HORN INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

KONRAD ADENAUER STIFTUNG

STUDY REPORT

Jihadi Diaspora: Online Radicalisation, Mobilisation and Terrorist Financing in Eastern Africa

November 2026

www.kas.de/en/web/sipodi-east
www.horninstitute.org

KONRAD
ADENAUER
STIFTUNG

Konrad Adenauer Stiftung

REGIONAL PROGRAMME
SECURITY DIALOGUE FOR EAST AFRICA

24, Kololo Hill Lane, Kololo
P.O. Box 647, Kampala, Uganda

Email: sipodi.east@kas.de
www.kas.de/en/web/sipodi-east

Acknowledgements

HORN International Institute for Strategic Studies (hereafter HORN Institute) gratefully acknowledges the individuals and institutions that contributed to this research, undertaken in partnership with the Konrad-Adenauer-Stiftung Regional Programme Security Dialogue for East Africa (KAS-RP SIPODI EA). Special appreciation goes to the researchers, academics, security and P/CVE practitioners, journalists, community researchers, civil society representatives, and other professionals who shared their expertise. The Institute also recognises the leadership, the HORN research team led by Edmond Pamba (Lead), Jeremy Oronje, Bravin Onditi and HORN staff especially Evans Ombisa and Husna Maalim who were involved in the design and layout of info-graphics.

The views expressed in this report reflect collected data and analysis and do not necessarily represent the official positions of all participating individuals, institutions, or partner organisations.

Abbreviations and Acronyms

ADF	Allied Democratic Forces
ADL	Anti-Defamation League
AI	Artificial Intelligence
AML/CTF	Anti-Money Laundering/Combating the Financing of Terrorism
AMYC	Ansaar Muslim Youth Centre
AQAP	Al-Qaeda in the Arabian Peninsula
ASWJ	Ahlu Sunnah Wal Jama'a (Ansar al-Sunnah)
BfV	Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
CAIR	Council on American-Islamic Relations
CTED	United Nations Counter-Terrorism Committee Executive Directorate
DRC	Democratic Republic of the Congo
ETH	Eidgenössische Technische Hochschule (Swiss Federal Institute of Technology)
EU	European Union
FATF	Financial Action Task Force
GDP	Gross Domestic Product
GIFiM	Gabinete de Informação Financeira de Moçambique (Financial Intelligence Office of Mozambique)
GNET	Global Network on Extremism and Technology
HOSSP	Hawala and Other Similar Service Providers
ICSR	International Centre for the Study of Radicalisation and Political Violence
ID	Identification Document
IEMed	European Institute of the Mediterranean
INSS	Institute for National Security Studies
IS	Islamic State
ISCAP	Islamic State Central Africa Province
ISD	Institute for Strategic Dialogue
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria

IS-S	Islamic State in Somalia
IVT	Informal Value Transfer
KAS-RP SIPODI EA	Konrad-Adenauer-Stiftung Regional Programme Security Dialogue for East Africa
KII	Key Informant Interview
KYC	Know Your Customer
MoU	Memorandum of Understanding
MTO	Money Transfer Operator
NFD	Northern Frontier District
NPO	Non-Profit Organisation
P/CVE	Preventing/Countering Violent Extremism
RSF	Rapid Support Forces
SAF	Sudan Armed Forces
TE-SAT	European Union Terrorism Situation and Trend Report
TVEC	Terrorist and Violent Extremist Content
UK	United Kingdom
UN	United Nations
U.S.	United States of America
USDT	Tether (U.S.-dollar stablecoin)
VASP	Virtual Asset Service Provider
VEO	Violent Extremist Organisation

Executive Summary

This study was informed by the increasing role of diaspora extremists based in Europe and North America in the virtualisation of jihadist radicalisation, mobilisation and terrorist financing in Eastern Africa. The study thus generates evidence-based, policy-relevant understanding on diaspora-linked online radicalisation, mobilisation, and terrorist financing affecting the trends and patterns of violent extremism in Eastern Africa. Specifically, it maps extremist narrative ecosystems on social media platforms, traces financial vulnerability pathways for diaspora-linked terrorist financing, and identifies regulatory and enforcement gaps across Europe, North America, and the Horn of Africa.

The study reveals that radicalisation into violent extremism is migrating from physical networks to encrypted digital platforms and transnational diaspora networks. Al-Shabaab remains the primary extremist group associated with diaspora-linked radicalisation, followed by Islamic State offshoots: Allied Democratic Forces (ADF) and Islamic State in Somalia (IS-S). Public-facing platforms particularly TikTok (87.5 per cent), Facebook (81.3 per cent), and X (43.8 per cent), facilitate terrorist and violent extremist content (TVEC) amplification, while encrypted platforms (Telegram, WhatsApp, Element, Signal and Rocket.chat) enable deeper ideological engagement and recruitment. Geopolitical events (Israel-Hamas conflict, regional disputes Ethiopia-Somaliland MoU, Israel's recognition of Somaliland...); inadequate socio-economic opportunities for the youth in home-countries; and poor diaspora integration and inclusion of immigrants in Europe and North America, drive radicalisation. Ineffective platform moderation for African languages and dialects: Swahili, Somali, Oromo, Amharic; informality of remittance networks; and weak financial monitoring mechanisms hamper prevention efforts.

Multi-stakeholder coordination among governments, civil society, religious institutions, and diaspora organisations is critical in curbing diaspora-linked radicalisation online. Governments in Europe and North America should strengthen integration programmes; regulate religious institutions to prevent extremist financing; and develop geopolitical risk monitoring capabilities. Eastern African governments must expand socio-economic opportunities to reduce youth vulnerability. Digital platforms must reform algorithmic recommendation systems; strengthen local-language moderation; and eliminate multiple-account holding. Governments across all jurisdictions should regularise remittance networks; enhance AML/CTF frameworks; and invest in digital literacy programmes in partnership with civil society and social media companies.

Given the transnational nature of modern violent extremism, the rapid youth population growth in Eastern Africa, and weaknesses in regional financial systems, coordinated cross-jurisdictional action is urgently needed. This evidence-based analysis provides strategic interventions to disrupt online radicalisation, terrorist financing, and recruitment pipelines sustaining violent extremist networks between Eastern Africa, Europe, and North America.

Table of Contents

Acknowledgements i
Abbreviations and Acronyms ii
Executive Summary iv

1.0 Introduction 1

1.1 Background 1
1.2 Objectives of the Study 2
1.3 Justification of the Study 3
1.4 Methodology 3
1.5 Limitations of the Study 4

2.0 Literature Review 5

2.1 Diaspora Radicalisation and Role in Violent Extremism 5
2.2 Geopolitics as a Driver of Diaspora Radicalisation 7
2.3 The Digital Front of Diasporic Violent Extremism 10
2.4 Diaspora, Virtual Networks and Terrorist Financing 12
2.5 Governance, Platform Moderation and Regulatory Gaps 15
2.6 Conclusion 16

3.0 Findings 17

3.1 Diaspora Radicalisation and Violent Extremism in Eastern Africa 17
3.2 Diaspora and Social Media Radicalisation 19
3.2.1 Which Platforms Matter Most 19
3.2.2 Platform Function Matters More Than Platform Name 21
3.2.3 Cross-Platform Migration 21
3.2.4 Online Extremist Messaging, Gains, Reach and Resonance 22
25
3.2.5 Vulnerability to Diaspora-Based Online Radicalisation 31

3.3 Terrorist Financing 33
3.3.1 Diaspora-Linked Terrorist Financing 33
3.3.2 Challenges in Curbing Diaspora-Linked Terrorist Financing 36
3.3.3 Platform Moderation: Effectiveness and Gaps 37

4.0 Conclusion and Recommendations 40

4.1 Conclusion 40
4.2 Recommendations 41
✓ **Platform level** 41
✓ **Government level** 41
✓ **Community level** 42
4.3 Principles for an Effective Whole-of-Society Response 43

5.0 Endnotes 44

1.0 Introduction

1.1 Background

The terrorist attacks in the United States of America (U.S.) on 11 September 2001, re-oriented global security around transnational terrorism, of which the Horn of Africa remains one of the world's most acute theatres. The Horn of Africa is engulfed by violent extremist groups including al-Shabaab and Islamic State in Somalia (IS-S) in Somalia, al-Qaeda in the Arabian Peninsula (AQAP) in Yemen, Allied Democratic Forces (ADF) in the Democratic Republic of the Congo (DRC), and Ansar al-Sunnah in Mozambique.[1] Such concentration of extremist violence is primarily attributable to state fragility in Somalia, DRC, and Mozambique; governance challenges and gaps in the region; jihadist networks in Afghanistan, Pakistan and the Middle East; and violent conflicts, which have also displaced populations into Europe, North America and Australia.

Despite the progress made against al-Shabaab in Somalia, ADF in DRC, and Ansar al-Sunnah in Mozambique through multilateral security and stabilisation efforts, violent extremism and terrorism remain a persistent threat not just in the Horn of Africa but to international security. The 2026 Global Terrorism Index identifies Sub-Saharan Africa, not the Middle East or South Asia, as the contemporary epicentre of global terrorism, being home to six of the ten worst-affected states.[2] Apart from the adaptability and resilience these extremist groups have shown over time, the acutely under-investigated trends and patterns reveal the virtualisation of radicalisation, terrorist financing and recruitment, and the role of diaspora sympathisers. Ideological indoctrination, operational guidance and community-building have migrated from physical face-to-face networks into online and encrypted spaces, and the epicentres have similarly shifted from the Horn of Africa to diaspora hubs in Europe and North America.[3]

The digital involvement of the diaspora in extremist radicalisation is two-pronged: (i) extremist groups deliberately target diaspora communities and (ii) diaspora sympathisers mobilise support for extremist groups and other militant causes back in home countries. Al-Shabaab for instance, targets the Somali diaspora communities in the United States of America (U.S.), United Kingdom (UK), Germany, Sweden, Canada, Kenya, Tanzania and Uganda long after the physical foreign-fighter pipelines of the 2007–2013 period had been disrupted.[4] On the other hand, a string of Somali-American recruits travels to join al-Shabaab and Islamic State in Somalia (IS-S). Between 2007 and early 2010s dozens of Somali diaspora members from the United Kingdom (UK), Sweden, Germany, U.S. and Canada travelled back to Somalia for jihadist ambitions.[5]

Similarly, the role of geopolitics is emerging as a structural driver of diaspora-linked online radicalisation and mobilisation. Narrative bridging, the linking of local grievances

(abroad and home countries) to global and regional geopolitical events, including most recently, Israel's recognition of Somaliland, is instrumental for construction of extremist narratives by the extremist diaspora elements and violent extremist organisations (VEOs) in the Horn of Africa.[6] The al-Shabaab group's propaganda for instance routinely fuses local grievances with global Muslim-solidarity and nationalist narratives, into a single register of "defensive jihad" against occupation, betrayal and foreign fragmentation of Muslim lands. The Dusit D2 Complex attack by al-Shabaab in January 2019 in Nairobi was carried out in response to U.S. recognition of Jerusalem as the capital of Israel.[7]

Not only do diaspora extremists radicalise and recruit online, they also raise financial resources from their pool of virtual followers enabled by structurally weak Anti-Money Laundering and Combating of Terrorism Financing (AML/CTF) frameworks globally and across the Horn of Africa. Somalia's formal financial sector, in which mobile money and hawala dominate a 2 billion U.S.-dollars annual remittance market (a fifth to a quarter of the country's gross domestic product – GDP), for instance, remains only partially supervised.[8] Neighbouring countries similarly affected by terrorism and violent extremist radicalisation such as Kenya, Yemen and DRC are grey-listed by the Financial Action Task Force (FATF).[9] This report documents the role of diaspora extremists in Europe and North America, in online mobilisation and radicalisation into violent extremism as well as terrorist financing in Eastern Africa. The report is structured into four main sections: section one is the introduction of the study and methodology, section two covers the literature review, section three presents the findings of the study, and lastly, section four presents the conclusion and the relevant policy recommendations. Horn of Africa and Eastern Africa are used inter-changeably across the report.

Because the study addresses sensitive issues including violent extremism, online radicalisation, diaspora networks, and security, findings should not be interpreted as characterising entire diaspora, migrant, refugee, religious, ethnic, or national communities. The analysis focuses on specific behaviours, narratives, actors, and networks and recognises the diversity and positive contributions of these communities. The study also seeks to balance legitimate security objectives with privacy, freedom of expression, due process, and non-discrimination. Online activity, political criticism, religious expression, migration concerns, or grievances should not in themselves be treated as evidence of radicalisation. Findings are presented for research, policy dialogue, and prevention purposes and should be interpreted considering the study's methodology, sample, and limitations.

1.2 Objectives of the Study

The overarching objective of this study is to generate an evidence-based, policy-relevant understanding on the role of diaspora-linked online radicalisation, mobilisation and terrorist-financing in Eastern Africa's violent extremism.

The specific objectives of the study are to:

- Map and analyse diaspora-linked extremist narrative ecosystems on public social media platforms, associated with extremist groups in Eastern Africa.
- Trace financial vulnerability pathways for diaspora-linked terrorist financing and in Eastern Africa.
- Identify regulatory and enforcement gaps related to online radicalisation and terrorist financing across European countries, the U.S., UK, Canada and Eastern Africa.

1.3 Justification of the Study

The study is of significant policy relevance; it provides independent, evidence-based analysis which can directly inform implementation priorities for regulatory and enforcement frameworks for AML/CTF laws as well as content moderation and disruption online. Additionally, the study underscores the urgency of disrupting the online radicalisation, terrorist financing and recruitment pipelines that sustain violent extremist networks between Eastern Africa, Europe and North America. Given the growing transnationalism of violent extremism, the fast-growing youth population vulnerable to radicalisation in Eastern Africa, the porosity of Eastern African borders, the weaknesses in Kenya's and Somalia's financial systems to money laundering and terrorist financing, and the changing regional and global geopolitical order, the study bears relevance to regional security and stability in the Horn of Africa and Eastern Africa at large. The findings will further strengthen cross-jurisdictional cooperation and collaboration between relevant stakeholders across Europe, North America and Eastern Africa by proffering strategic interventions to this end. Beyond policy, the study enriches the current research on violent extremism and radicalisation by addressing the existing analytical and research gap, which is diaspora-driven online terrorist mobilisation and financing.

1.4 Methodology

The study is an exploratory research; it adopted a mixed-methods design, employing systematic secondary-source and documentary analysis, triangulated with verified quantitative and qualitative primary data collected to strengthen the study's validity through research across multiple data sources. Primary data was collected across Somalia, Kenya, Sudan, the Democratic Republic of the Congo (DRC), Mozambique, Israel, UK and U.S. over a period of two months (July to August 2026). Secondary data sources were identified through a criterion-based selection process, which prioritised publications such as reports published by multilateral and governmental institutions, published research reports by think tanks and security research organisations, peer-reviewed journal articles, and verified media and open-source materials.[10] The mixed-

methods exploratory approach is particularly relevant for this understudied phenomenon, as it captures both the scale and nuance of diaspora-linked radicalisation mechanisms while reflecting the geographically dispersed and complex nature of transnational terrorist financing and online mobilisation pathways.

Primary data was collected using key informant interviews (KIIs) using semi-structured questionnaires. A multidisciplinary sample of 27 respondents was purposively selected across Kenya (eleven), DRC (one), Mozambique (one), South Africa (one), Tanzania (one), Ethiopia (two), U.S. (one), Israel (one), Sudan (three), Somalia (three), UK (one), and Singapore (one). The respondents were drawn from the academia and security research organisations, banks, remittance firms, as well as anti-money laundering and combating the financing of terrorism (AML/CTF) agencies. Digital activists; social media analysts; preventing and countering violent extremism (P/CVE) practitioners; community, youth, religious leaders; and reformed violent extremists, was critical for triangulation purposes. Supplementary multimedia material and 50 accounts on social media were analysed separately as qualitative digital evidence. The quantitative responses were analysed using descriptive frequencies and percentages, while qualitative data was subjected to thematic and cross-case analysis; sentiment analysis was applied to social media material.

This study was conducted with attention to informed consent, confidentiality, responsible data handling, and participant protection. Respondents were informed of the study's purpose and intended use of the information collected, and identifying information was anonymised where confidentiality was required or attribution had not been explicitly authorised.

1.5 Limitations of the Study

Various limitations can be noted; first, the study mainly covers the Eastern African diaspora, hence it does not address radicalisation and extremist associations with the other diaspora communities in Europe, North America, Middle East and the Levant and the larger Eastern Africa. Second, the study does not empirically trace how a given geopolitical trigger event correlates with measurable shifts in diaspora online mobilisation activity and with subsequent financing typologies, and how the differential AML/CTF capacity of Kenya, Somalia, Uganda, Tanzania and Ethiopia shapes where in the region such flows concentrate. Third, the study does not explore the impact of diaspora radicalisation in Europe and North America.

2.0 Literature Review

2.1 Diaspora Radicalisation and Role in Violent Extremism

In the period 1970s to 1990s, transnational violent extremist mobilisation in the Horn of Africa was traditionally driven by Cold War-era proxy conflicts, such as the Soviet-backed Ethiopian–Somali Ogaden War and the Soviet invasion of Afghanistan, as well as physical radicalisation by Wahhabist-Salafist networks in the Middle East.[11] Following the Cold War's end and the rise of the internet and social media in the 1990s, radicalisation began adapting to digital tools and intensified. The post-Cold War internecine conflicts and globalisation-driven migration from conflict-affected, low-income states, such as Somalia, Sudan, the DRC, Afghanistan, Sri Lanka, Indonesia, the Philippines, Middle East, and the former Yugoslavia, to stable, high-income democracies in Western Europe, North America, and Australia, produced large diaspora populations in the latter hubs.

