integrated approaches that combine physical, informational, and cyber dimensions (Schmid, 2021; Downing, 2023).

In Nigeria, counter-terrorism efforts have traditionally emphasized military-led operations, with Operation Hadin Kai serving as the cornerstone of the federal government's campaign against Boko Haram and ISWAP in North-East Nigeria. Launched in 2015, the operation aimed to reclaim territory, dismantle insurgent networks, and restore security in Borno State and surrounding areas (UNDP, 2019). While Operation Hadin Kai has achieved significant successes in weakening insurgent capabilities, the persistence of attacks, propaganda dissemination, and recruitment activities highlights the limitations of a purely kinetic approach. Terrorist groups continue to exploit social media to coordinate operations, recruit youth, and influence public perception, illustrating the growing importance of digital engagement as a complementary aspect of military strategy (Chukwuere & Onyebukwa, 2018).

In the Nigerian context, scholars note that while Operation Hadin Kai has integrated some level of digital intelligence and psychological operations, the lack of specialized capacity, inter-agency coordination, and strategic use of social media for non-kinetic purposes undermines the full potential of counter-terrorism operations (Nyadera et al., 2019). Furthermore, the misuse or overreach of digital monitoring can exacerbate public distrust, potentially fueling support for insurgents or undermining community cooperation.

Thus, the literature underscores the necessity of adapting military counter-terrorism strategies to the realities of the digital age, where success depends not only on kinetic operations but also on the strategic exploitation of social media for intelligence, propaganda countermeasures, and public engagement. In the case of Operation Hadin Kai, leveraging social media effectively is essential for complementing physical operations, shaping narratives, and mitigating the influence of Boko Haram and ISWAP in North-East Nigeria.

Theoretical Framework

The theoretical framework for this study draws on Information Warfare Theory to analyze the role of social media in counter-terrorism operations, particularly in the context of Operation Hadin Kai in North-East Nigeria. Information Warfare Theory (IWT), first systematically

explored by Martin Libicki (1995), posits that information itself constitutes a critical domain of modern conflict. The theory asserts that in contemporary warfare, controlling, manipulating, and protecting information can be as decisive as conventional military superiority. IWT emphasizes that the acquisition, dissemination, and disruption of information are fundamental instruments for gaining strategic advantage, influencing decision-making, shaping perceptions, and undermining adversaries. The theory identifies several key tenets: the centrality of information as a force multiplier, the strategic value of perception management, the vulnerability of networks to manipulation, and the interplay between offensive and defensive informational operations (Libicki, 1995; Alberts & Hayes, 2003). These principles collectively highlight that success in conflict increasingly depends on the ability to control the narrative, detect and neutralize adversarial messaging, and leverage information channels for operational and psychological advantage.

Applying IWT to the study, social media platforms such as Facebook, X (formerly Twitter), WhatsApp, and Telegram become critical arenas of conflict in counter-terrorism operations. Terrorist organizations like Boko Haram and ISWAP exploit these platforms to propagate extremist ideologies, recruit members, coordinate attacks, and influence both local and global public perceptions. Their sophisticated use of digital content, ranging from propaganda videos to encrypted messaging channels, exemplifies the offensive application of information as outlined in IWT (Schmid, 2021; Conway et al., 2019). Conversely, Nigerian counter-terrorism agencies, through initiatives linked to Operation Hadin Kai, employ non-kinetic information strategies to counteract extremist narratives. These include digital intelligence gathering, dissemination of counter-narratives, real-time public communication, and online monitoring of terrorist networks. By strategically targeting misinformation and manipulating narratives, security agencies attempt to weaken insurgent influence, enhance public confidence, and support operational decision-making.

The adoption of IWT for this study is justified for several reasons. First, the theory directly addresses the central phenomenon under investigation: the strategic use of information, particularly via social media, in both terrorist and counter-terrorism operations. It provides a conceptual lens for analyzing how insurgents in North-East Nigeria exploit digital channels and how state actors can counteract these efforts through integrated information strategies. Second, IWT facilitates a nuanced understanding of the interplay between kinetic and non-kinetic operations, highlighting how information management can amplify the effects of physical military campaigns like Operation Hadin Kai. Third, the theory accounts for the

psychological and perceptual dimensions of conflict, which are critical in contexts where public trust, community cooperation, and online radicalization play significant roles in determining the success or failure of counter-terrorism initiatives.