These diasporic communities historically sustained ties to homeland reconstruction and politics, with a minority becoming entangled in conflict, violent extremism and terrorism online and offline.[12] As such, radicalised diaspora individuals have further been driven by political and geopolitical events associated with home countries. Al-Shabaab's October 2023 exploitation of Gaza conflict messaging provides a case study in diaspora targeting: the group leveraged real-time Gaza updates to reinforce narratives of Muslim oppression, thereby widening appeal among diaspora populations in Kenya, Ethiopia, the Middle East, Europe, and North America.[13]

Diaspora communities have historically been prone to religious and separatist radicalisation, and that in the post-Cold War period, Salafi-jihadist ideology became the most significant ideational driver of radicalisation within Muslim diaspora in Western Europe and North America.[14] A recurring sequence is observable among the sections of the radicalised diaspora elements: alienation, susceptibility to indoctrination, re-education, and deployment. European diaspora unlike their North American counterparts, tend to form parallel societies under pressure from both assimilationist demands and host-society marginalisation, a condition that leaves them more exposed to exploitation by radical recruiters.[15]

Somalia, the Horn of Africa's principal epicentre of violent extremism, driven by al-Shabaab's Islamist insurgency, protracted conflict, poverty, and over three decades of state collapse since 1991, maintains a large diaspora community, concentrated in Western Europe, North America, and, regionally, Kenya.[16] The diaspora, estimated at over two million people globally, is anchored by roughly 250,000 in the UK, 170,000 in the U.S. (concentrated in Minneapolis-St. Paul), 66,000 in Sweden, and 63,000 in Canada.[17] It plays a critical role in the reconstruction of Somalia, remitting 1.3 to 1.7 billion U.S.-dollars annually, exceeding Somalia's national budget and combined foreign aid.[18]

The diaspora has also formed much of the country's post-transition political and civil-service leadership. Yet a minority element sustains instability: al-Shabaab, generating an estimated 100 to 200 million U.S.-dollars annually chiefly through extortion and taxation, controls roughly 70 per cent of southern-central Somalia, was linked to 2,553 violent incidents and 6,225 fatalities in a single recent year, and has helped drive Somalia's internal displacement crisis past 3.8 million people.[19] Diaspora-linked online mobilisation, radicalisation, and financing sustain this violence, as well as clan fragmentation and national instability.

While the Somali diaspora communities have generally displayed a significant degree of resistance to radical Islamist appeals relative to other diasporic communities, a shift had struck as early as 2009, following Ethiopia's invasion of Mogadishu in 2006. American citizens of Somali descent started getting involved in the Somali conflict through contact with al-Shabaab, as some of the group's earliest foreign-fighter pipeline could be observed. In this period, Canada similarly experienced the "spill-over effect" of homeland conflicts, with segments of the Somali-Canadian community travelling to Mogadishu (as foreign fighters) to fight for a wide range of national-liberation and jihadist movements, not only al-Shabaab.[20] Between 2006 and 2012, 1,000 ethnic Somalis and 200 to 300 non-Somalis were recruited from the U.S., UK, Canada, Australia, Sweden, and Denmark while dozens were either convicted or killed, while providing material support to al-Shabaab.[21]

In the case of al-Shabaab and the Islamic State in Somalia, radical diaspora individuals have played and continue to play key leadership, recruitment, mobilisation and command roles. Omar Hammami (Abu Mansur al-Amriki), al-Shabaab commander and propagandist, who was born in the U.S., became the group's most prolific English-language ideologue, used concepts of *hijrah* (religious migration) and the construction of an "*Ummah* consciousness" to persuade Western Muslims that identification with the global Muslim community was incomplete without physical relocation to a conflict zone.[22] Abdul Qadir Mumin, the leader of the Islamic State in Somalia, lived in Sweden in the 1990s before moving to Slough, UK where he obtained British citizenship until 2010 when he left for a brief sojourn.in Kenya, before heading to Somalia to join al-Shabaab and later to pledge allegiance to the Islamic State in Somalia[23] The latter was formed in 2015 and recognised as an official Islamic State province *('wilaya')* in 2017 by the IS's central command.[24]

Separately, in January 2015, Abu Hamza al-Masri, the Egyptian-born preacher formerly of the Finsbury Park Mosque in London, was sentenced to life imprisonment by a U.S. court on terrorism charges following his extradition from the UK.[25] Importantly, this study underscores that the diaspora-radicalisation pipeline is neither anecdotal nor confined to a single country and ideological single-strand analytical frame alone. As ICSR report notes explicitly, al-Shabaab's outreach "[...] does not rely exclusively on Islamist ideology," and nationalism, anti-Ethiopian sentiment following the 2006 invasion, and anti-American sentiment associated with perceived U.S. support for that invasion were independently significant drivers of diaspora sympathy.[26]

Further, part of the Somali diaspora-driven radicalisation is nationalist and clan-based, driven by Somaliland separatist tensions rather than explicitly jihadist dynamics. Writing on the 2025 armed conflict between the Republic of Somaliland and the newly declared North Eastern State of Somalia (formerly SSC-Khatumo), Abdullahi Ali Hassan argues that the geographically dispersed but digitally connected Somali diaspora functions as a "digital remitter of violence," coining the term *afkudhiigle* ("murderer by mouth") to describe diaspora social media users who amplified dehumanising hashtags such as *#faqashta* and *#GalaDagaalka* ("go to war") and circulated graphic imagery of casualties and humiliated prisoners during the conflict.[27] Hassan situates this behaviour within a pre-existing Somali moral taxonomy that distinguishes *gacan ku dhigle* ("murderer by hand"), *af kudhiile* ("murderer by mouth"), and *qalbi ku dhiigle* ("murderer by moral complicity"), arguing that platform-enabled "self-mass communication" has made a historically marginal category of wartime conduct, inflammatory rhetoric, into a mass, globally visible phenomenon for the first time.[28]

This diaspora engagement is reinforced by material incentives: prominent diaspora social media influencers who cultivate large "virtual clan" followings have translated online popularity into tangible political capital, including appointment to senior government positions, which in turn incentivises further partisan and inflammatory content production as a route to status and patronage.[29] While this clan-nationalist digital conflict is analytically distinct from jihadist radicalisation, the literature suggests the two ecosystems are not hermetically sealed: al-Shabaab's messaging apparatus has repeatedly sought to exploit clan grievances and disputes over territorial legitimacy, as seen in its 2026 statement on Somaliland; to position itself as a defender of a unified, authentically Islamic Somali identity against both secessionist and Western-aligned actors.[30]

2.2 Geopolitics as a Driver of Diaspora Radicalisation

Diaspora communities occupy a structurally ambivalent position between the political life of their country of settlement and the unresolved conflicts of their country or region of origin. The dual embeddedness thus gives geopolitical events such as wars, foreign military interventions, and great-power rivalries, a direct and often immediate bearing on diaspora identity and grievance formation, in a way that domestic events in the host state alone do not. The RAND Corporation and the Center for Security Studies at ETH Zurich, in one of the earliest systematic treatments of the subject, found that diaspora communities "frustrated with a perceived war against the Muslim world" have in some instances turned against their adopted homelands, supporting terrorism through recruitment, fundraising, and training networks that draw on financial and social lifelines within the diaspora itself.[31] The UK Foreign and Commonwealth Office–commissioned reports similarly list international geopolitics, alongside identity crisis, discrimination, and home-country

linkages, as a recognised meso-level driver of radicalisation risk in diaspora and migrant communities.[32]

A study published in the Journal of Strategic Security finds that geopolitics functions as a rhetorical resource that Islamist and jihadist movements deliberately tailor to their audience, with the recurring master narrative framing the Western-led "war on terror" as a war against Islam itself; a frame that combined with identity crisis among second- and third-generation diaspora youth negotiating national and religious belonging, works to shift vulnerable individuals toward in-group solidarity with the *Ummah* and away from the host society.[33] Such a narrative does not require the individual to have any direct connection to the conflict invoked; its power lies in its ideological transferability across other geopolitical events including: the 2003 Iraq War, the Syrian civil war from 2011, the Israel–Hamas war following the 7 October 2023 attacks, and the instability in the Sahel and Horn of Africa.

Perhaps the easiest large-scale demonstration of geopolitics converting diaspora grievance into mobilisation is the outflow of foreign fighters, including of diasporic origins, from the European Union (EU) countries to Syria and Iraq after 2011, precipitated by the civil war against the Assad government and the subsequent rise of the Islamic State (ISIS). U.S. congressional research estimated that more than 20,000 foreign fighters travelled to the Syria–Iraq theatre from 2011 onward, including at least 3,400 Westerners, drawn principally from Austria, Belgium, Denmark, France, Germany, the Netherlands, Spain, Sweden, and the United Kingdom.[34] By Europol's own accounting, approximately 5,000 Europeans, mostly from Britain, France, Germany, and Belgium, had travelled to join the Islamic State, of whom roughly 1,500 had returned home by 2019.[35]

Country-level figures illustrate the scale within specific diaspora communities: in France and Belgium, an estimated 1,300 French and 400 Belgian citizens travelled to Iraq and Syria; roughly 700 French and 150 Belgian fighters remained in the theatre as of 2020, with 270 French and 125 Belgian nationals having returned.[36] In Germany, more than 1,050 individuals left for Iraq and Syria since 2013 according to the domestic intelligence service (BfV); about one-third later returned, and roughly 200 were reported killed.[37] In the United Kingdom, an estimated 900 people travelled to the Syria region; about one-fifth died and roughly half returned, leaving an estimated 360 unaccounted for in the region.[38] However, the returnee risk did not end with the collapse of the territorial "caliphate"; the Foreign Policy Research Institute documents cases of French and Belgian returnees reactivating extremist facilitation networks inside Europe, radicalising others, and channelling funds and recruits back toward conflict zones, including one Belgian returnee who travelled to Britain specifically to obtain funding from an extremist network before returning to Belgium.[39]

The European Institute of the Mediterranean (IEMed) studies reveal how jihadist recruiters address diaspora youth through a de-territorialised, "imagined geography" of the *Ummah*, presenting recruits from France, Belgium, and elsewhere in Europe as members of a single transnational body irrespective of national origin, a framing that explicitly subordinates host-country citizenship to religious-political identity.[40] Field and prison-based research further shows that recruiters exploit real or

perceived discrimination directly[41]; French prison audits describe Islamist inmates forming an informal "aristocracy" that recruits vulnerable, aggrieved young offenders by invoking the treatment of immigrants in Europe and Muslim civilian deaths in Western military interventions.[42]

Geopolitical grievances are thus an increasingly unifying jihadist mobilisation frame that transcends organisational and regional boundaries, aided in part by virtual platforms, to decentralised radicalisation levels that reach, mobilise and recruit individual sympathisers. Such episodes function less as triggers for immediate large-scale violence than as durable additions to a cumulative grievance narrative that recruiters redeploy over years. The instrumentalisation of geopolitical grievances and narratives for jihadist causes thus not only affects the conflict theatres, through the diaspora-based amplification of geopolitical grievances and flows of terrorist financing and foreign fighters, but also the diaspora hubs through related terror threats and attacks. Such a dynamic can be observed from the 2023–2025 Gaza war, which handed jihadist propagandists a fresh "rallying cry" to portray Western and allied governments as occupiers and enemies of Muslims.[43]

The Hamas-led attack on Israel of 7 October 2023 and the subsequent Gaza war constitute perhaps the most significant recent illustration of an acute geopolitical shock rapidly reshaping the Western threat landscape, across both jihadist and identity-based extremist currents. Europol's EU Terrorism Situation and Trend Report (TE-SAT) 2024 recorded 120 terrorist attacks across seven EU member states in 2023 (98 completed, nine failed, 13 foiled) and 426 arrests for terrorism-related offences across 22 member states, of which 334, the majority, concerned jihadist terrorism, a marked increase on 266 such arrests in 2022.[44] TE-SAT 2025, covering 2024, recorded 24 jihadist attacks (up from 14 in 2023, and the largest single-ideology category that year), most perpetrated by lone actors (20 of 24), alongside 449 total arrests across 20 member states, 289 of them jihadism-related; the report explicitly attributes the shift in the threat landscape to developments beyond EU borders.[45]

The same geopolitical shock (Israel-Hamas war) is associated with parallel, reciprocal radicalisation risks in the U.S.; the Anti-Defamation League for example, recorded 8,873 anti-semitic incidents across the United States in 2023 and, per subsequent reporting, 9,354 incidents in 2024, the highest figure in the 46-year history of its audit.[46] Israel's Institute for National Security Studies (INSS) documented anti-semitic-incident increases of 500 per cent in the United Kingdom, 400 per cent in Germany, 813 per cent in the Netherlands, and 430 per cent in the United States between October and December 2023, alongside a 1,200 per cent spike in online anti-semitic content, specifically between 7 and 10 October 2023.[47] The Council on American-Islamic Relations (CAIR) reported 8,061 anti-Muslim incidents in the United States in 2023, the highest total since the organisation's founding roughly thirty years earlier, with nearly half occurring after 7 October, while the European Islamophobia Report concluded that "the War on Gaza has functioned as a geopolitical catalyst of anti-Muslim racism in Europe," with Norway, Spain, and Greece recording spikes in anti-Muslim hate crimes.[48] Such threat dynamic demonstrates that a single geopolitical trigger event can simultaneously radicalise across ideologically opposed currents (jihadist, far-right,

and grievance-driven lone actors), reinforcing one another through what practitioners increasingly describe as ideologically "mixed" or hybrid radicalisation pathways rather than discrete and siloed movements.

A more regionally specific geopolitical driver in the Horn of Africa, is the January 2024 Ethiopia–Somaliland MoU, under which Ethiopia secured a 50-year lease on Somaliland coastline for a naval base in exchange for a stated pathway toward recognising Somaliland's independence.[49] Al-Shabaab's spokesman publicly rejected the deal as illegal and backed by "apostates and traitors," warning that "blood will be spilled over it" and explicitly likening it to the loss of Palestine to Israel, a framing that fused the local sovereignty dispute directly into the group's global jihadist register.[50] The MoU and Somalia's subsequent characterisation of Ethiopia as an enemy on par with al-Shabaab, generated an anti-Ethiopian nationalist backlash that al-Shabaab has actively sought to exploit through organised protests and propaganda, potentially reversing several years of declining popular tolerance for the group.[51] Israel's subsequent recognition of Somaliland has reinforced the al-Shabaab narrative that external powers are deliberately fragmenting Somali territory to sustain conditions of state weakness.[52] At the same time, al-Shabaab has historically struggled to establish an operational foothold inside Somaliland itself, meaning the MoU's radicalising effect is likely to be felt more strongly in its rhetorical and recruitment value than in direct territorial gain.[53]

2.3 The Digital Front of Diasporic Violent Extremism

Digital platforms such as social media and other virtual sites have become alternative battlefronts for extremist elements in two-fold. First, extremist groups exploit these communication channels not only to project global jihadism, but to also appeal to their international audience including the diaspora sympathisers. In 2012, the International Centre for the Study of Radicalisation's (ICSR) study of al-Shabaab's Western media strategy, showed that the group's English-language video output, press releases, and pioneering use of Twitter were purpose-built to recruit and radicalise members of the Somali diaspora and English-speaking Western Muslims more broadly, at a time when Western governments had been slow to proscribe the organisation.[54] The ICSR quantitative analysis of al-Shabaab's official Twitter account (@HSMPress) 541 tweets between December 2011 and April 2012, reveals that narrative promotion (33.5 per cent) and operational capacity (25.5 per cent) dominated the group's messaging.[55] The account was also used reactively to rebut Western media reporting and to manage perceptions of internal cohesion after Commander Omar Hammami's public fall-out with the leadership. This early case demonstrates that al-Shabaab treated social media as an integrated instrument of information warfare rather than as an ancillary communications channel from the outset.