By applying IWT, this study is able to investigate social media not merely as a communication tool but as a strategic battlefield where information operations influence recruitment, radicalization, and public perception. It also provides a framework for assessing the effectiveness of digital counter-terrorism strategies, including online counter-narratives, intelligence gathering, and public engagement campaigns. The theory's focus on both offensive and defensive information operations aligns with the objectives of the study, which seeks to explore how social media can be leveraged to strengthen counter-terrorism efforts while mitigating the influence of Boko Haram and ISWAP in Borno State. Ultimately, Information Warfare Theory offers both explanatory and practical utility, grounding the study in a robust conceptual foundation that bridges military strategy, digital communication, and counter-terrorism practice.

Research Methodology

This study adopts a descriptive research design with a case study approach, which is appropriate for examining the role of social media in counter-terrorism operations within the specific context of Operation Hadin Kai in North-East Nigeria. A descriptive design enables the researcher to systematically explore, document, and analyze the characteristics, patterns, and relationships of phenomena as they exist in real-life settings (Babbie, 2020). The case study approach further allows for an in-depth understanding of the complex interplay between social media, terrorist networks, and counter-terrorism strategies, offering detailed insights that may not be captured through broader survey-based methods.

The population of this study is considered infinite due to the broad and dynamic scope of social media users and stakeholders involved in counter-terrorism operations in North-East Nigeria, particularly in relation to Operation Hadin Kai. This includes military personnel, counter-terrorism operatives, intelligence officers, cybersecurity experts, policymakers, and members of the general public who interact with social media platforms such as Facebook, X (formerly Twitter), WhatsApp, and Telegram. The infinite population assumption is appropriate because the number of potential interactions, posts, messages, and digital engagements related to

counter-terrorism and terrorist propaganda is unbounded and constantly evolving, making it impossible to enumerate every individual or data point (Kothari, 2019).

Given that the population of this study is considered infinite due to the dynamic nature of social media interactions and the multi-agency composition of Operation Hadin Kai, a sample was drawn to obtain representative and manageable data for analysis. To determine the sample size, the study uses the Cochran (1963) formula, which is appropriate for research involving large or infinite populations:

$$n_0 = \frac{Z^2 \cdot p \cdot q}{e^2}$$

Where:

- n_0 = desired sample size
- Z = standard normal deviate at 95% confidence level (1.96)
- p = estimated proportion of an attribute present in the population (0.5 for maximum variability)
- q = 1 − p (0.5)
- e = desired level of precision or margin of error (0.05)

Substituting the values:

$$n_0 = \frac{(1.96)^2 \cdot 0.5 \cdot 0.5}{(0.5)^2}$$

$$n_0 = \frac{3.8416 \cdot 0.25}{(0.5)^2}$$

$$n_0 = \frac{0.9604}{0.0025}$$

$$n_0 = 384.16$$

$$n_0 = 384$$

The study employs a mixed-method approach to data analysis, integrating descriptive statistical methods for quantitative data and content analysis for qualitative data. This approach allows

for a comprehensive examination of how social media is leveraged in counter-terrorism operations, particularly in the context of Operation Hadin Kai in North-East Nigeria.

Data Presentation and Analysis

Analysis of Objective One

Examine the patterns and methods through which terrorist groups in Borno State utilize social media platforms for propaganda dissemination, recruitment, and the undermining of Operation Hadin Kai.

Table 1: Patterns and Methods of Social Media Utilization by Terrorist Groups in Borno State

Statement	1 (SD)	2 (D)	3 (N)	4 (A)	5 (SA)	Mean	Remark
Terrorist groups use social media to disseminate propaganda	8 (2.2%)	14 (3.9%)	32 (9.0%)	142 (39.9%)	160 (45.0%)	4.18	High
Social media is used to recruit new members into Boko Haram/ISWAP	6 (1.7%)	12 (3.4%)	28 (7.9%)	154 (43.3%)	156 (43.8%)	4.21	High
Terrorist groups exploit social media to coordinate attacks	10 (2.8%)	16 (4.5%)	34 (9.6%)	140 (39.3%)	156 (43.8%)	4.11	High
Social media undermines the effectiveness of Operation Hadin Kai	12 (3.4%)	18 (5.1%)	40 (11.2%)	138 (38.8%)	148 (41.6%)	4.00	High
Terrorist use of encrypted social media platforms hinders monitoring	14 (3.9%)	20 (5.6%)	36 (10.1%)	136 (38.2%)	150 (42.1%)	3.98	High

Source: Field Survey (2025)

Table 1 reveals that terrorist groups in Borno State extensively exploit social media platforms for both operational and ideological purposes. Respondents largely agreed that social media serves as a crucial medium for propaganda dissemination, recruitment, operational coordination, and the undermining of counter-terrorism efforts such as Operation Hadin Kai.

These findings align with global and regional studies which show that digital platforms have become central tools in modern insurgencies, allowing extremist groups to spread narratives, influence public perception, and expand their reach beyond physical territories.

The data further indicate that social media is widely used by terrorist groups for propaganda and recruitment. Respondents strongly agreed that platforms such as Facebook, Telegram, and YouTube enable extremist organizations to disseminate persuasive content that justifies violence and reinforces ideological identity. In the Nigerian context, Boko Haram and ISWAP have adapted these strategies by producing propaganda materials in local languages and targeting vulnerable populations, particularly unemployed and marginalized youth. This highlights the effectiveness of social media as a recruitment tool, as it allows insurgent groups to exploit socio-economic grievances, psychological vulnerabilities, and identity-based narratives.

In addition, respondents agreed that social media facilitates coordination of terrorist activities and undermines the effectiveness of Operation Hadin Kai. Encrypted messaging platforms such as WhatsApp and Telegram provide channels for insurgents to plan operations and communicate across dispersed networks, making detection more difficult for security agencies. At the same time, online propaganda can weaken public trust in government counter-terrorism operations by portraying security forces negatively. The widespread use of encryption further complicates monitoring efforts, creating a persistent tension between the need for effective intelligence gathering and the protection of privacy and civil liberties.

Additionally, Key Informant Interview (KII) narratives are presented below to compliment the findings of the data presented in Table 5.3.

In an interview, a senior military officer involved in Operation Hadin Kai explained:

> Boko Haram and ISWAP have become very sophisticated in how they use social media. They do not just post messages, they produce videos, audios, and graphics designed to intimidate the public, glorify their operations, and undermine the morale of security forces. These materials reach a wide audience and are shared rapidly, making it difficult for us to counter their narratives in real-time. (Personal Interview, 2025)

This narrative underscores the quantitative finding that a majority of respondents perceive social media as a primary channel for terrorist propaganda. It also highlights the operational challenges faced by security forces in countering extremist messaging.

Furthermore, a cyber-security analyst working with the Joint Task Force noted:

> We have observed that many young people, particularly unemployed youths, are targeted online through WhatsApp groups, Telegram channels, and other platforms. They are often drawn by promises of financial incentives, social identity, or religious justification. Social media allows terrorists to reach individuals we cannot easily access in rural or isolated areas. (Personal Interview, 2025)

This observation complements the survey result showing high agreement (Mean = 4.21) on social media's role in recruitment. It emphasizes the psychological and socio-economic factors that terrorist groups exploit online.

A counter-terrorism intelligence officer highlighted:

> Encrypted messaging apps have become essential for insurgents to coordinate attacks. Even when we intercept some communications, they often use coded language or private groups, which makes it challenging to track their operations. Social media is now both a battlefield and a logistics tool for terrorists. (Personal Interview, 2025)

This supports the survey finding that social media is used to coordinate attacks (Mean = 4.11). It demonstrates how digital communication extends the operational reach of terrorist groups beyond the physical battlefield.

A local community liaison officer observed:

> Some propaganda campaigns online actively portray military operations as oppressive or unjust. This not only discourages civilians from cooperating with security forces but sometimes even instigates sympathy for the insurgents. Social media has, unfortunately, become a tool for

psychological warfare against our counter-insurgency operations. (Personal Interview, 2025)

This narrative aligns with the survey result (Mean = 4.00) showing that social media activities undermine the effectiveness of Operation Hadin Kai, confirming that public perception and information control are critical elements in counter-terrorism strategy.

Analysis of Objective Two

Assess the extent to which Operation Hadin Kai integrates social media into its counter-terrorism operations for intelligence gathering, strategic communication, and counter-narrative dissemination.