Second, transnational networks of sympathisers, financiers, and propagandists located far beyond the primary theatre, exploit social media to radicalise and call

to extremist action. A joint DW–ARD media investigation illustrates how diaspora members exploit social media to radicalise and mobilise violence back home. "Kabtan Ayub" (Ayub Abdirizak), a Somali asylum-seeker based in Germany from 2017, built a network of hundreds of thousands of followers on TikTok and Facebook, using clan-based hate speech to urge followers to "take the guns and fight," offering tactical advice on ambush positions and instructing supporters to shoot uniformed personnel on sight.[56] Chatbots have also been deployed by websites and social media platforms to lure some diaspora members into joining jihadist groups, as exemplified by the case of Mohamed Mohamoud, a 22-year-old Somali immigrant in the UK (Bristol), arrested in January 2026 after failed attempts of joining the Islamic State in Somalia, after returning from Puntland, where the group operates.[57]

The internet is thus no longer merely an instrumental and logistical tool for extremist groups, which increasingly recognise it as a jihadist frontier in its own right. A study of two decades of European terrorism identifies the virtualisation of recruitment as the single most consequential driver reshaping how individuals become radicalised.[58] The virtualisation has facilitated the rise of lone-actor ("lone wolf") violence, ideological hybridisation, younger demographics and compressed ("turbo") radicalisation trajectories across European diaspora hubs including Germany, France, UK, Sweden, Belgium and others.[59] While this framework was developed primarily from European lone-actor cases, it can be adapted to the Eastern African context, in which al-Shabaab and the IS-S, remain highly organised and hierarchical, on the basis of the migration of the recruitment and indoctrination process itself into online and encrypted spaces. Such tactical and operational shift, virtualisation without de-organisation, allows a hierarchical organisation to sustain diaspora-facing recruitment pipelines without the physical infrastructure that sustained counter-terrorism pressure has made increasingly difficult to build.[60]

Critical to understanding the virtualisation of violent extremism, is the platform-level analysis of the digital ecosystem and content moderation models, which permit such destabilising infiltration. The Institute for Strategic Dialogue's (ISD) 2022 investigation, "*Under-Moderated, Unhinged and Ubiquitous*," found jihadi virtualisation strategy had matured into a resilient and multi-platform ecosystem.[61] ISD researchers identified 30 public Facebook pages, operating in Somali, Kiswahili, and Arabic and presenting themselves as independent "media outlets," that were sharing official al-Shabaab and Islamic State-Somalia propaganda largely undisturbed by moderation; these pages posted roughly 850 videos over a two-year period, generating approximately 450,000 views, with individual videos remaining online for as long as six years.[62] ISD attributed this persistence to language-moderation blind spots; Facebook's community standards, at the time of the report, existed in more than 60 languages but not in Somali and Swahili, and moderators were found to be allotted as little as 15 seconds to review a video before clearing it.[63] Facebook's language gaps were not unique to al-Shabaab-related content; independent reporting on internal Facebook documents released in 2021 found comparable moderation deficits for Pashto, Dari, and Arabic dialects in other at-risk countries, suggesting a structural rather than group-specific vulnerability that platform governance has yet to close.[64]

2.4 Diaspora, Virtual Networks and Terrorist Financing

Virtual platforms have also become a financial resource mobilisation instrument, creating a pool of financiers and donations as well as loopholes against financial monitoring systems, for extremist groups. Financial mobilisation through virtual platforms has evolved from online appeals, to informal money transfer systems, to adoption of cryptocurrencies. The study by Global Network on Extremism and Technology (GNET) finds that Islamic State and al-Qaeda propaganda ecosystems function as financial infrastructure in their own right: propaganda content builds the trust and legitimacy that allow cryptocurrency transfers and hawala transactions, often arranged through encrypted messaging platforms such as WhatsApp, to be coordinated among dispersed diaspora sympathisers who first connected through propaganda communities on mainstream social media.[65]

Violent extremist organisations (VEOs) operating in Eastern Africa have increasingly embraced cryptocurrency as a primary method to exploit diaspora networks and move funds across borders. Islamic State-Somalia (IS-S) has emerged as a significant player in this ecosystem, with its monthly revenue estimated to have risen from 100,000 to 360,000 U.S.-dollars between 2023 and 2024, generated through extortion, digital fundraising and private donations known as *sadaqah*.[66] The latter constitute major revenue sources, and are increasingly channelled through digital wallets. Notably, IS-S functions as the Islamic State's primary revenue hub for African operations, overseeing financial networks across Kenya, Uganda, Tanzania, and South Africa through its al-Karrar office.[67] The group strategically targets diaspora communities through stablecoins like Tether USDT, which facilitate transfer of funds while maintaining reduced traceability compared to traditional banking channels.

Africa is experiencing exponential cryptocurrency adoption, emerging as the third-fastest growing crypto market globally. Between July 2024 and June 2025, Sub-Saharan Africa received over 205 billion U.S.-dollars in on-chain value, representing a 52 per cent year-over-year increase, with stablecoin usage surging 180 per cent across the region.[68] Nigeria leads continental adoption with approximately 92 billion U.S.-dollars in cryptocurrency value, ranking second globally on the Crypto Adoption Index, while Kenya (ranked fifth globally), South Africa, Ethiopia, and Ghana comprise the top five African nations.[69] However, regulatory fragmentation poses significant challenges across the continent. Sub-Saharan Africa faces weak institutional supervision of Virtual Asset Service Providers (VASPs), leading to both South Africa and Nigeria being placed on the FATF's increased monitoring list in February 2023 (removed in October 2025).[70]

Moreover, the lack of harmonisation across jurisdictions, insufficient Travel Rule compliance frameworks, limited blockchain-specific legislation, and gaps in AML/CTF enforcement create vulnerabilities. While countries like South Africa, Nigeria, Kenya, and Ghana have introduced regulatory frameworks, many

jurisdictions remain in exploratory phases, pushing significant transaction volume toward unregulated peer-to-peer markets.[71] The regulatory weakness can only increase the risk and volume of leakages to terrorist groups. For example, between July 2023 and June 2024, approximately 59 billion U.S.-dollars in cryptocurrency transactions occurred in Nigeria alone, a scale that allows terrorist groups to obscure illicit transfers within legitimate trading volumes.[72]

The hawala system, an informal value transfer (IVT) network requiring only trust and community connection and informal money transfer systems, has become the primary exploitation mechanism for terrorist organisations targeting diaspora remittances to East Africa. The hawala system is used to move money across borders or cities without physically transporting cash. A person hands cash to a local broker, known as a *hawaladar*, along with instructions for who should receive the funds and where.[73] The originating *hawaladar* then contacts a trusted counterpart *hawaladar* in the destination location, often via phone, messaging apps, or coded references, and instructs them to pay the equivalent amount, in local currency, to the intended recipient. Critically, no money physically crosses the border at the time of the transfer; the recipient is paid out of the second *hawaladar*'s own liquidity.[74] The two *hawaladars* now hold an informal debt between them. This is settled later, not necessarily in cash, through mechanisms such as reverse hawala transactions in the opposite direction, trade invoicing (real or manipulated), property transfers, or by simply netting the balance against future flows between the same pair of brokers. Over time, and across many customers, these bilateral debts largely offset one another, so very little money ever needs to physically move at all. [75]

As such, the hawala networks are difficult to monitor, trace and disrupt any terrorist financing flows because they are not built to run Know Your Customer (KYC) procedures as regulated banks and money transfer operators (MTOs) KYC requires banks and MTOs to verify a customer's legal identity, screen them against sanctions and watch lists, identify beneficial owners, and understand the purpose of the transaction, before a transfer is allowed to proceed. On the contrary, the hawala system has no customer identification program, no beneficial-ownership check, no sanctions screening, and no requirement to record or report the transaction. Money transfers are arranged through verbal agreements, personal reputation, or simple codes exchanged between broker and client, rather than through account numbers or verified identification (ID) documents.[76] The absence of KYC has several concrete effects on traceability; there is no reliable paper trail, and no beneficiary information attached to the payments the way a wire transfer carries originator and beneficiary data, so investigators cannot simply subpoena a bank to find out who really sent or received funds.[77] Further, the settlement layer between *hawaladars* is itself opaque; since it is often disguised inside ordinary-looking trade transactions (over- or under-invoicing goods, for example), it is hard to distinguish a legitimate business payment from a hawala settlement. Finally, because trust rather than documentation underpins the whole system, the identity of the ultimate customer may never be captured anywhere in writing, making it vulnerable to money laundering, sanctions evasion, and terrorist financing; the hawala networks thus cannot trigger the reporting mechanisms that formal banks are obligated to use.[78]

Legitimate remittance flows to Somalia alone exceed 1.7 billion U.S.-dollars annually, with

the global Somali diaspora sending approximately 1.3 billion U.S.-dollars yearly, representing 15 to 20 per cent of Somalia's economic output.[79] A landmark federal prosecution in Minnesota (2010 to 2011) demonstrated this vulnerability when two Somali-American women were convicted of sending 8,600 U.S.-dollars to al-Shabaab fighters through hawala intermediaries, a case exemplifying the use of diaspora networks for terrorist support.[80] The recent investigations in Minneapolis uncovered evidence that welfare funds fraudulently diverted from state programmes were systematically routed through hawala networks to Somalia, with federal counter-terrorism officials reporting that millions of dollars reached al-Shabaab.[81] Al-Barakaat, a Somali hawala operator designated as a terrorist financing entity in 2001 for alleged links to bin Laden, operated in 40 countries with 140 million U.S.-dollars in annual revenue, illustrating the scale at which informal systems can be weaponised.[82]

Between 2007 and 2010, al-Shabaab reportedly channelled significant resources through informal systems before the 2010–2011 de-risking decisions, when U.S. banks closed accounts of Somali Money Transfer Operators, paradoxically strengthened the group's reliance on unmonitored hawala networks in Minnesota, East Africa, and the Diaspora regions, creating a shadow financing infrastructure that formal regulation cannot penetrate. Domestic prosecutions provide further evidence of the financing pathway's persistence: in September 2025, a Somali court sentenced a woman to sixteen years' imprisonment for laundering more than 2.1 million U.S.-dollars through her personal bank account to finance al-Shabaab bombings and assassinations, illustrating that in addition to informal hawala transactions, formal-sector financial channels remain exploitable.[83]

FATF's 2013 typology study on hawala and other similar service providers (HOSSPs) identifies these trust-based, largely undocumented settlement networks as a recognised high-risk channel for both money laundering and terrorist financing, precisely because the same properties (speed, low cost, minimal documentation) that make them attractive for legitimate diaspora remittances also make them attractive for illicit diversion once a transfer corridor matures.[84] FATF's July 2025 Comprehensive Update on Terrorist Financing Risks for instance, confirms that hawala and other unlicensed remittance providers remain an active terrorist-financing method, alongside a marked increase in the mixed use of diverse financing methods and the integration of digital tools, including online payment services and crowdfunding features on social media, with conventional cash-based techniques.[85] United Nations Counter-Terrorism Committee Executive Directorate (CTED) trend analysis covering 2014–2024 also finds that funds supporting foreign terrorist fighters travelling to Syria and Iraq typically moved from countries of origin through conventional banking, hawala, or informal value transfer systems, or as cash physically carried below reporting thresholds, with countries bordering the conflict zone serving as key transit and cash-out hubs.[86]

Such fundraising strategies are not unique to al-Shabaab nor do they only target North American and European diaspora hubs. Between 2017 and 2024, Mozambique's Financial Intelligence Office (GIFiM) detected over seven million U.S.-dollars in terrorist financing flows linked to ISIS-Mozambique, systematically mobilised through fragmented cash deposits, bank and mobile money transfers.[87] The July 2025 report of the United Nations (UN) Analytical Support and Sanctions Monitoring Team on the Islamic State

of Iraq and the Levant (ISIL or Da'esh) and al-Qaida confirmed criminal-terrorist hybridisation of these networks.[88] Islamic State groups, especially Islamic State-Somalia, the Allied Democratic Forces, and ISIS-Mozambique (Ansar al-Sunnah), and other extremist militant causes have developed sophisticated social media infrastructures specifically targeting diaspora audiences through encrypted messaging platforms and open networks.

The Islamic State's Central Africa Province (operating through ADF in DRC and ISIS-Mozambique) coordinates financial appeals across these platforms. Evidence indicates that private donors reached via Telegram are directed to transfer funds through cryptocurrency or prepaid card systems. ISIS-Mozambique/Ansar al-Sunnah operates through regional recruitment networks, such as the Ansaar Muslim Youth Centre (AMYC), a Tanga-based Tanzanian group linked to the late radical Kenyan cleric Aboud Rogo (killed in 2012), facilitating diaspora recruitment from East and Southern Africa.[89] Social media appeals have proven particularly effective in recruiting diaspora-origin fighters, with captured ISIS-Mozambique operatives reporting that initial radicalisation occurred through Telegram and WhatsApp before physical recruitment into operations.

2.5 Governance, Platform Moderation and Regulatory Gaps

Governance gaps operate simultaneously at the platform level and at the level of cross-jurisdictional law enforcement. At the platform level, ISD's Facebook investigation indicates that al-Shabaab and Islamic State-Somalia networks exploit persistent East African language-moderation blind spots, that takedown enforcement is inconsistent, official al-Kataib-branded content survived on the platform for up to six years, and that even confirmed "super-user" accounts sharing officially branded terrorist content routinely reappear under duplicate identities after enforcement action, indicating that current content-moderation infrastructure struggles to achieve durable disruption rather than temporary displacement.[90]

At the jurisdictional level, the diaspora-terrorism literature from the UK and Canada documents a structurally similar pattern of belated recognition and adaptation. Michael Whine's account of UK counter-terrorism policy indicates that British authorities were slow to proscribe extremist preachers and organisations operating openly; the country was informally dubbed "Londonistan" by foreign intelligence services frustrated at the UK's tolerance of exiled Islamist activists, and that the Prevent strategy's later community-engagement efforts were criticised for engaging disproportionately with self-appointed Islamist-aligned representative bodies rather than genuinely representative moderate community voices.[91]

Stewart Bell's Canadian case studies similarly document how the Anti-terrorism Act's terrorist-financing provisions were only enacted after 2001 and were not retroactive, and how the country's Supreme Court jurisprudence on non-refoulement and citi-

zenship has constrained the deportation of suspected financiers and returnees, obliging authorities to rely on lengthy, resource-intensive criminal investigations such as Project "Osaluki" against the World Tamil Movement, a template increasingly applied to Somali-Canadian financing networks as well.92 The ICSR report's framing of al-Shabaab's early Western outreach highlights that group's propaganda, videos, and fundraising activity "remained freely available for a number of years because Western governments were slow to proscribe the group", the United States designated al-Shabaab a foreign terrorist organisation only in February 2008, and the UK not until March 2010, by which point recruitment networks were already established and entrenched.93 The recurring lag between the emergence of a transnational radicalisation or financing vector and the activation of an effective legal and regulatory response is thus arguably the single most significant "governance blind-spot" and a structural feature of diaspora-linked extremism in the Horn of Africa.[94]

2.6 Conclusion

Several converging vulnerabilities to diaspora-based online radicalisation, mobilisation and terrorist financing can be observed as critical governance blind-spots in Eastern Africa and diaspora hubs (Europe and North America). First, the amplification of extremist narratives through diaspora-linked social media ecosystems, indicates the shift from physical to virtual networks for extremist radicalization, mobilization and recruitment, and the challenge governments and digital platforms face in building adequate capabilities to combat violent extremism on the digital front. Second, the financial leakage through alternative money transfer systems, digital currencies and informal diaspora remittance channels, indicates new regulatory challenges in financial monitoring and combating terrorist financing.

Third, the cross-jurisdictional weaknesses in enforcing or adapting governance (legal and policy) frameworks and platform-moderation regulations to the evolution of the threat of violent extremism across the U.S., UK, Germany, Sweden, Canada, and the larger Eastern Africa, contributes to the poor outcomes in preventing and combating online diaspora-based radicalization, mobilization, and terrorist financing between these jurisdictions.[95] Lastly, the role of politics, conflict, geopolitics, socio-economic vulnerabilities and Islamism in the construction of mobilisation frames and narratives for radicalization and terrorist financing in the Horn of Africa by diaspora-based extremists, poses a constant challenge for reactionary and hard-power counter-terrorism strategies and warrants counter-terrorism and P/CVE strategy review across EU countries (especially Germany, France, Belgium and Sweden among others), U.S., UK, Canada, and the larger Eastern Africa.

3.0 Findings

3.1 Diaspora Radicalisation and Violent Extremism in Eastern Africa

The most common diaspora networks in Europe and North America linked to extremist radicalisation in the Horn of Africa, are from the broader Eastern Africa region (66.7 per cent), the Somali diaspora (50 per cent) and Middle Eastern/Levantine diaspora networks (41.7 per cent). Social media analysis additionally illustrates a specific connection, especially for the case of the U.S. (North America), between Minnesota-based Somali diaspora activity and political or conflict-related developments concerning al-Shabaab and nationalist violent extremism targeting Somaliland as shown in Figure 1 below:

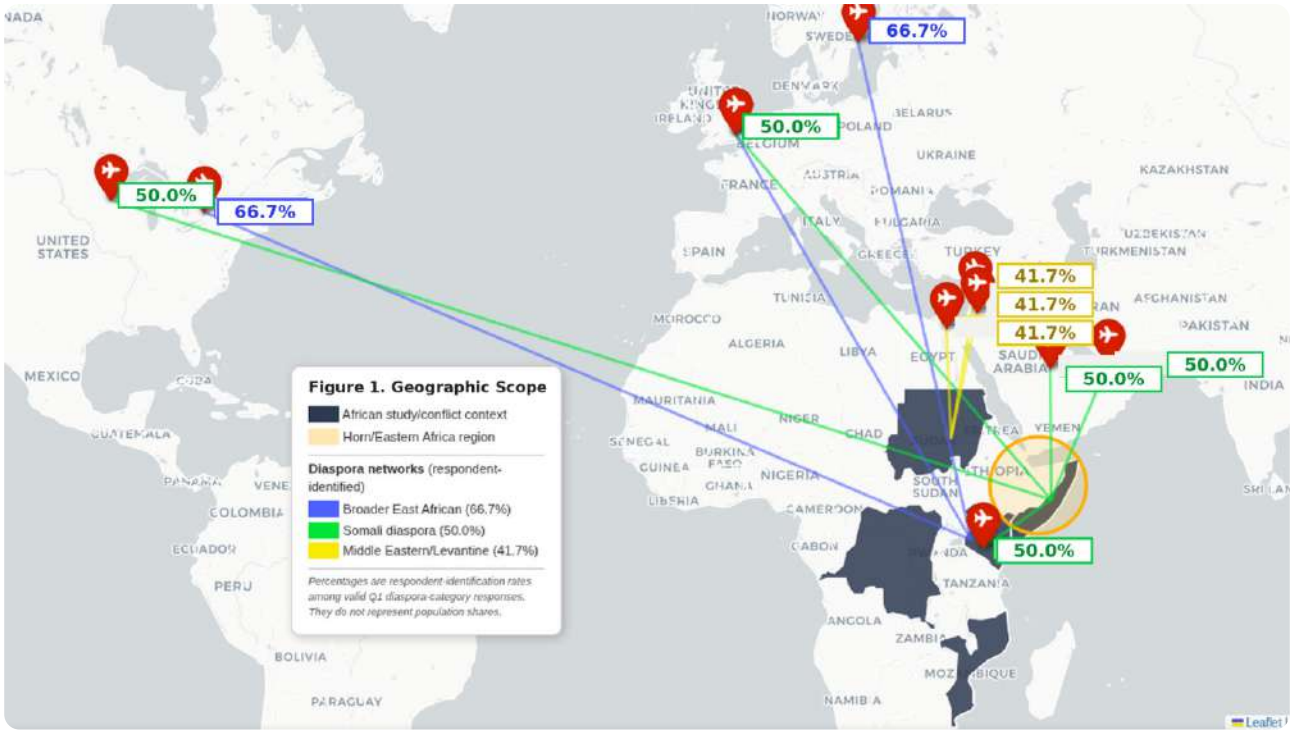

Figure 1: Extremist Radicalisation and Diaspora Hubs. Source: HORN Institute.