Table 2: Integration of Social Media into Operation Hadin Kai

Statement	1 (SD)	2 (D)	3 (N)	4 (A)	5 (SA)	Mean	Remark
Social media is effectively used for intelligence gathering	10 (2.8%)	18 (5.1%)	42 (11.8%)	148 (41.6%)	138 (38.8%)	4.14	High
Social media platforms are used to disseminate counter-narratives	12 (3.4%)	20 (5.6%)	38 (10.7%)	150 (42.1%)	136 (38.2%)	4.09	High
Operation Hadin Kai uses social media for strategic communication with communities	14 (3.9%)	22 (6.2%)	36 (10.1%)	140 (39.3%)	144 (40.4%)	4.05	High
Social media enhances coordination between military and intelligence units	16 (4.5%)	24 (6.7%)	34 (9.6%)	142 (39.9%)	140 (39.3%)	4.02	High
Training is provided for personnel on the use of social media in operations	18 (5.1%)	28 (7.9%)	40 (11.2%)	136 (38.2%)	134 (37.6%)	3.93	Moderate

Source: Field Survey (2025)

Table 2 assessed the extent to which Operation Hadin Kai integrates social media into its counter-terrorism operations, focusing on intelligence gathering, strategic communication,

counter-narrative dissemination, inter-agency coordination, and personnel training. The descriptive results show that respondents generally believe social media is actively used across these operational areas. Overall agreement among respondents suggests that digital platforms are becoming embedded in modern security practices. However, the findings also reveal certain limitations, particularly in structured training for personnel. These results align with broader scholarly evidence that security institutions worldwide are increasingly incorporating digital technologies into counter-terrorism frameworks, although the effectiveness of such integration varies depending on institutional capacity and strategic implementation.

The results indicate that social media plays a particularly significant role in intelligence gathering and strategic communication within Operation Hadin Kai. A strong majority of respondents (about 80.4%) agreed that social media is effectively used for intelligence purposes, reflecting the growing reliance on open-source intelligence (OSINT) to track extremist communications, monitor recruitment networks, and understand evolving threat dynamics. Respondents also agreed that social media is used to disseminate counter-narratives and strengthen communication between the military and local communities. These functions help challenge extremist propaganda, provide accurate information about security operations, and build trust with civilians, which is essential in conflict-affected regions such as North-East Nigeria.

The findings further show that social media contributes to improved coordination among military and intelligence units by facilitating rapid information sharing and operational collaboration. Digital communication tools allow agencies to synchronize responses, exchange intelligence, and support decision-making in dynamic security environments. Nevertheless, the relatively lower rating for training highlights a gap in the institutional capacity to fully exploit social media tools. Without systematic training and professional development, personnel may lack the necessary skills to analyze online data, manage digital communication strategies, or handle ethical considerations related to social media use. Overall, the results suggest that while social media has become an important component of contemporary counter-terrorism operations, its full potential depends on strengthening training, coordination, and institutional readiness.

To complement the findings above, the KII narratives are presented as follows:

A senior intelligence officer involved in Operation Hadin Kai explained:

> Social media is now a core part of our intelligence cycle. We monitor open platforms like Facebook, X, and Telegram for extremist content, track recruitment patterns, and identify potential threats. Without digital intelligence, we would be blind to much of the insurgents' activities, especially in remote areas where physical surveillance is difficult. (Personal Interview)

This aligns with the quantitative finding (Mean = 4.14) that respondents perceive social media as effectively integrated for intelligence purposes, highlighting its role as a low-cost, wide-reaching intelligence tool.

A communication officer noted:

> We actively use social media to push counter-narratives to communities affected by Boko Haram. Our campaigns aim to challenge extremist messaging and provide factual information on security operations. It's about winning hearts and minds as much as it is about disrupting their networks. (Personal Interview)

This narrative supports the survey result (Mean = 4.09) indicating that counter-narrative dissemination is a key function of social media in Operation Hadin Kai, reinforcing the need for strategic messaging alongside military operations.

A community liaison officer stated:

> Social media allows us to reach communities directly with safety advisories and operational updates. People are more responsive when they get timely information online, which also builds trust and encourages cooperation with our forces. (Personal Interview)

This reinforces the quantitative finding (Mean = 4.05) that social media facilitates engagement with local communities, critical for both intelligence collection and public support.

A digital operations officer observed:

> We have joint WhatsApp and Telegram groups that link military, intelligence, and civilian units. These groups enable real-time coordination and quick sharing of actionable intelligence. It reduces delays and ensures that everyone is on the same page during field operations. (Personal Interview)

This aligns with the survey outcome (Mean = 4.02) on the use of social media for coordination, demonstrating how digital tools strengthen operational integration across diverse agencies involved in counter-terrorism.

Analysis of Objective Three

Identify the technological, institutional, legal, and ethical challenges constraining the effective use of social media in supporting Operation Hadin Kai's counter-terrorism objectives in Borno State.

Table 3: Challenges Constraining the Use of Social Media in Operation Hadin Kai

Statement	1 (SD)	2 (D)	3 (N)	4 (A)	5 (SA)	Mean	Remark
Limited technological infrastructure and internet access hinder monitoring of terrorist activities	12 (3.4%)	18 (5.1%)	36 (10.1%)	148 (41.6%)	142 (39.9%)	4.08	High
Insufficient training for personnel in social media intelligence and digital tools	14 (3.9%)	22 (6.2%)	38 (10.7%)	140 (39.3%)	142 (39.9%)	4.01	High
Lack of institutional coordination between military, intelligence, and civilian agencies	16 (4.5%)	26 (7.3%)	36 (10.1%)	138 (38.8%)	140 (39.3%)	3.97	High
Legal limitations restrict surveillance and monitoring of social media platforms	18 (5.1%)	28 (7.9%)	40 (11.2%)	136 (38.2%)	134 (37.6%)	3.92	High
Ethical concerns regarding privacy, civil liberties, and data protection constrain operational activities	20 (5.6%)	30 (8.4%)	38 (10.7%)	132 (37.1%)	136 (38.2%)	3.88	High

Source: Field Survey (2025)

Table 3 examined respondents' perceptions of the technological, institutional, legal, and ethical challenges that limit the effective use of social media in supporting Operation Hadin Kai's counter-terrorism efforts in Borno State. The findings indicate that although social media is recognized as an important tool for modern counter-terrorism, several interconnected constraints reduce its operational effectiveness. Respondents identified issues relating to infrastructure, training, coordination, and regulatory frameworks as key barriers. These challenges reflect patterns identified in global and regional research, which show that digital counter-terrorism initiatives often struggle when technological capacity and institutional preparedness are insufficient.

Technological limitations emerged as the most prominent challenge, with a majority of respondents identifying unstable internet connectivity, outdated monitoring software, and inadequate analytical tools as significant obstacles. In conflict-affected regions such as North-East Nigeria, inconsistent power supply and weak broadband coverage further limit real-time monitoring and analysis of online extremist activity. Respondents also emphasized inadequate training of personnel as a major constraint, noting that security officials often lack the specialized skills required to analyze social media data, detect online threats, and deploy effective counter-narratives. In addition, poor coordination among military, intelligence, and civilian agencies was highlighted as another barrier, as bureaucratic structures and unclear operational protocols can slow the exchange of digital intelligence and hinder timely responses.

Legal and ethical concerns were also identified as important constraints on the use of social media for counter-terrorism operations. Respondents noted that national laws, privacy regulations, and the need to respect civil liberties can limit the extent to which security agencies monitor online platforms. Ethical considerations, including data privacy and the potential misuse of surveillance tools, further complicate digital security operations and may undermine public trust if not carefully managed. Overall, the findings suggest that the challenges affecting social media integration in Operation Hadin Kai are multi-dimensional and interconnected. Addressing these issues will require improved technological infrastructure, enhanced training for personnel, stronger inter-agency collaboration, and balanced legal frameworks that support security objectives while protecting fundamental rights.

Additionally, KII narratives are presented to complement the findings of the data presented above. A senior intelligence analyst involved in Operation Hadin Kai stated:

> One of the biggest problems we face is infrastructure. Many rural areas have poor internet connectivity, and our monitoring tools are often outdated. Even when we try to track insurgent activity online, slow networks and limited software capabilities make it difficult to respond quickly. (Personal Interview, 2025)

This narrative corroborates the survey finding (Mean = 4.08) that technological limitations, including inadequate internet access, outdated software, and low analytic capacity, significantly constrain the effective use of social media in counter-terrorism.

A digital operations officer observed:

> Not all personnel are equipped to handle digital intelligence. Some lack basic skills to analyze online data or identify extremist networks. We need continuous training to keep up with evolving tactics, but current programs are insufficient and sporadic. (Personal Interview, 2025)

This supports the finding (Mean = 4.01) that insufficient training of personnel is a critical challenge, highlighting the need for structured capacity-building initiatives to optimize the use of social media for counter-terrorism operations.

A military operations planner noted:

> Coordination between different units, military, intelligence, and civilian agencies, is often complicated. We have multiple platforms for sharing information, but bureaucracy and unclear roles sometimes slow down decision-making. Social media data could be more useful if we had streamlined communication protocols. (Personal Interview, 2025)

This aligns with the survey result (Mean = 3.97) that institutional and inter-agency silos hinder timely sharing of intelligence and operational integration, reducing the overall efficiency of Operation Hadin Kai's social media strategy.