The findings indicate that the diaspora of Eastern African extraction is not only confined to the "far diaspora" (EU, U.S., UK, and Canada), but also includes the "near diaspora" made up of regional migrant destinations and sociological extensions through cross-border co-ethnics in the broader Eastern Africa, especially Kenya for the Somali community and migrants from Central Africa. Secondly, diaspora-linked radicalisation and mobilisation into violent extremism in the Horn of Africa is a two-way traffic: regional VEOs targeting the diaspora communities and (ii), the diaspora extremists targeting vulnerable populations in Eastern Africa either to influence them into jihadism or other extremist militant causes.

The al-Shabaab group (75 per cent) emerged as the most connected extremist organisation to diasporic support and targeting in Europe and North America, as well as within Eastern Africa diaspora hubs. Al-Shabaab is connected to Somalia and Kenya, Somali and Swahili-language communication, public propaganda, recruitment, diaspora-oriented messaging and movement between public and private digital environments as illustrated in Figure 2 below:

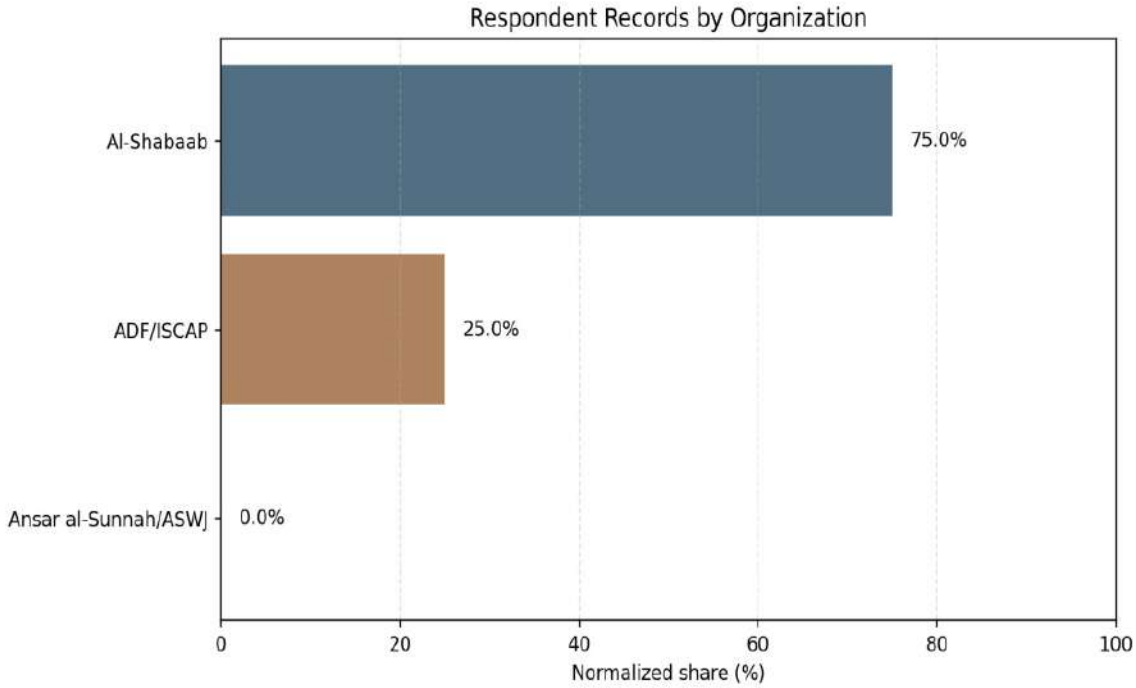

Figure 2: Extremist Groups in Eastern Africa and Diaspora Links. Source: HORN Institute.

The al-Shabaab extremist group was prominently linked to jihadist violent extremism in Somalia and Eastern Africa region; connections to Somali diaspora hubs in Kenya, larger Eastern Africa, Europe and North America; as well as online communication in multiple languages (mostly Somali, English, Swahili, and Arabic). One respondent described al-Shabaab as

> *"...using public videos and statements to maintain visibility while more direct recruitment discussions moved into private platforms such as Telegram and WhatsApp"*[96]

Another respondent identified Facebook, Telegram, WhatsApp, X, and other services serving different communication functions and specifically discussed al-Shabaab's historical use of X and its multilingual communication strategy. However, not all diaspora-linked extremist activity in Somalia and Eastern Africa relates to al-Shabaab, given the existence and transnational networks of other regional groups including the Islamic State in Somalia. For example, in August 2026, Mohamed Mohamoud was convicted by a UK court for attempting to fly to Somalia to join the Islamic State in Somalia, after using AI bots to contact the group and watching extremist videos on YouTube and TikTok.[97]

ADF/ISCAP was identified as the other violent extremist organisation (25 per cent) with links to diaspora networks but appeared more regionalised within the wider East and Central African diaspora hubs. ADF/ISCAP is associated with Swahili-language communication with audiences across Kenya, Tanzania, the DRC and northern Mozambique and other regionally aligned extremist messaging. Ansar al-Sunnah/ASWJ is principally localised within Mozambique with mostly regional ideological messaging and mobilisation. The three organisations occupy different geographic and communication contexts rather than forming a single uniform digital ecosystem as further illustrated in Table 1 below:

Table 1: Digital Ecosystem of Extremist Groups in Eastern Africa. Source: HORN Institute.

Organisation	Main context in the study	Digital/communication relevance	Overall interpretation
Al-Shabaab	Somalia, Kenya, Somali diaspora and wider Horn	Public propaganda, multilingual messaging, recruitment, public-to-private migration and diaspora engagement	Most consistently and explicitly discussed named organisation in respondent narratives
ADF/ISCAP	Eastern/Central African regional context, including DRC-linked and Swahili-speaking environments	Regional and Swahili-linked messaging; connection of local grievances with wider ideological narratives	Important but more context-specific
Ansar al-Sunnah/ ASWJ	Mozambique and wider East African extremist dynamics	Regional ideological messaging and mobilisation	Important but more geographically specific
Other conflict/ extremist ecosystems	Particularly Sudan and conflict-related environments	Ethnic/clan incitement, hate speech, conflict propaganda and armed-actor support for militias in the ongoing civil war in Sudan	Shows that the phenomenon extends beyond formal terrorist organisations

3.2 Diaspora and Social Media Radicalisation

3.2.1 Which Platforms Matter Most

TikTok and Facebook emerged as the dominant public-facing platforms, with TikTok identified by 87.5 per cent of the respondents and Facebook by 81.3 per cent, followed by X 43.8 per cent as shown in Figure 3 below:

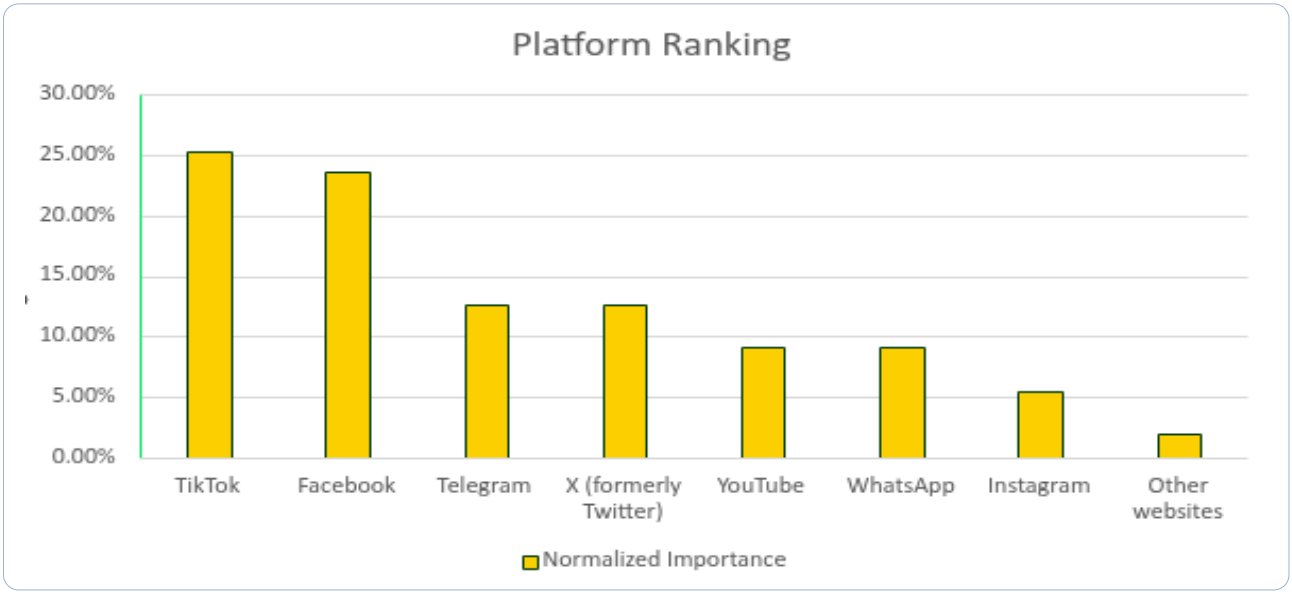

Figure 3: Platform Vulnerability to Online Radicalisation and Extremist Messaging. Source: HORN Institute.

The importance of such public-facing platforms lies primarily in promoting discovery or exposure, visibility, rapid amplification, and broad audience reach for TVEC, especially through short-form video, reposting, public groups, and algorithmic recommendation systems.

> *"The platforms most commonly used are TikTok, along with other major social media channels (Facebook and X). The content shared most frequently includes short videos, brief news-style updates, and commentary on current affairs. This content often spreads disinformation and extremist messages, and is used to openly support terrorist groups…..".*

By contrast, Telegram (43.7 per cent), YouTube (31.2 per cent) and WhatsApp (31.2 per cent) were identified less frequently but appear to perform more specialised functions such as private conversations, ideological reinforcement and recruitment. Respondents associated these platforms with closed groups, direct messaging, persistent interaction, and movement from public exposure into more private communication spaces. Other similar encrypted platforms for private conversations instrumental in recruitment mentioned by respondents include Element, Rocket. chat, and Signal. The digital ecosystem is not defined by one platform, but by the different capabilities and roles platforms play across stages of exposure, engagement, reinforcement, and possible mobilisation. The finding therefore suggests that social media has been instrumentalised by extremist groups and individuals as critical messaging platforms and frontiers of violent extremist campaigns. As a respondent explained,

> *"Extremist groups regularly post daily messages, news updates, and propaganda content designed to inspire people to join them. They use platforms for active recruitment, targeting individuals and community leaders with direct messages that encourage them to join and often provide practical guidance on how to travel to their locations. Social media is also used for fundraising and for building and maintaining networks of supporters and followers around the world, helping them expand their reach and sustain their activities."*

3.2.2 Platform Function Matters More Than Platform Name

The heat-map demonstrates that platform function matters more than platform name alone. TikTok, Facebook and Instagram are strongest in discovery or exposure and public amplification, while Telegram is more strongly associated with sustained engagement, private interaction and reinforcement. WhatsApp performs a primarily interpersonal and private communication role, while X is particularly relevant to rapid public amplification. YouTube occupies a different position by supporting longer-form engagement and ideological reinforcement. Together, these patterns demonstrate how users and narratives may move through a multi-platform ecosystem, rather than remaining on a single service as shown in Figure 4 below:

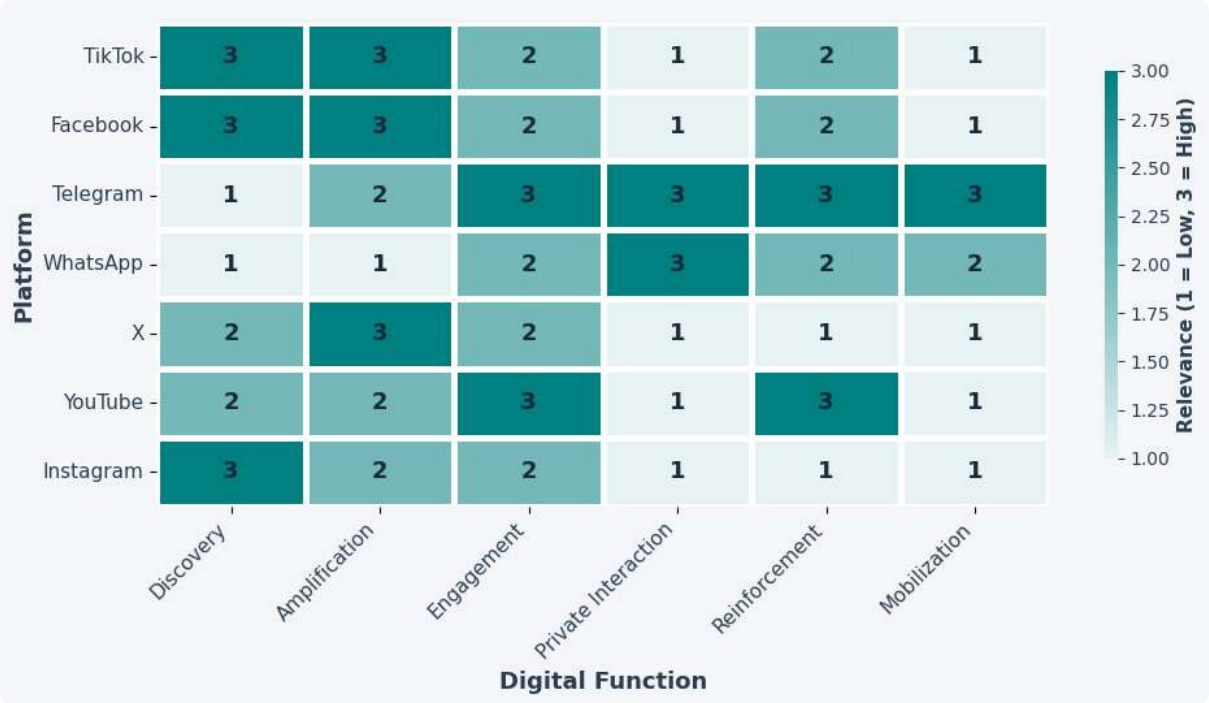

Figure 4: Platform Functional Roles in the Online Radicalisation Ecosystem. Source: HORN Institute.

The other key defining feature of X, YouTube, Instagram and TikTok platforms in the amplification of TVEC, is the algorithmic recommendation system. As a respondent observed,

> *Algorithmic recommendation systems play a significant role in increasing users' exposure to extremist content. Once a user begins engaging with this type of material, the algorithms tend to continuously feed them similar or more extreme content, creating a cycle that amplifies and deepens their exposure over time. This is one of the most important factors in how radicalisation can be accelerated on these platforms*[100]

3.2.3 Cross-Platform Migration

Online radicalisation can develop across a connected digital ecosystem rather than within a single platform. Public-facing platforms such as TikTok, X, Facebook, Instagram and YouTube are most important for discovery and early amplification, while Telegram, WhatsApp and closed groups become more

relevant as communication moves into more private and sustained forms of interaction that can lead to ideological reinforcement, recruitment, behaviour change and financial support to extremist causes and groups. As such, understanding how platforms function together is more important than focusing on any one platform in isolation. The movement from public to private spaces can also reduce visibility for platforms, researchers and authorities, making harmful interactions more difficult to identify and assess. This suggests that effective prevention should combine public-platform moderation with cross-platform cooperation, community awareness, and rights-respecting approaches to activity occurring in more private digital environments as illustrated in Figure 5 below:

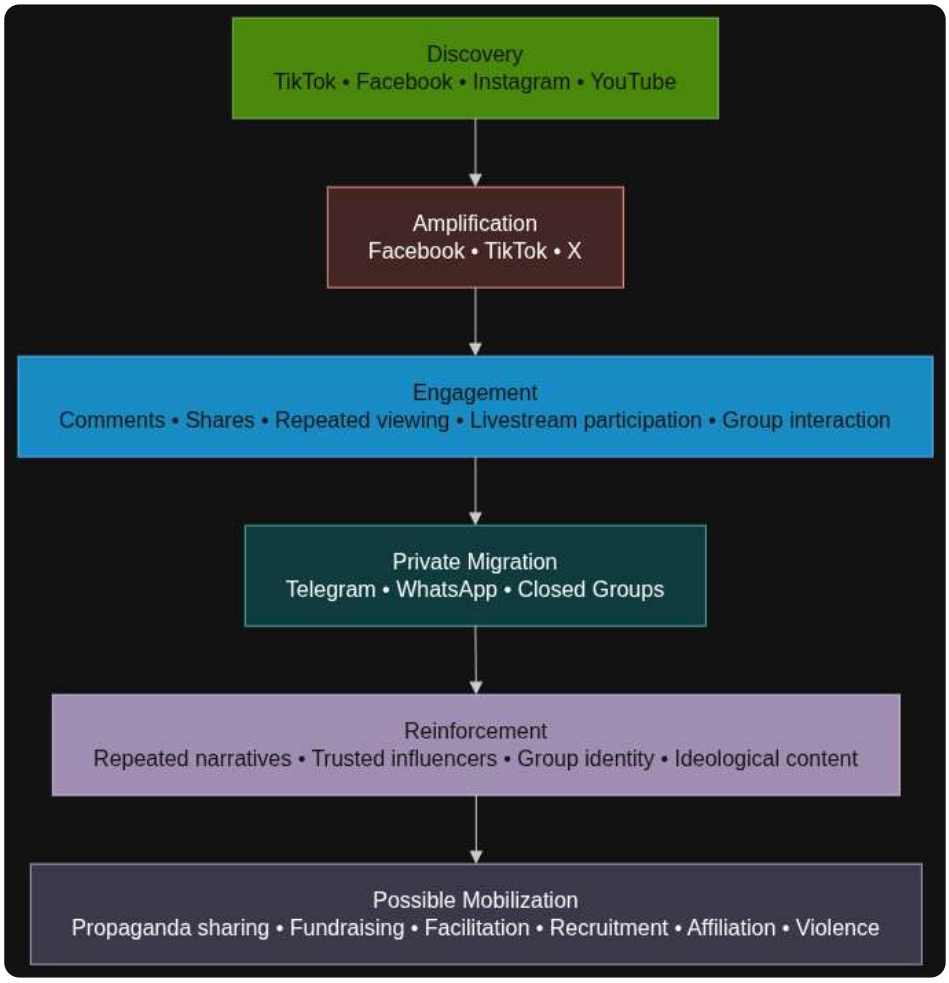

Figure 5: Public-to-Private Migration across the Digital Platform Ecosystem. Source: HORN Institute.