Analysis of Objective Four

Propose context-specific and ethically grounded social media strategies capable of strengthening non-kinetic counter-terrorism operations and complementing Operation Hadin Kai in Borno State.

Table 4: Strategic Measures for Enhancing Social Media Use in Operation Hadin Kai

Statement	1 (SD)	2 (D)	3 (N)	4 (A)	5 (SA)	Mean	Remark
Development of context-specific counter-narrative campaigns targeting vulnerable populations	10 (2.8%)	14 (3.9%)	32 (9.0%)	150 (42.1%)	150 (42.1%)	4.18	High
Training of personnel on ethical and effective use of social media tools	12 (3.4%)	18 (5.1%)	34 (9.6%)	142 (39.9%)	150 (42.1%)	4.14	High
Collaboration with social media companies to monitor and remove extremist content	14 (3.9%)	20 (5.6%)	36 (10.1%)	140 (39.3%)	146 (41.0%)	4.09	High
Use of social media to engage communities and build public trust in security operations	16 (4.5%)	22 (6.2%)	34 (9.6%)	138 (38.8%)	146 (41.0%)	4.05	High
Continuous evaluation and adaptation of social media strategies to evolving terrorist tactics	18 (5.1%)	24 (6.7%)	40 (11.2%)	136 (38.2%)	138 (38.8%)	3.99	High

Source: Field Survey (2025)

Table 4 examines respondents' perspectives on strategic measures that could strengthen the integration of social media in supporting Operation Hadin Kai in Borno State. The findings indicate broad agreement that structured and multi-dimensional strategies are necessary to enhance the effectiveness of social media in counter-terrorism operations. Respondents emphasized that improvements in personnel capacity, technological infrastructure, legal and

ethical guidelines, inter-agency collaboration, and community engagement are key components of effective digital counter-terrorism. These views align with broader research highlighting that modern counter-terrorism increasingly requires comprehensive approaches that combine technological tools with institutional readiness and public cooperation.

A major recommendation from respondents is the need for regular training and skill development for personnel responsible for digital intelligence operations. The majority agreed that strengthening human capacity is essential for effectively monitoring social media, identifying extremist networks, and developing counter-narratives. In addition, respondents highlighted the importance of upgrading technological infrastructure, including advanced monitoring software, data analytics tools, and secure communication systems. Improved technological capacity would enable security agencies to detect extremist activities more efficiently, analyze digital information in real time, and respond quickly to emerging threats.

Respondents also stressed the need for clear ethical and legal frameworks to guide social media use in counter-terrorism operations, ensuring that surveillance and digital engagement respect privacy rights and maintain public trust. Stronger coordination between military, intelligence, and civilian agencies was identified as another key strategy, as integrated information-sharing systems can improve the speed and effectiveness of operational responses. Finally, the findings highlight the value of community engagement and public awareness through social media platforms, which can help counter extremist narratives, encourage information sharing, and strengthen local resilience against radicalization. Overall, the results suggest that a balanced approach combining human capacity development, technological advancement, institutional cooperation, and community participation is essential for maximizing the role of social media in supporting Operation Hadin Kai's counter-terrorism efforts.

Furthermore, below are the Key Informant Interview (KII) narratives to complement objective four: propose context-specific and ethically grounded social media strategies capable of strengthening non-kinetic counter-terrorism operations and complementing Operation Hadin Kai in Borno State.

A senior digital intelligence officer involved in Operation Hadin Kai stated:

> Our officers need regular and structured training to understand the dynamics of social media. Terrorists are constantly evolving their tactics online, and unless we build

> our capacity to monitor, analyze, and counter their activities, we will always be a step behind. (Personal Interview, 2025)

This emphasizes the need for continuous skill development as a core strategic measure, aligning with Table 5.6's finding (Mean = 4.21) that personnel competence is critical for effective social media integration in counter-terrorism.

A cybersecurity specialist noted:

> Investing in advanced analytic tools and secure communication systems is essential. We need software capable of processing large volumes of data from multiple platforms, detecting extremist content in real-time, and generating actionable intelligence for field operations. (Personal Interview, 2025)

This supports the survey finding (Mean = 4.18) that technological upgrades are central to strengthening Operation Hadin Kai's social media capabilities. Secondary literature highlights similar practices globally, where AI-driven monitoring and predictive analytics enhance operational readiness (Kumar, 2023).

A legal advisor commented:

> Any strategy must be ethically and legally sound. Monitoring social media should protect national security without infringing on civil liberties. Clear protocols help maintain public trust while ensuring that our actions are defensible under national and international law. (Personal Interview, 2025)

This reflects the 80.7% agreement in Table 5.6 that codified ethical and legal frameworks are necessary for sustainable social media use in counter-terrorism, reinforcing the need to balance security imperatives with human rights (Downing, 2023).

A military operations coordinator stated:

> We must ensure that intelligence gathered from social media is shared quickly and efficiently across all units. Establishing joint platforms and protocols for real-time communication can reduce delays and improve operational coordination. (Personal Interview, 2025)

This supports the finding (Mean = 4.05) emphasizing inter-agency collaboration as a strategic measure, consistent with studies showing that coordinated digital operations enhance the impact of non-kinetic counter-terrorism efforts (Richards, 2021).

Discussion of Major Findings

The analysis of data from both the survey and key informant interviews reveals several critical insights regarding the role of social media in supporting Operation Hadin Kai and counter-terrorism operations in Borno State. First, the study confirms that terrorist groups in the North-East extensively leverage social media platforms for propaganda dissemination, recruitment, and operational coordination. Table 5.3 highlighted that platforms such as Facebook, X (formerly Twitter), YouTube, and Telegram are used to spread extremist ideologies and mobilize sympathizers, which aligns with global trends where terrorist organizations exploit the accessibility, reach, and relative anonymity of social media to influence vulnerable populations (Schmid, 2021; Jain & Vaidya, 2020). The KII narratives reinforced this, indicating that the insurgents' digital sophistication poses significant challenges for conventional military operations, necessitating a shift toward non-kinetic strategies.

Second, the findings demonstrate that Operation Hadin Kai has integrated social media into its counter-terrorism framework, particularly for intelligence gathering, counter-narrative dissemination, strategic communication, and inter-agency coordination (Table 5.4). Respondents noted that monitoring extremist content on social media allows for timely identification of threats, enhances situational awareness, and strengthens operational responsiveness. These findings resonate with global and regional studies, which show that open-source intelligence (OSINT) and digital communications are essential for contemporary counter-terrorism operations (Steinert, 2020; Conway et al., 2019).

Third, the study identifies a range of challenges constraining social media utilization in Operation Hadin Kai, as shown in Table 5.5. Technological limitations, inadequate training, weak inter-agency coordination, legal restrictions, and ethical concerns were consistently

highlighted by respondents and KII participants. These findings corroborate secondary literature emphasizing that digital counter-terrorism is complex and requires addressing both human and institutional factors (Brown & Douglass, 2022; Kumar, 2023). Specifically, legal and ethical dilemmas, including privacy rights and community trust, emerge as critical considerations that can influence operational effectiveness and public perception.

Finally, the study reveals that strategic measures, focusing on capacity building, technological upgrades, clear legal-ethical frameworks, improved inter-agency collaboration, and community-oriented counter-narratives, can significantly enhance social media's contribution to Operation Hadin Kai (Table 5.6). KII narratives stressed that sustained personnel training, investment in analytic tools, and culturally sensitive engagement strategies are vital to maximizing the operational impact of non-kinetic measures. These insights are consistent with both global best practices and African case studies, which show that social media is most effective when integrated strategically, ethically, and collaboratively into counter-terrorism operations (Okoro & Erukwuro, 2021; UNDP, 2019).

Conclusion

The study concludes that context-specific, non-kinetic strategies leveraging social media can substantially strengthen Operation Hadin Kai and broader counter-terrorism initiatives. By integrating personnel training, technological upgrades, ethical frameworks, inter-agency collaboration, and community-focused counter-narratives, security agencies can mitigate the influence of extremist groups while fostering public trust. Social media, when strategically managed, thus represents a complementary and indispensable tool that enhances operational intelligence, communication, and the overall effectiveness of counter-terrorism interventions in North-East Nigeria.

Recommendations

Based on the findings and analysis of this study, the following recommendations are proposed to enhance the strategic use of social media in supporting Operation Hadin Kai and broader counter-terrorism efforts in Borno State:

i. Operation Hadin Kai should institutionalize the use of social media for real-time intelligence gathering, threat monitoring, and dissemination of culturally sensitive counter-narratives to disrupt extremist propaganda and recruitment.

ii. Security personnel should receive continuous, structured training on digital intelligence, social media monitoring, and ethical use of online platforms to ensure effective non-kinetic operations.

iii. The Nigerian government should invest in advanced digital tools, data analytics software, and secure communication systems to enable timely detection of extremist activity and enhance operational coordination across agencies.

iv. Clear policies and ethical guidelines should be developed to govern the use of social media in counter-terrorism, balancing operational effectiveness with privacy, civil liberties, and public trust.

v. Establish joint platforms for information sharing among military, intelligence, and civilian units, while using social media to engage local communities and raise awareness about counter-terrorism initiatives, fostering cooperation and resilience against radicalization.