3.2.4 Online Extremist Messaging, Gains, Reach and Resonance

a. Content Formats

Short-form video and livestreaming were the most frequently identified content formats, reported by 66.7 per cent and 60.0 per cent of the respondents, respectively as illustrated in Figure 6 below. The prominence of such content suggests that visually immediate and interactive content is particularly important for attracting attention, increasing visibility, and encouraging early engagement.

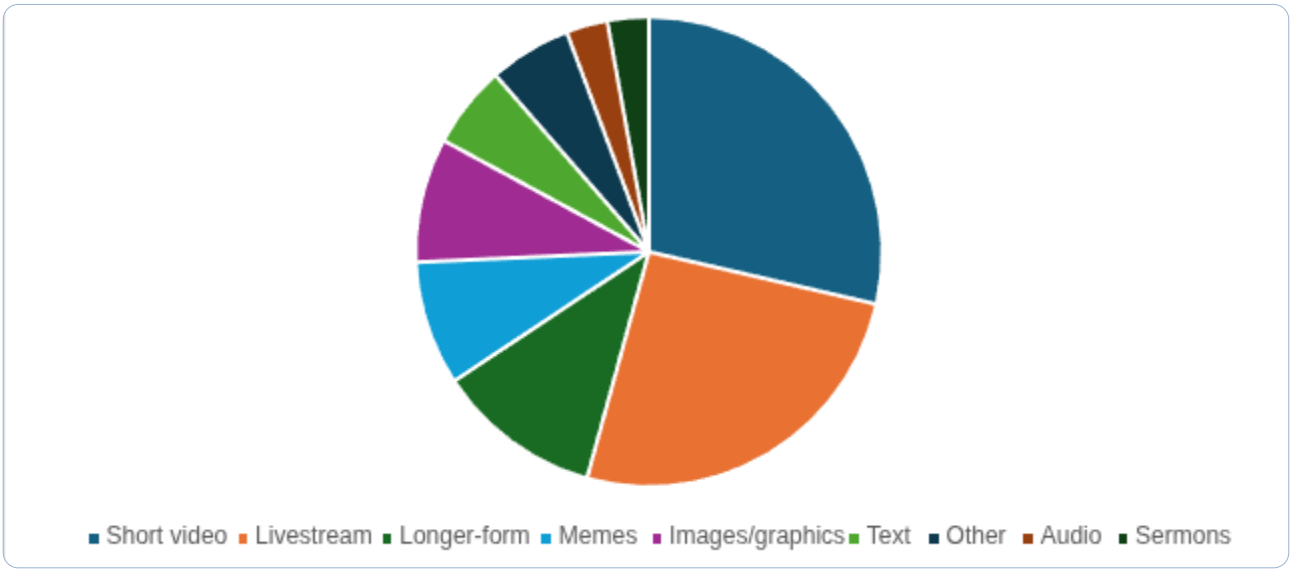

Figure 6: TVEC Formats on Digital Platforms. Source: HORN Institute.

Longer-form material was identified less frequently but may serve a different function by providing greater space for ideological explanation, narrative reinforcement, and sustained engagement. The findings therefore suggest that content format should be understood in terms of function as well as frequency, with different formats supporting different stages of the digital engagement process.

b. Language and Localisation

Arabic was the most frequently identified language with diaspora-linked online radicalisation, cited by 73.3 per cent of the respondents, and followed by Swahili at 46.7 per cent and Somali at 40.0 per cent English was also relevant, although less prominent, while French, Amharic and Oromo appeared in more specific contexts related to localised conflicts in DRC and Ethiopian (Amharic and Oromo) as illustrated in Figure 7 below:

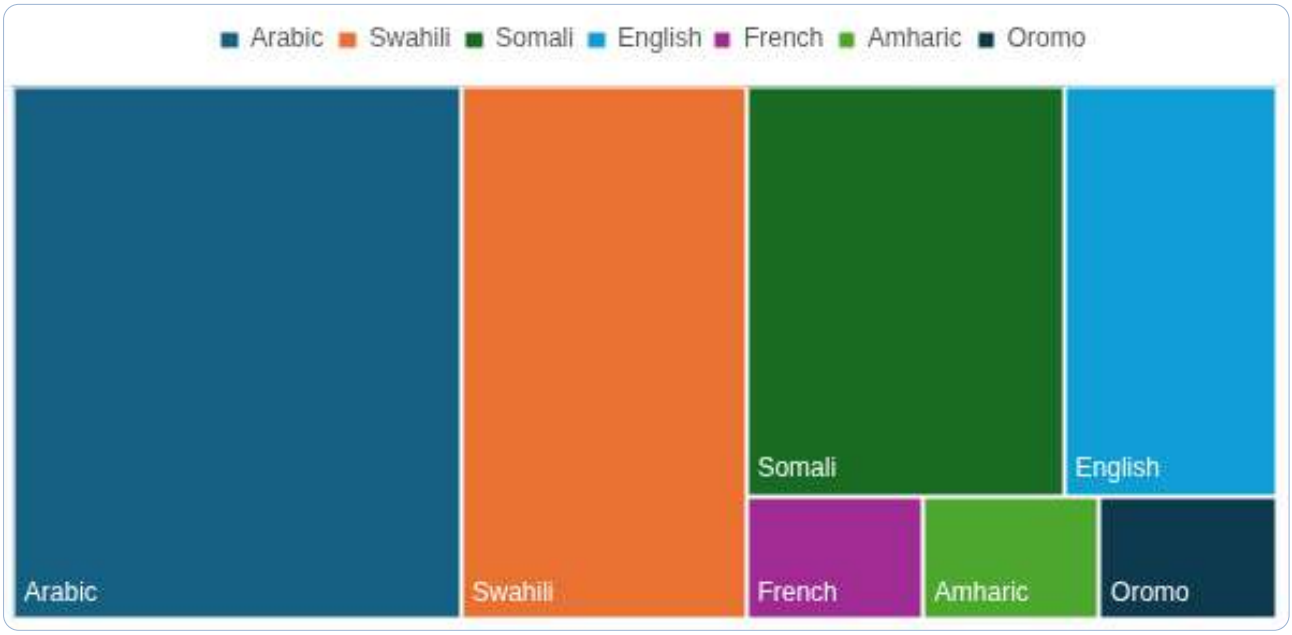

Figure 7: Language Distribution and Localisation of Extremist Messaging. Source: HORN Institute.

The findings highlight the importance of language localisation and contextual understanding, particularly because extremist or conflict-related messaging can be adapted to regional languages, dialects, slang and culturally specific expressions that may be harder for automated moderation systems to interpret accurately. The findings indicate that language plays different functions across the regional digital ecosystem. Arabic was associated with broader transnational and religious discourse as well as Middle Eastern and Levantine diaspora, while Somali was particularly relevant to Somalia and Somali diaspora networks in Eastern Africa, North America and Europe. Arabic was also associated with the violent extremism related to the civil war in Sudan between Rapid Support Forces (RSF) and Sudan Armed Forces (SAF). Oromo and Amharic languages are similarly instrumental to diaspora-based networks linked to localised ethno-nationalist struggles and armed conflicts in Ethiopia. Swahili extended regionalised messaging across East Africa and parts of Central Africa and is useful for its usage of locally embedded idioms and coded expression. English supported international and diaspora communication in North America and Europe. The DRC context highlighted the combined relevance of French and Swahili. These patterns reinforce the need for moderation systems and prevention strategies that account for regional language use, local context and multilingual communication.

These findings suggest that language choice can support audience targeting and contextual adaptation, but these functions are qualitative findings rather than separate frequency measures. The moderation implications are equally important; English and, in some cases, Arabic material may be easier for existing moderation systems to process than Somali, Swahili, regional dialects or coded local expressions. This creates a potential localisation gap whereupon the same languages that provide cultural credibility and regional reach may also be those for which automated detection and contextual human review are less developed. Figure 8 below illustrates the language functions and geographic reach across the regional digital ecosystem.

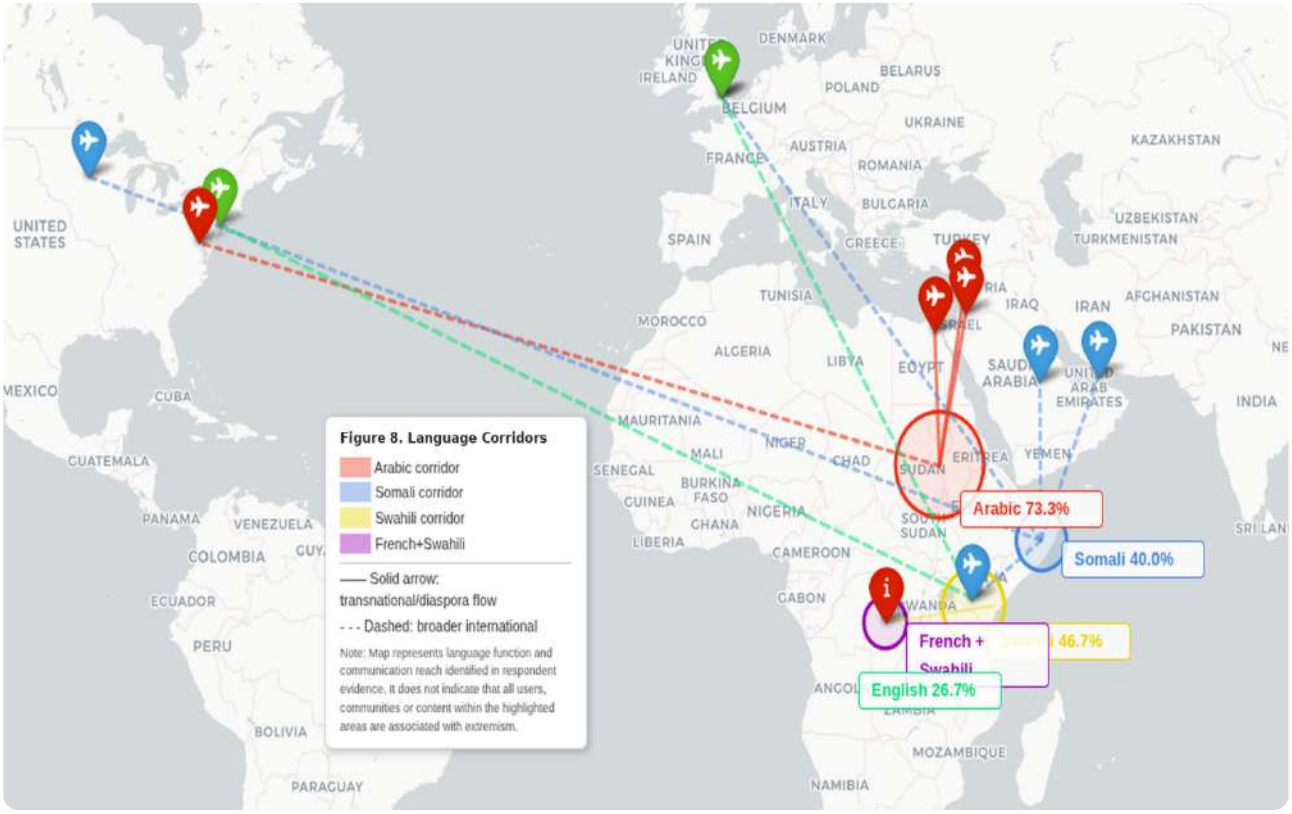

Figure 8: Language Functions and Geographic Reach across the Regional Digital Ecosystem. Source: HORN Institute.

c. Narratives and Grievances

The extremist narratives employed in diaspora-linked radicalisation reveal a multi-factor frame as opposed to single-factor mobilisation frames. Politics, conflict, geopolitics and Islamism in the Horn of Africa, which provide expedient mobilisation frames and narratives, can be situated within the motivational frames of diaspora-based extremists as illustrated in Figure 9 below.

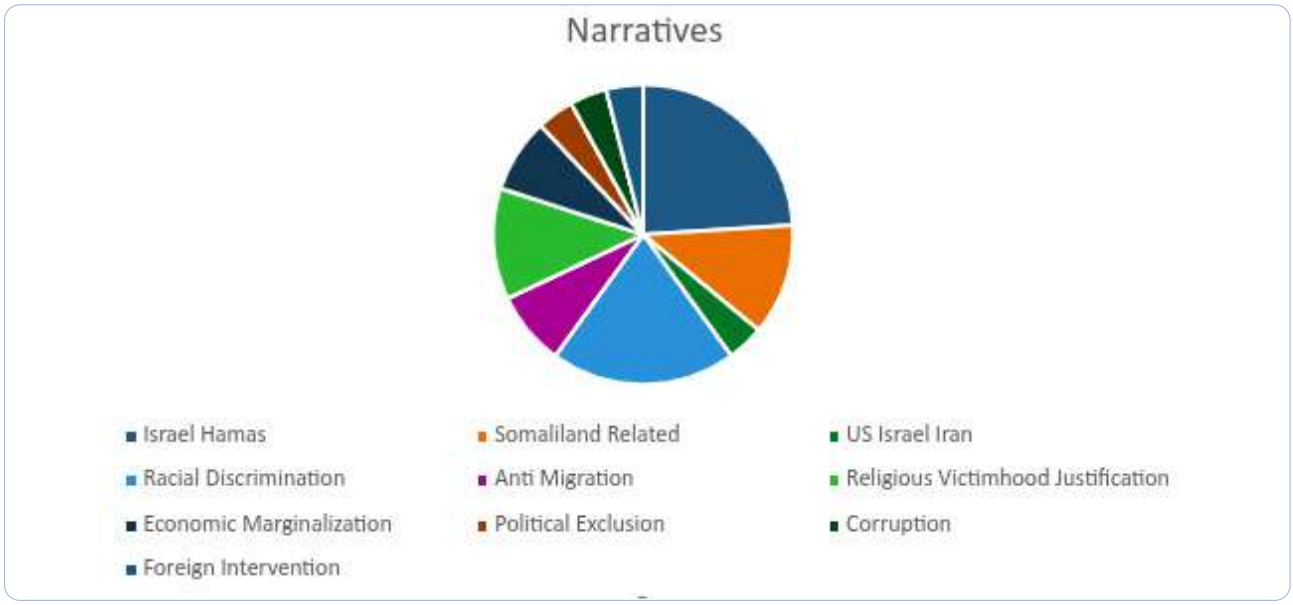

Figure 9: Drivers and Narratives for Diaspora-Linked Extremist Radicalisation. Source: HORN Institute.

The most frequently identified narrative was linked to Israel-Hamas-Palestine conflict (42.9 per cent), which is consistent with the "oppression of Muslims" narrative VEOs propagate; geopolitical events thus hold the strongest opportunistic value for extremist mobilisation and radicalisation. The narrative bridging strategy enables extremist organisations and the extremist networks within the Horn of Africa diaspora in Europe and North America, to link geopolitical events to local grievances and narratives, to gain powerful traction among existing sympathisers and gain new sympathisers driven singly by the respective geopolitical issue or event. Indeed, during the Hamas-Israel conflict, al-Shabaab-linked accounts circulated a graphic image of Palestinian children killed in the al-Ahli hospital blast before the story had been corroborated by international human-rights monitors, and drew direct comparisons between a September 2023 U.S. Africa Command strike in Somalia's Jilib district and Israeli air operations in Gaza, framing both as instances of the same "Western-backed" violence against Muslims. This was a deliberate two-track strategy: inciting the existing sympathiser base while using the higher-volume, less clearly attributable stream of pro-Palestinian content circulating globally to reach and identify new audiences for recruitment, since "enmeshed content" of this kind is far harder for platform moderators to disentangle from legitimate pro-Palestinian advocacy.[101]

Narrative bridging through exploitation of Hamas-Israel conflict in diaspora-linked radicalisation is followed by grievances of racial discrimination (35.7 per cent) that the diaspora communities face in host countries. This reveals extremist exploitation of poor integration and social tensions experienced by diaspora communities across Europe and North America. Grievances linked to Somalia's break-away region of Somaliland, consistent with extremist nationalist narratives of "defending the homeland" against "invasion" (outsiders and non-Muslims) and "traitors" (secessionists) ranked the third most common. Common narratives target Ethiopia's Memorandum of Understanding (MoU) with Somaliland, which was interpreted as quasi-recognition of Somaliland's sovereignty, and Israel's subsequent recognition of Somaliland's sovereignty.[102]

Diaspora extremists have called for "jihad", a weaponisation and instrumentalisation of religion and theological concepts in pursuit of political ends (defence of Somalia's territorial integrity couched as "Muslim land") against Israel (non-Muslims) and the people and officials of Somaliland (traitors and collaborators). The role of the diaspora extremists has not been limited to radicalisation and mobilisation, but has included raising resources (fighters and finances) to "jihadist" ends; they have either flown back as fighters in the regional conflicts as between Somaliland and the emerging North East state of Somalia over Las Anod disputed territory or urged Somalis in the region to either take up arms or mete extreme hostility to "weak" Somali officials and citizens unwilling to respond forcefully against Somaliland.

Social media evidence corroborates the instrumentalisation of "jihad" and digital platforms as well as diaspora networks and influence on shaping extremist and militant causes in Eastern Africa as in the case of Somalia and the question of Somaliland's separatism. The call to "jihad" in defence of Somalia's territorial integrity is shared by al-Shabaab and the extremist members of the Somali diaspora

online, persuading at-risk individuals with the idea of martyrdom (dying for one's faith, rewarded by God) for their participation in jihadist violence in defense of "Muslim lands" and the Ummah, against perceived "enemies of Islam" or "traitors". More recently, in June 2026, al-Shabaab issued a lengthy Arabic-language statement condemning Somaliland's opening of a diplomatic mission in Jerusalem following Israel's late-2025 recognition of the break-away territory, invoking the same anti-"Zionist" and anti-"crusader" framing while calling on Somalilanders to reject their government's authority, illustrating how the group continues to fuse the Israel–Palestine narrative with domestic Somali political fault lines even as its operational rhetoric has moderated somewhat compared with 2023.[103]

The excerpts below are translated from videos circulated on social media (X and TikTok) showing diaspora extremists spreading violent extremist ideologies and revealing their role in radicalizing at-risk populations in Eastern Africa into violent extremism of different forms (jhadist and nationalist):

In one video file on TikTok, a section of the Somali diaspora in Minnesota (U.S.) are holding a meeting themed "MINNESOTA, *KULANKA DIFAACA DALKA HOOYO*" (Minnesota Council for National Defence), in which speakers aim to build consensus among the participants (members of the Somali diaspora) on the instrumental and strategic urgency of "jihad" against Ethiopia and Somaliland. The meeting underscores the division of labour as ideological, material and financial support (diaspora extremists); and jihadist war-fighting (home-country extremists) respectively. One speaker is heard openly saying[104]:

- ✓ ".....you MUST DECLARE JIHAD.[105] The president has to declare JIHAD." The speaker seeks to portray the current official policy of diplomacy and dialogue of the Somali government towards Ethiopia and Somaliland as weak, and militaristic "jihad" as an effective instrument of policy towards Somaliland and Ethiopia.
- ✓ "....first, it [declaration of jihad by Somalia's president] will install fear in Ethiopian troops' hearts.....yes! That fear will apply pressure [enough for Somaliland and Ethiopia to reverse course].... and second, it will unite all Somalia."[106]
- ✓ "...any Somalian who dies fighting will gain a religious reward."[107]
- ✓ "....and lastly, unity [sic]...the five pointed star of Greater Somalia [representing Somali irredentism which claims North-eastern Kenya, Djibouti and South-eastern Ethiopia. Such irredentism led to the 1963-67 Shifta War between Kenya and Somalia, and the 1977-78 Ogaden War between Ethiopia and Somalia] ..... Do y'all [you all] support it? ...shall we seek it?"[108] .....to which the attendees respond emphatically in affirmative.

In another video on TikTok, a member of the Somali diaspora in Minnesota (U.S.), standing in the building of the Minnesota State Capitol, openly calls all Somalis globally to "jihad" against Somaliland, justifying extremist violence on religious grounds. He says[109]:

- ✓ "...this is JIHAD ...we will fight them [Somaliland Government] until the last man".[110]

- ✓ "I am informing the people of Las Anod [an anti-separatist clan occupying the territory of Las Anod disputed between Somalia's Federal Government and the authorities in Somaliland] to FIGHT and this is [sic] JIHAD for the sake of AL-LAH".[111]
- ✓ "....Weapons [are readily] bought [sic] and we have more weapons and money than them [Somaliland authorities]", and adds that "....we will bring weapons from Ukraine and South Africa".[112]
- ✓ "I swear to Allah we will bomb [preferred method and weapon] them [Somaliland] and bury their dead". [113]

The speaker resorts to threats directed at all Somalis [in the diaspora and home-country], saying [114]:

- ✓ "What will you say in the hereafter [to Allah if you refuse to fight]".....The one who REFUSES to take part in this JIHAD is a COWARD". [115]
- ✓ "May Allah make that person [non-combatant] experience hellfire on this earth and the hereafter". [116]
- ✓ "To the ones who refuse [to join this Jihad] and finance this war, may Allah burn you in hell". [117]

Other excerpts of several videos on X (formerly Twitter), captures a member of the Somali diaspora in Sweden boasting [truthfully or not] of providing financing support and fuelling armed conflict between in Las Anod [disputed between Somalia and Somaliland], especially between secessionist clans and unionist clans, following Israel's recognition of Somaliland in 2025. He calls all ["right-thinking"] Somalis to join him in the war and pledges to travel to the battlefield to join others in "wiping the town clean" of separatist sympathisers. He says [118]:

- ✓ "The Harti (a member of an East Sool clan opposed to Somaliland's independence from Somalia) who is martyred or injured [in Las Anod] is a JIHADI ..... while the Idoor (derogatory term for the Isaaq clan which supports Somaliland's independence) who is killed by [anti-Somaliland fighters in Las Anod] is an INFIDEL [deserving of punishment by death as per jihadi edicts]", and that, "...They [the Isaaq clan] will not be able to escape the hellfire". [119]
- ✓ "This [jihad] is because we [anti-Somaliland fighters in Las Anod] have a righteous plight ...while others [Somaliland armed forces] stand for injustice [secession and betrayal]". [120]
- ✓ "I swear anyone who works for the enemy in this town is finished even if they are my own brother." [121]
- ✓ "Anyone who works for Idoor [derogatory term for the Isaaq clan] or is an informant, our forces [anti-Somaliland fighters in Las Anod] are ordered to apprehend them and execute them."[122]

Lastly, religious victimhood and clan/ethnic grievances were each identified by 21.4 per cent of the respondents, while anti-migration policies, and economic marginalisation in Europe and the U.S. were each identified by 14.3 per cent of the respondents. The findings suggest that extremist or mobilising narratives are most effective when they combine broader geopolitical events with locally meaningful experiences of exclusion,

identity conflict, injustice, or marginalisation through narrative bridging. Broader geopolitical developments, such as the Israel-Hamas / Palestine conflict, thus gain greater influence when they are framed through experiences of discrimination, marginalisation, exclusion, or communal threat. As such, extremists or mobilising narratives often become effective not because of global events alone, but because those events are linked to locally meaningful grievances and identity-based interpretations. The result is a sense of perceived injustice, which can generate emotional resonance and increase the likelihood of engagement with TVEC.

d. From Exposure to Possible Mobilisation

Exposure to digital TVEC was found not to automatically lead to radicalisation, and radicalisation did not automatically lead to violence; the pathway to radicalisation into violent extremism is mostly non-linear as identified by 90 per cent of the respondents. Ideological reinforcement and sympathy, cited by 80 per cent of the respondents, are the most likely to play a key role in online radicalisation, while repeated engagement was cited by 70 per cent of the respondents, initial exposure and offline factors by 60 per cent and private groups by 50 per cent. However, in terms of behavioural outcomes, 30 per cent of the respondents described online extremist radicalisation as likely to contribute to recruitment, while 50 per cent cited violence and 30 per cent cited fundraising (terrorist financing) as shown in Figure 10 below:

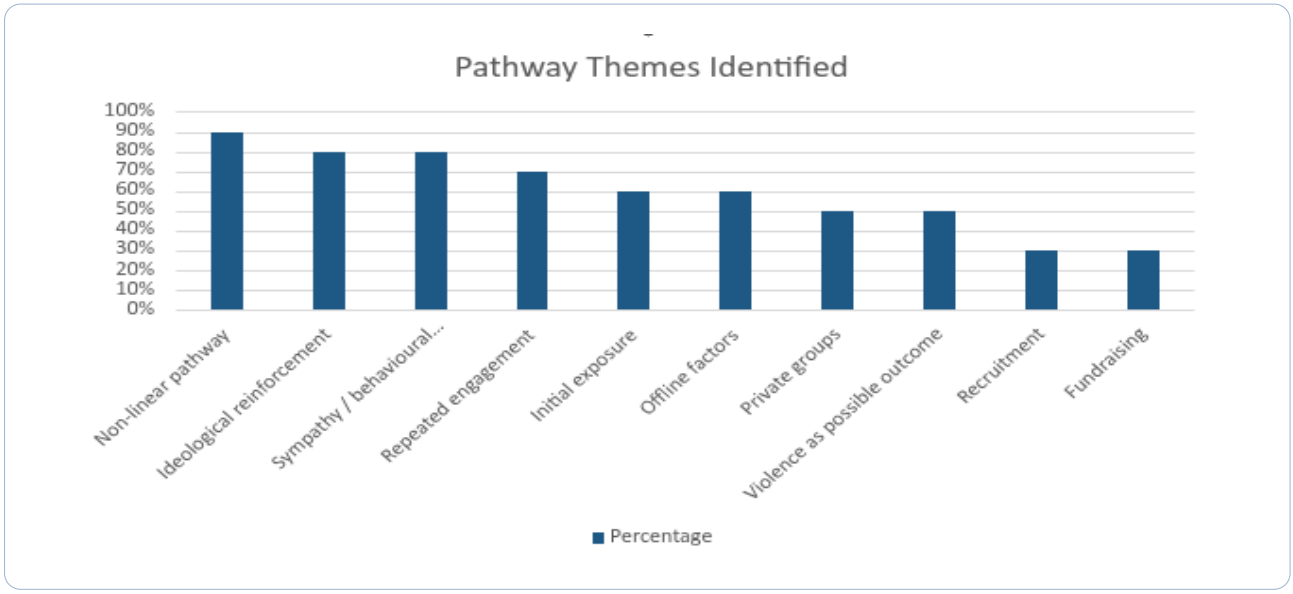

Figure 10: Pathways to Extremist Radicalisation and Mobilisation Online. Source: HORN Institute.

Radicalisation is thus not a fixed or automatic sequence; instead, the process may involve initial exposure, repeated exposure, movement into private groups, or communities, and contact with broader networks, ideological reinforcement, and different forms of behavioural support. These stages should not be interpreted as a fixed sequence, as individuals may move between stages, disengage, reject the content, or remain at non-violent levels of sympathy or support.



Figure 11: Radicalisation Pathway: From Initial Exposure to Possible Mobilisation. Source: HORN Institute.

The findings further show that online engagement interacts with offline factors, including conflict, discrimination, economic pressure, identity, social relationships, and displacement. This means digital content should be understood as part of a broader social and political environment rather than an isolated cause. Violence, recruitment and fundraising are possible outcomes, but they are not inevitable end points for everyone exposed to extremist or mobilising content. The pathway emphasises that exposure alone does not constitute radicalisation and radicalisation does not automatically result in violent action, particularly because online engagement is shaped by wider offline conditions, relationships, identity, and personal circumstances.

A consistent finding is the role of algorithmic recommendation systems in driving the pathways to violent extremism. A respondent observed that

> *"The progression often begins with algorithm-driven exposure. A person may initially encounter relatively general content because it matches interests. As the person interacts with this material (by watching, liking, commenting, or following related accounts) the platform's recommendation algorithms may continue to feed them similar content. Over time, they get connected to increasingly ideologically committed accounts and online communities. The content may gradually become more extreme, moving from religious/political messaging to explicit extremist narratives, glorification of violence and, in some cases, calls for action. At the same time, individuals can become part of closed or semi-closed online communities where these views are reinforced by other users. Thus, the pathway involves repeated exposure, algorithmic reinforcement, social connection and "normalisation" of increasingly extremist content, which may lead individuals to mobilisation and action."*[123]

A three-stage pattern can be observed: the first is the narrative stage, where a geopolitical event (foreign intervention, transnational war, great-power conflict) is reframed by extremist propagandists as evidence of Western or state hostility toward the diaspora's religious, ethnic, or national in-group, activating identity grievance among individuals already navigating host–home identity tension. The second is the mobilisation stage at which the extremist narrative is operationalised through peer networks, prison contacts, and increasingly closed-loop online ecosystems (encrypted chats, algorithmically amplified short-form video) that convert grievance into willingness to travel, recruit, or act, often within pre-existing friendship or family circles. Finally, is the financing stage where diaspora remittance infrastructure built for legitimate family and community support (hawala corridors, informal value transfer, diaspora crowdfunding, and non-profit channels) is exploited, sometimes with the knowledge of a small number of participants and sometimes through the diversion of funds raised for unrelated purposes, to move resources to designated organisations in the diaspora hubs. The second and third stages may occur simultaneously or non-linearly depending on the levels of radicalisation and choices made by the radicalised individuals.

3.2.5 Vulnerability to Diaspora-Based Online Radicalisation

The most vulnerable demographic group by diaspora-based online radicalisation is the home-country youth (78.6 per cent), followed by deportees and the diaspora youth (seven per cent). In terms of factors contributing to vulnerability to diaspora-linked radicalisation, unemployment plays a major role 28.6 per cent followed by marginalisation, social isolation, and economic disadvantage (14.3 per cent), while displacement plays marginal role (seven per cent). The vulnerability is thus an intersection of social, economic, and identity-related pressures, rather than as a characteristic of any one demographic group as shown in Figure 12 below:

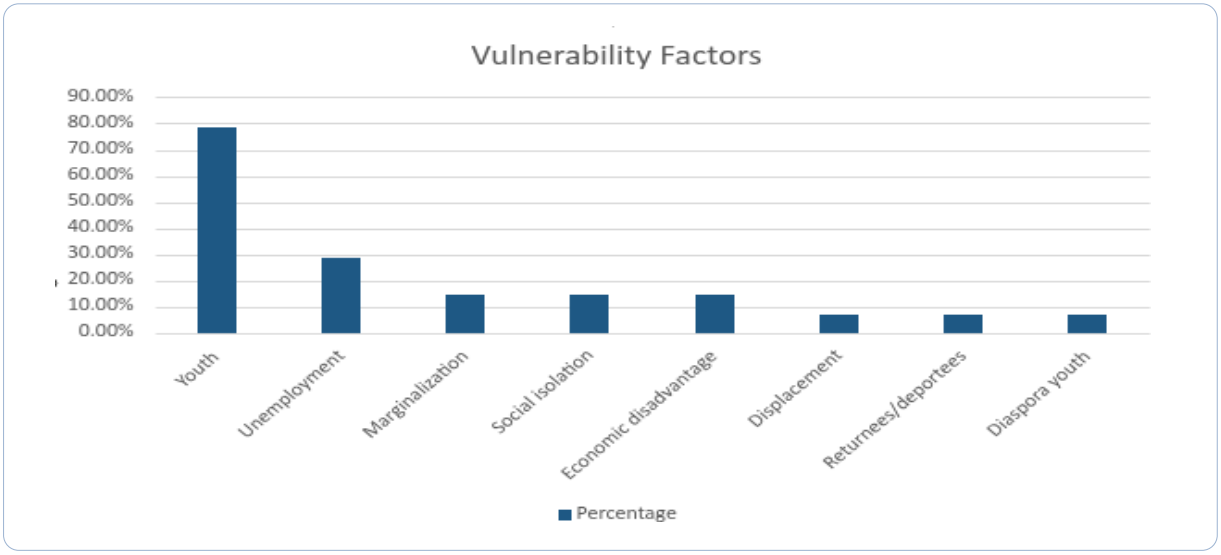

Figure 12: Vulnerability Factors and Vulnerable Groups to Diaspora-Based Extremist Radicalisation. Source: HORN Institute.

Although the home-country youth were the most frequently identified group, the respondents consistently linked vulnerability to wider social and economic circumstances. Unemployment, social isolation, marginalisation, displacement, conflict exposure, identity uncertainty and economic pressure can overlap and reinforce one another, creating conditions in which extremist or highly polarising narratives may gain greater emotional relevance. These factors do not operate uniformly; a young person experiencing unemployment and social isolation, may encounter online narratives very differently from another young person with strong social support, economic opportunities, and trusted community networks. Similarly, displacement or conflict exposure may heighten feelings of insecurity or injustice without necessarily resulting in radicalisation.

The findings therefore support an intersectional understanding of vulnerability, in which digital exposure interacts with individual circumstances, relationships and offline environments. Given that vulnerability is an intersection of circumstances (offline and online), not membership in a demographic category, interventions based on broad demographic profiling only risk stigmatising communities while overlooking the underlying conditions that make extremist narratives more persuasive. Prevention should therefore prioritise resilience, opportunity, belonging, trusted relationships, integration and inclusion, and access to support, rather than attempting to identify a fixed demographic profile of a person likely to radicalise or be radicalised.

Table 2: Intersectional Vulnerability to Diaspora-Based Online Radicalisation. Source: HORN Institute.