References

Adeeb, N., & Mirhoseini, S. (2023). Social media risks, misinformation, and psychological impacts on youth in the digital age.

Adesola, A., et al. (2024). Structural drivers of terrorism and insurgency in Nigeria.

Alberts, D. S., & Hayes, R. E. (2003). Power to the Edge: Command and Control in the Information Age. Washington, DC: Department of Defense.

Asongu, S., Nwachukwu, J., & Tchamyou, V. (2019). Information technology and terrorism dynamics in Africa.

Babbie, E. (2020). The Practice of Social Research (15th ed.). Boston: Cengage Learning.

Bappah, H. Y. (2016). Regional security cooperation and counter-terrorism in West Africa: The role of the Multinational Joint Task Force.

Benigni, M. C., Joseph, K., & Carley, K. M. (2017). Online extremism and the role of social media in terrorist recruitment and propaganda.

Benson, D. (2016). Social media and the transformation of extremist communication networks.

Braddock, K. (2020). Weaponized words: The strategic role of propaganda in terrorist recruitment.

Brown, T., & Douglass, K. (2022). Digital infrastructure and counter-terrorism in Africa.

Byman, D. (2019). Road Warriors: Foreign Fighters in the Armies of Jihad. Oxford University Press.

Chukwuere, J., & Onyebukwa, C. (2018). The use of social media in terrorism and counter-terrorism in Nigeria.

Cochran, W. G. (1963). Sampling Techniques (2nd ed.). New York: John Wiley & Sons.

Connor, P. (2020). Youth radicalization and online recruitment strategies in extremist movements.

Conway, M., Scrivens, R., & Macnair, L. (2019). Right-wing extremists' persistent online presence: History and contemporary trends.

De Oliveira Santini, R., et al. (2020). Social media and digital advertising dynamics in global communication networks.

Downing, S. (2023). Digital counter-terrorism strategies and the role of online communication platforms.

Hartley, J. (2023). Community engagement and resilience in counter-terrorism strategies.

Jain, A., & Vaidya, R. (2020). Social media, radicalization, and counter-terrorism strategies.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. Business Horizons, 53(1), 59–68.

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in social media research: Past, present and future. Information Systems Frontiers, 20, 531–558.

Kent, M. L., & Taylor, M. (2021). Dialogic communication and social media: Theory and practice in public relations.

Kothari, C. R. (2019). Research Methodology: Methods and Techniques (Revised ed.). New Delhi: New Age International.

Kumar, S. (2023). Encryption, surveillance, and counter-terrorism in the digital era.

Libicki, M. (1995). What Is Information Warfare? Washington, DC: National Defense University.

Malik, S. (2018). Terrorism and the dark web: Emerging security challenges.

Njoku, E., et al. (2025). Governance challenges and the persistence of terrorism in Nigeria.

Nyadera, I. N., Ndubuisi, C., & Ng'ang'a, M. (2019). The Boko Haram insurgency and state response in Nigeria.

Ogbondah, C., & Agbese, P. (2018). Social media, extremist propaganda, and digital radicalization.

Okeowo, A. (2014). The Chibok girls and the global campaign against Boko Haram. The New Yorker.

Okoro, N., & Erukwuro, C. (2021). Counter-narratives and digital engagement in African counter-terrorism initiatives.

Richards, A. (2021). Inter-agency collaboration in contemporary counter-terrorism operations.

Risius, M., et al. (2023). Information cascades and online radicalization in digital communication networks.

Schmid, A. P. (2021). Handbook of Terrorism Prevention and Preparedness. The Hague: International Centre for Counter-Terrorism.

Steinert, J. (2020). Open-source intelligence and social media analysis in modern security operations.

UNDP. (2019). Journey to Extremism in Africa: Drivers, Incentives and the Tipping Point for Recruitment. United Nations Development Programme.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151.

Walker, M., & Masta, A. (2021). Social media as a primary source of news in the digital age.

Wilson Sonsini. (2022). The European Union Digital Services Act: Implications for online content regulation.