Vulnerability factor	Potential relevance
Youth	Period of identity formation, high digital engagement and greater exposure to online social networks
Unemployment	May increase frustration, economic insecurity and perceptions of exclusion
Identity uncertainty	Can increase receptiveness to narratives offering belonging, certainty or purpose
Social isolation	May increase dependence on online communities for recognition and social connection
Conflict exposure	Can strengthen grievance, insecurity, anger and perceived injustice
Displacement	May involve disrupted social networks, loss of livelihoods and weakened community support
Marginalisation	Can reinforce perceptions of discrimination or political and social exclusion
Economic pressure	May deepen dissatisfaction and increase susceptibility to narratives centred on inequality or injustice

3.3 Terrorist Financing

3.3.1 Diaspora-Linked Terrorist Financing

The threat of diaspora-based financing for VEOs in the Horn and Eastern Africa, was only confirmed by 30 per cent of the respondents, indicating the limited scale of such a threat as shown in Figure 13 below:

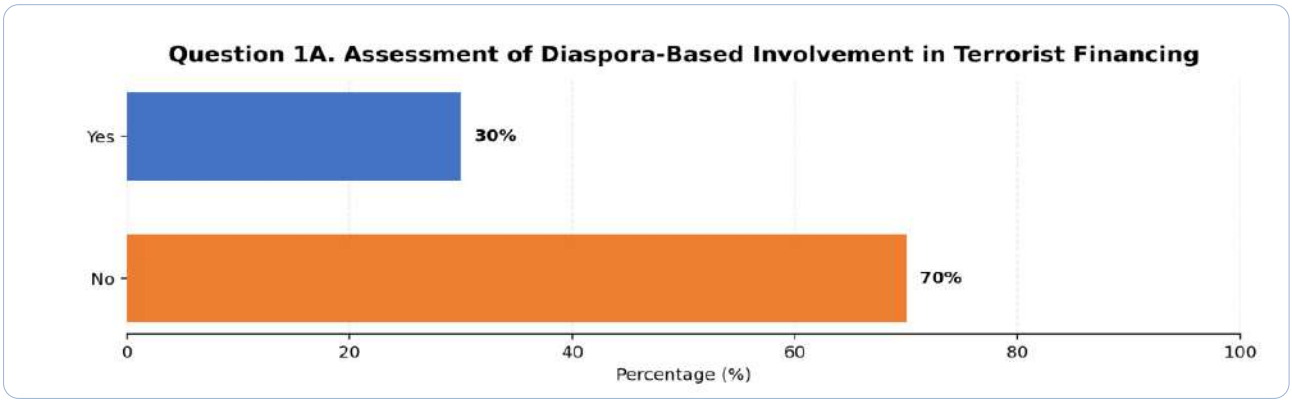

Figure 13: The Role of the Diaspora in Terrorist Financing. Source: HORN Institute.

However, the role of the diaspora in financing militant and extremist causes is at play in Eastern Africa, only the scale is difficult to estimate. As a respondent working for AML/CTF agency argued,

> *...it is difficult to determine the precise scale of diaspora financing because extremist groups exploit informal remittance and financial channels, making diaspora-linked flows difficult to identify and quantify. Once funds reach the region, the predominantly cash-based nature of many economies in the Horn and wider East Africa further complicates efforts to trace the movement of funds across jurisdictions.*[124]

The excerpts below are translated from a leaked audio recording circulated on TikTok, documenting a fundraising discussion among members of a Somali diaspora group in the UK mobilising funds for militant action against Somaliland, including the purchase of weapons through a London-based committee (recording on file with HORN Institute):

- ✓ "I would like you all to complete your duty and send funds [to purchase weaponry]."[125]
- ✓ "A committee in London responsible for sending these funds also exists."[126]
- ✓ "These efforts [to purchase weapons] are primarily coming from the diaspora."[127]

In another excerpt of a video on X (formerly Twitter), a member of the Somali diaspora in Sweden is captured [truthfully or not] revealing his role in a jihadist campaign against Somaliland authorities and pro-secession citizens, which involves financial support to those heeding his jihadist call. He says:[128]

- ✓ "I am the one funding this war [against Somaliland]."[129]

- ✓ "This war is multifaceted and I am the one funding the firing of weaponry [against Somaliland]."[130]
- ✓ "Some men fight [with arms] while others fight by fuelling [this war] and providing funds."[131]

In terms of the diaspora hubs associated with terrorist financing, North America (U.S.) was identified by respondents 49 per cent as the leading, followed by Europe (35 per cent), Eastern Africa (ten per cent), and lastly, the Middle East (six per cent) as shown in Figure 14 below.

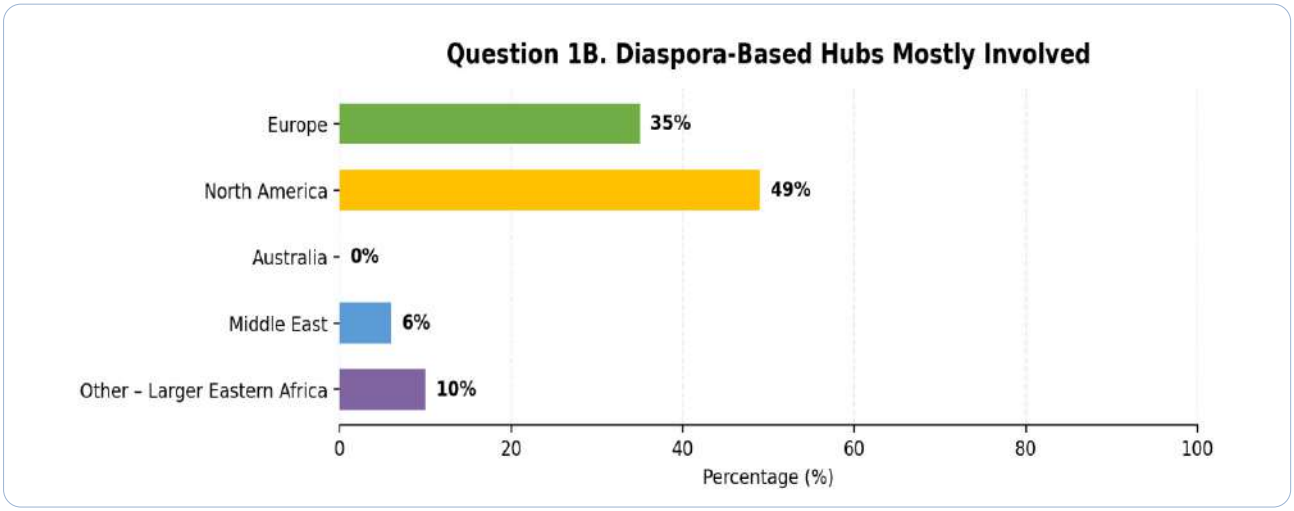

Figure 14: Role of Diaspora Hubs in Terrorist Financing. Source: HORN Institute.

In terms of the channels most commonly used to transfer funds by diaspora extremist sympathisers to VEOs and militant causes in Eastern Africa, hawala networks were widely reported by 48 per cent of the respondents, followed by cryptocurrencies (30 per cent), mobile money (15 per cent), social media appeals (five per cent), and lastly banks (two per cent) as shown in Figure 15 below:

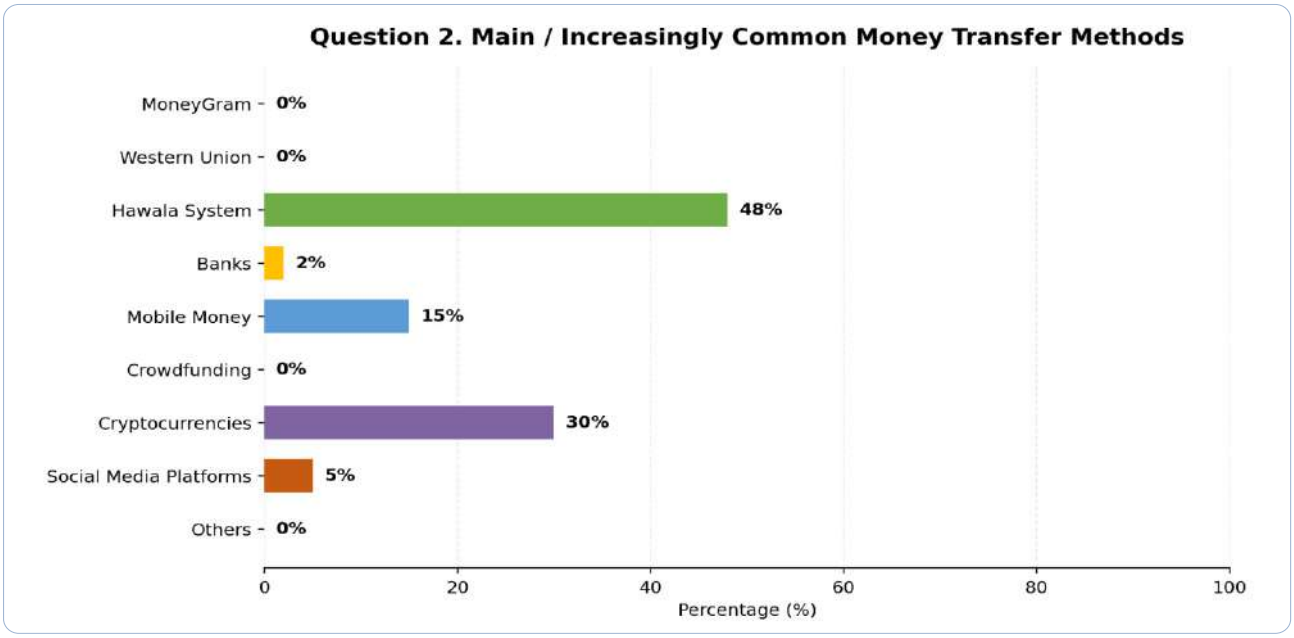

Figure 15: Channels for Diaspora-Linked Terrorist Financing. Source: HORN Institute.

The findings above point to various factors including the size of regional diaspora communities in the respective hubs whereupon North America leads, financial regulatory and AML/CTF gaps both in the diaspora hubs and in home countries in Eastern Africa, which enable the flows of funds to VEOs and other militant causes in Eastern Africa. However, the key finding is that AML/CTF regulations and frameworks are more effective in the mainstream financial sector organisations and channels such as banks and money transfer organisations such as Western Union. A respondent in Kenya observed that,

> *Even though as a country we are grey-listed, there have been robust mechanisms to curb terrorist financing from international destinations and even locally...we have some of the most thorough Know Your Customer (KYC) frameworks and financial monitoring...actually any amount above 77 U.S.-dollars is captured and monitored if it an international transfer*[132]*....*

However, as another respondent observed,

> *Banks and established money transfer companies such as Western Union are not entirely secure from terrorist financing....there have been cases of al-Shabaab fronting third parties to open bank accounts as proxies and collect the remittances as legitimate ...also such proxies can open multiple bank accounts or accounts in different banks...the regulatory frameworks here [Somalia and Eastern Africa] are not that strong to quickly pick such patterns and curb terrorist financing by sympathisers abroad*[133]*...*

This is reinforced by a respondent's explanation that

> *....alongside the use of informal remittance channels, al-Shabaab continues to exploit formal money-transfer services, including Western Union, to facilitate the movement of funds. The group reportedly relies on individuals who are not subject to sanctions to facilitate such transactions and obscure the identity of the ultimate beneficiaries.*[134]

The under-regulated crypto-currency networks are more vulnerable to terrorist financing as well as the mobile money networks; however, the use of these technologies is not uniform across VEOs across Eastern Africa. With regard to cryptocurrency, a respondent working in the AML/CTF Eastern and Southern Africa indicated that he had not observed significant use of digital technologies by al-Shabaab in his work. However, he added that their work had identified instances involving the Islamic State Central Africa Province (ISCAP) in which cryptocurrency had been used.

Overall, digital technologies have expanded the reach, speed, and accessibility of extremist fundraising, while simultaneously creating challenges for enforcement agencies in identifying dispersed, small-value contributions and distinguishing legitimate online fundraising from terrorist-financing activity. While social media appeals play a limited direct role in terrorist financing, they are instrumental as a mobilisation tool. As a respondent observed,

> *Social media has made it easier for extremist groups to reach diaspora communities, disseminate narratives,*

> *and mobilise financial support. In particular, social media platforms can be used to communicate and amplify narratives about prevailing situations in conflict-affected areas, which can be used to generate sympathy and encourage diaspora communities to provide financial assistance.*[135]

In the case of Somalia where remittances from the diaspora and humanitarian aid and givings, sustain livelihoods across the country, extremist groups have exploited such networks and funds to mobilise their own revenues. As one respondent observed,

> *Al-Shabaab has demonstrated an ability to exploit prevailing humanitarian and social circumstances, particularly in Somalia, to solicit financial support from diaspora communities. Such fundraising may be conducted through community-based structures and framed as support for vulnerable populations, including children, although the funds may subsequently be diverted for other purposes……there are regulatory and legislative gaps in the governance and oversight of non-profit organisations (NPOs) in the region, which can create vulnerabilities for the misuse of charitable and community-based structures. Weaknesses in regulatory frameworks and oversight mechanisms may therefore make it more difficult to distinguish legitimate charitable activities from organisations or fundraising initiatives that are being exploited for terrorist financing.*[136]

Other strategies used for revenue collection domestically by groups such as al-Shabaab, especially extortion, are also applied to the Somali diaspora. As a respondent noted,

> *Al-Shabaab engages in extortion of members of the Somali diaspora, particularly by leveraging threats against their families, businesses, or other assets in Somalia. In addition, the group reportedly solicits Zakat contributions from members of the Somali diaspora, particularly wealthy individuals who maintain family, business, or other ties to Somalia.*[137]

It is thus important to adopt a risk-based approach when strengthening oversight mechanisms. The overly broad or restrictive measures could unintentionally disrupt legitimate financial flows to genuine non-profit organisations that provide essential services to vulnerable populations in Eastern Africa as well as legitimate remittances that support households' socio-economic needs in the region. The efforts to address terrorist-financing risks should thus seek to strengthen transparency, and information-sharing while preserving legitimate humanitarian and charitable activities.

3.3.2 Challenges in Curbing Diaspora-Linked Terrorist Financing

Beyond the nature of the crime and the financial channels for terrorist financing, several key challenges were observed:

Limited Institutional Capacity: limited institutional capacity and weak transnational coordination are significant obstacles to detecting and estimating terrorist-financing flows. In particular, relevant institutions may lack adequate personnel, specialised expertise (in terrorist financing typologies), and resources to effectively identify transactions associated with terrorist financing.

Weak coordination and information-sharing among mandated financial and law-enforcement institutions, both nationally and across jurisdictions undermine effective monitoring and curbing of financial flows to extremist groups. Such institutional and coordination gaps create vulnerabilities that extremist groups can exploit, making it difficult to establish the scale, origin, and destination of diaspora-linked financial flows with confidence.

Informal Channels: the informality of remittance networks is the major challenge to curbing terrorist financing given their operations by-pass mainstream finance and banking infrastructure which can easily help detect and curb such flows.

3.3.3 Platform Moderation: Effectiveness and Gaps

a. How Effective Is Platform Moderation?

Among the respondents, 37.5 per cent characterised platform moderation as having limited effectiveness, while a further 37.5 per cent described it as mixed or conditional. Moderately effective and ineffective assessments each accounted for 12.5 per cent, while no respondent categorised moderation as fully effective as illustrated in Figure 16 below.

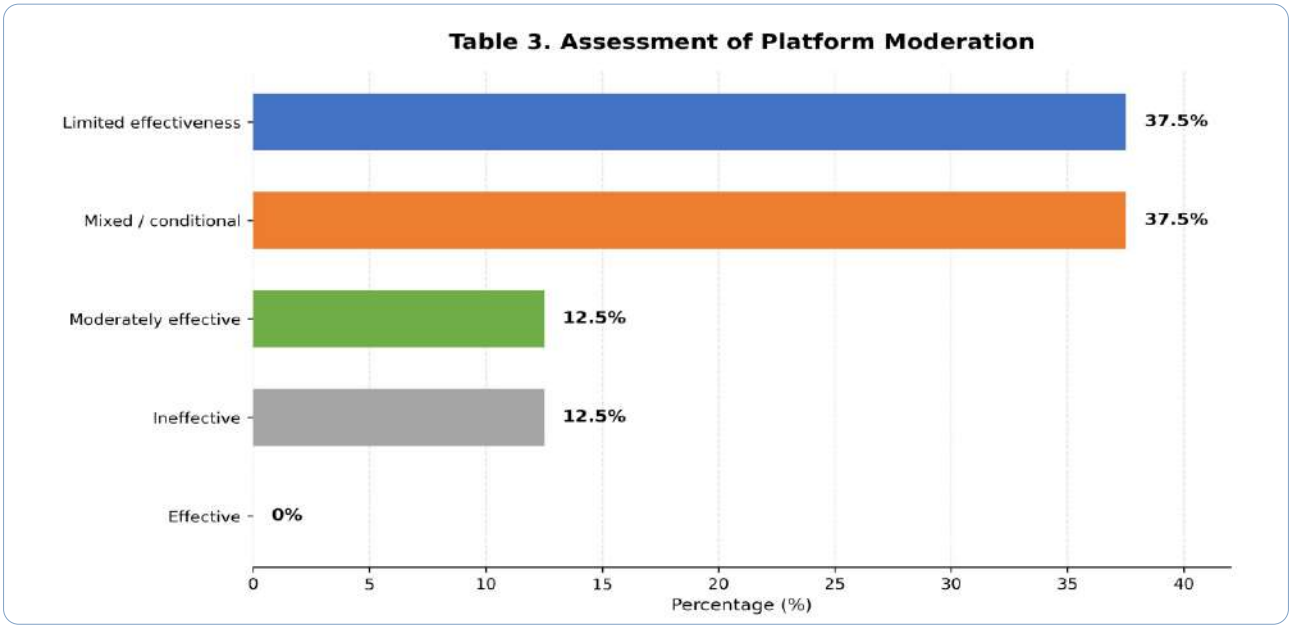

Figure 16: Platform Moderation Effectiveness against TVEC. Source: HORN Institute.

Majority of the respondents (75 per cent) characterised the effectiveness of content moderation as either limited or mixed or conditional, suggesting that the main issue is not simply whether platforms moderate content, but how consistently and contextually they are able to do so. Moderation may perform relatively well against clearly identifiable material while struggling with rapidly changing terminology, local grievances, coded language, dialects and content whose harmful meaning depends heavily on regional context. As a respondent explained,

> *Overall, the effectiveness remains poor. Social media platforms' rules are not applied consistently, and extremist content can remain online or reappear quickly after removal. Detection systems are generally more effective in major languages such as English and Arabic, while they can be significantly weaker in languages such as Somali and Swahili, where there may be fewer training datasets, moderators and language-specific tools.*[138]

The findings suggest that platform exposure to extremist or highly polarising content is shaped not only by the presence of harmful users, but also by design, moderation, and governance weaknesses. These findings show that moderation failure is partly technical and partly institutional; for instance, platforms may be capable of detecting known accounts, symbols or previously classified material while remaining less effective when harmful communication uses new accounts, coded terminology, local languages, or rapidly changing political narratives. The problem is therefore not simply insufficient removal; it is also the difficulty of recognising harmful context early enough, following activity across an interconnected digital ecosystem and capacity to detect harmful livestreaming.

b. Platform Regulation and Content Moderation Challenges

Social media platforms are confronted by several challenges, which undermine content moderation and TVEC disruption. The main challenges against the current platform moderation efforts include:

Cross-platform persistence: the migration of extremist TVEC from one platform to the other, limits one platform's moderation efforts. As such removal of TVEC from one public platform does not necessarily eliminate harmful material from the wider digital ecosystem. TVEC can be reposted, archived, re-edited or transferred into other services, including more private channels where detection and intervention become considerably more difficult.

Local language capacity: Arabic, Swahili and Somali were among the most frequently identified languages used by diaspora extremists in the study, yet effective moderation requires more than literal translation. As such, the capacity to understand slang, coded references, religious terminology, humour, political grievances and locally specific historical references requires contextual expertise among content moderators. Digital platforms should thus invest in regional language capabilities and include human expertise alongside automated detection systems. This is especially important when the same phrase can have different meanings depending on location, speaker, political context, or community. As a respondent observed,

> *Another major gap is context. The same word, image, symbol or religious reference can have different meanings depending on the context, making automated detection difficult. Extremist actors can also adapt their language, use coded terms, memes, altered spellings, images and videos to evade automated systems*[139]

Livestreams and rapid amplification: Livestreaming presents a different challenge because content can circulate before traditional review mechanisms have sufficient time to respond. Even when a livestream is subsequently removed, recordings, clips and screenshots may already have been redistributed across multiple services.

Public-to-private migration: The findings also show why moderation cannot focus exclusively on visible public content. Exposure may begin through open platforms before discussion or interaction moves into closed groups, private messaging or invitation-only channels. This shift reduces visibility and makes prevention increasingly dependent on community awareness, platform cooperation, and lawful investigative procedures.

Cross-Platform and Cross-Jurisdictional Policy and Enforcement Gaps: Online radicalisation and extremist mobilisation frequently operate across several jurisdictions simultaneously. A message may be created in one country, distributed through a platform headquartered in another, amplified by diaspora-linked actors in a third jurisdiction and ultimately reach audiences elsewhere in the Horn of Africa or Eastern Africa. This creates a governance problem that cannot be resolved through domestic legislation alone but multilateral or bilateral cooperation. The challenge becomes particularly significant when authorities require timely evidence of preservation, account information, platform cooperation, or cross-border investigative assistance. Differences in national laws, evidentiary standards, data-protection rules and definitions of prohibited activity can delay investigations and complicate coordinated responses.

Algorithmic Recommendation: the algorithmic model focused on promoting or enhancing user-engagement with content online, risk creating radicalisation funnels by tracking user behaviour and increasing exposure to preferred content including TVEC, in the case of at-risk groups. As another respondent observed

> *...algorithmic recommendation is a structural and predictable contributor of radicalisation. While platforms do not officially endorse algorithmic radicalisation as an economic trade-off—their (in)actions effectively normalises it....For vulnerable young people, this can create a fast-track pathway into increasingly harmful communities and beliefs. Over time, repeated exposure can normalise violence, desensitise empathy, increase social isolation, and reinforce extremist worldviews inside online echo chambers*[140]

4.0 Conclusion and Recommendations

4.1 Conclusion

This study specifically set out to examine the role of Eastern Africa's diaspora based in Europe, America, the Middle East and the larger Eastern Africa region in: (i) driving extremist narrative ecosystems, mobilisation and radicalisation online, especially through social media platforms, and (ii) in terrorist financing in Eastern Africa. Of policy relevance, the study identified the drivers, triggers and vulnerabilities which shape the diaspora's involvement in extremist radicalisation, including social media platform moderation gaps and anti-terrorist financing regulatory and enforcement gaps across Europe, North America, and the Horn of Africa. The study thus focused on generating evidence-based, policy-relevant understanding on diaspora-linked online radicalisation, mobilisation, and terrorist financing affecting Eastern Africa's violent extremism.

Five key conclusions emerge from the study:

- The digital radicalisation environment is multi-platform: Interventions should focus on the digital ecosystem rather than individual platforms. Removing content from one service may have limited effect if users, narratives and communities simply migrate elsewhere. Platform cooperation and ecosystem-level risk assessment are therefore necessary.
- The environment is multilingual: Language is not simply a translation issue. Somali, Swahili, Arabic, English and other regional languages carry different cultural, political and religious meanings. Effective moderation requires linguistic competence combined with local contextual expertise.
- Radicalisation is non-linear: Digital exposure should not be interpreted as automatic evidence of radicalisation. Individuals may engage temporarily, disengage, reject extremist narratives, or remain at non-violent levels of sympathy. Prevention frameworks should therefore avoid rigid stage models and recognise multiple possible pathways and outcomes.
- Online and offline conditions interact: Digital platforms can amplify grievances, reinforce identities, and connect individuals with communities, but they do not replace the offline environment. Conflict, discrimination, economic insecurity, social relationships, marginalisation and displacement remain important influences on how online narratives are interpreted.
- No institution can respond alone: The scale and complexity of the digital ecosystem require coordinated action among technology companies, governments, law enforcement, civil society, youth organisations, religious leaders, diaspora organisations, and regional partners. Each actor controls only part of the environment in which prevention must occur.

4.2 Recommendations

The study indicates that no single intervention level is sufficient; the challenge are both a technology-governance issue as well as a wider security and social-policy issue. Community-based responses remain equally important because prevention ultimately depends on trusted relationships, credible messengers and the ability to address grievances before they become opportunities for extremist exploitation. The findings therefore strongly support a coordinated model in which technology companies, public institutions, and communities perform complementary roles:

✓ Platform level

Technology companies should reduce digital risks while preserving legitimate expression. Priority areas include:

- Improving local-language-and-content moderation;
- Employing or consulting regional experts for improved detection of coded and context-dependent content
- Social media platforms to develop a proactive counter-narrative approach by programming algorithms to suggest more empathic content that promotes equality and equity would ensure positive exposure to balanced content and interrupt radicalisation patterns
- Strengthening or ensuring faster response mechanisms for livestream and rapid-amplification;
- Reviewing recommendation systems to prevent harmful amplification patterns;
- Improving accessibility of user reporting and appeal mechanisms;
- Increasing transparency around regional moderation performance and enforcement practices.
- Enhancing coordination across platforms;
- Continued protection of privacy, due process and legitimate political or religious expression.

✓ Government level

Governments should strengthen institutional capacity without relying primarily on censorship or coercive intervention. Priorities include:

- Building digital-forensic capacity within the law enforcement agencies;
- Developing clearer legal and evidentiary procedures for such digital threats;
- Prevention-focused social and economic programmes; given the prominence of youth in the vulnerability findings, prevention should prioritise positive opportunities for young people. Employment programmes alone are insufficient; initiatives should also strengthen belonging, mentorship, civic participation, digital literacy, and trusted social networks.
- Narrative monitoring: tracking geopolitical trigger events in near-real time, should be built into early-warning systems; evidence shows measurable radicalisation effects within weeks of a major geopolitical shock.
- Strengthen efforts addressing marginalisation, social exclusion and conflict-related grievances.
- Rights respecting law enforcement

responses; avoiding profiling and protecting privacy, due process and freedom of speech. Law enforcement should avoid treating online exposure, political anger, or religious expression as equivalent to criminal intent. Investigation should focus on behaviour, evidence, and credible indicators of unlawful activity.

- Platform liaison: clearly identified channels through which authorised agencies can communicate with technology companies.
- Reciprocal-radicalisation monitoring: tracking both jihadist and far-right or identity-based extremist responses to the same geopolitical trigger, should be built into early-warning systems, since a single event has been shown to accelerate multiple, ideologically opposed threat streams concurrently
- Legal cooperation: stronger procedures for lawful information sharing and mutual assistance across borders.
- Creating common understanding: greater regional coordination around terminology, emerging threats and evidentiary standards.

✓ Community level

Communities provide an essential layer of prevention because they often understand local grievances and behavioural changes better than distant institutions. Community-based responses through diaspora organisations, civil society organisations, youth organisations, religious institutions and leaders, as well as community leaders should emphasise:

- Implementing programmes promoting digital and media literacy;
- Diaspora communities should be treated as partners in prevention rather than objects of suspicion. Diaspora organisations can provide insights into transnational information flows, challenge harmful narratives, support community dialogue, and connect prevention initiatives across countries
- Youth and community engagement; civil society organisations can bridge the gap between institutions and affected communities given their comparative advantage lies in local knowledge, trust, and the ability to communicate in culturally relevant ways. Programs should invest in community-led research, digital resilience, youth dialogue, as well as early support and referral mechanisms;
- Credible counter-messaging; religious and community leaders can help distinguish legitimate religious teaching from manipulative interpretations used to justify hostility or violence and develop credible alternatives to extremist or highly polarising narratives. Their effectiveness depends on credibility, independence, and meaningful engagement with young people rather than simply delivering top-down counter-messages.

4.3 Principles for an Effective Whole-of-Society Response

Effective prevention requires simultaneous action across the digital, institutional, and community environments in which radicalisation risks develop. Across stakeholders, five principles should guide implementation:

- **Context before content:** Harm cannot always be identified through keywords alone. Language, political context, identity, and intent matter.
- **Prevention before crisis response:** Investments in resilience, belonging and opportunity are more sustainable than relying solely on removal or enforcement after mobilisation occurs.
- **Follow the ecosystem:** Interventions should account for movement between platforms, formats, and private communication environments.
- **Work with communities:** Local communities, youth organisations, religious leaders, and diaspora organisations should participate in designing prevention responses.
- **Protect rights and avoid stigmatisation:** Counter-extremism interventions should uphold privacy, due process, legitimate expression, and non-discrimination.

5.0 Endnotes

1 Council on Foreign Relations 2022: Al-Shabaab [Backgrounder], 6 Dec 2022, in: https://www.cfr.org/backgrounders/al-shabaab [14 Sep 2026]; on U.S. Africa Command's characterisation of al-Shabaab as al-Qaeda's largest, wealthiest and most lethal affiliate, and on the group's origins in the Islamic Courts Union and the 2006 Ethiopian intervention, see: Congressional Research Service 2023: Al Shabaab, In Focus No. IF10170, 14 Feb 2023, in: https://www.congress.gov/crs-product/IF10170 [14 Sep 2026].

2 Institute for Economics and Peace 2026: Global Terrorism Index 2026, Sydney, Mar 2026, in: https://reliefweb.int/report/world/global-terrorism-index-2026 [21 Sep 2026].

3 Neumann, Peter R. 2026: The New Grey Zone: How Terrorism in Europe Has Changed, Perspectives on Terrorism XX: 1, pp. 109-113.

4 Composite background assessment on East and Central African extremist networks, drawing on Institute for Strategic Dialogue, Combating Terrorism Center at West Point, U.S. Department of State Country Reports on Terrorism and United Nations monitoring-group reporting (reference document compiled for this study), on clandestine, multilingual (Somali, Arabic, Swahili and English) networks operating through proxy pages and encrypted applications.

5 CBS News 2013: FBI: Al-Shabaab Released Video to Recruit Minn. Men for Jihad, 8 Aug 2013, in: https://www.cbsnews.com/minnesota/news/fbi-al-shabaab-released-violent-video-to-recruit-minn-men-for-jihad/ [14 Sep 2026]. The report indicates that more than two dozen Somali-Americans from the Twin Cities (Minneapolis and Saint Paul) were recruited by al-Shabaab.

6 Hassan, Abdirahim M. 2026: Israel's Recognition of Somaliland: A Dangerous Precedent in Fragile Horn of Africa, Politics Today, 1 Jan 2026, in: https://politicstoday.org/israels-recognition-of-somaliland-a-dangerous-precedent-in-fragile-horn-of-africa/ [14 Sep 2026].

7 Middle East Media Research Institute 2017: Jihad and Terrorism Threat Monitor Roundup: Jihadi Groups React to U.S. Recognition of Jerusalem as Capital of Israel, 8 Dec 2017; International Centre for Counter-Terrorism: Jihadists Respond to Trump: In al-Quds We Meet.

8 U.S. Department of State 2025: 2025 Investment Climate Statements: Somalia, Washington, D.C.; U.S. Department of Commerce: Somalia Country Commercial Guide: Banking and Financial Services, in: trade.gov; World Bank: Somali Remittance, Summary Report. On annual remittances of approximately 2 billion U.S.-dollars, equal to roughly 18 to 25 per cent of GDP.

9 Institute for Security Studies 2024: Kenya Is Once Again in FATF's Crosshairs, Mar 2024; Institute for Security Studies 2025: Risk and Reward of Kenya's Push to Reverse FATF Grey-Listing, 30 Sep 2025; Trigarc 2026: Kenya FATF Grey List: AML/CTF Compliance Implications.

10 Representative sources across the four tiers include: United Nations Panel of Experts on Somalia; U.S. Department of the Treasury; Financial Action Task Force, Kenya country monitoring page, in: fatf-gafi.org; Kenya Financial Reporting Centre 2025: Terrorism Financing National Risk Assessment Guidance, Feb 2025, in: frc.go.ke; Combating Terrorism Center at West Point; Institute for Strategic Dialogue; International Centre for Counter-Terrorism; Jamestown Foundation 2026: Houthis and al-Qaeda Growing Terror Supply Chain; and the Critical Threats Project.

11 Woodward, Peter 2003: The Horn of Africa: Politics and International Relations, London. On Soviet-U.S. Cold War competition in the Ogaden War (1977 to 1978).

12 Zimmermann, Doron/Rosenau, William (eds.) 2009: The Radicalization of Diasporas and Terrorism, Zürcher Beiträge zur Sicherheitspolitik No. 80, Zurich, pp. 9-10.

13 Gilroy, Georgia 2023: How al-Shabaab Is Using Social Media to Build a Bridge between Gaza and Somalia, GNET Insights, 31 Oct 2023, in: https://gnet-research.org/2023/10/31/how-al-shabaab-is-using-social-media-to-build-a-bridge-between-gaza-and-somalia/ [21 Sep 2026].

14 Zimmermann/Rosenau 2009, n. 12, pp. 9-13.

15 Ibid., p. 14, summarising Menkhaus, Ken: African Diasporas, Diasporas in Africa and Terrorist Threats.

16 Meleagrou-Hitchens, Alexander/Maher, Shiraz/Sheehan, James 2012: Lights, Camera, Jihad: Al-Shabaab's Western Media Strategy, International Centre for the Study of Radicalisation and Political Violence, London; World Bank 2020: Somalia Poverty and Vulnerability Assessment, Washington, D.C.

17 Office for National Statistics 2021: Census 2021 (United Kingdom); U.S. Census Bureau 2023: American Community Survey; Statistics Sweden 2024; Statistics Canada 2021: Census of Population 2021. Figures aggregated from national census data (2015 to 2024) and United Nations diaspora data.

18 World Bank 2020: Somalia Economic Update: Remittances, Washington, D.C.; The New Humanitarian 2025: The Diaspora Lifeline That Helps Keep Somali Families Afloat, 30 Sep 2025 (1.7 billion U.S.-dollars in 2023; approximately 40 per cent of households reliant); United Nations Development Programme 2001, as cited in World Bank 2006: Working Paper No. 38 (diaspora of more than one million, approximately one-sixth of the Somali population).

19 Combating Terrorism Center at West Point 2025: The Global State of al-Qa'ida 24 Years after 9/11 (100 to 200 million U.S.-dollars revenue); Africa Defense Forum 2023: Somalia Targets al-Shabaab's Revenue Streams, 18 Apr 2023 (70 per cent territorial control); Africa Center for Strategic Studies 2023: Reclaiming al-Shabaab's Revenue (2,553 incidents; 6,225 fatalities); International Organization for Migration 2022: Displacement Tracking Matrix: Somalia (3.8 million internally displaced persons, end-2022).

20 Bell, Stewart 2009: The Spillover Effect: The Canadian Diasporas and Terrorism, in: Zimmermann/Rosenau 2009, n. 12, pp. 41-56.

21 Meleagrou-Hitchens/Maher/Sheehan 2012, n. 16, pp. 43-47.

22 Ibid., pp. 31-33.

23 The Times 2025: The Jihadi Mastermind Who Fled MI5 to Bring ISIS Back from the Dead, 1 Dec 2025.

24 Tyson, Kathrin 2025: The Islamic State in Somalia's Area of Operations, Critical Threats, 11 Jun 2025, in: https://www.criticalthreats.org/analysis/the-islamic-state-in-somalias-area-of-operations [15 Sep 2026].

25 U.S. Department of Justice 2015: press release on the sentencing of Mustafa Kamel Mustafa (Abu Hamza al-Masri) to life imprisonment by the U.S. District Court for the Southern District of New York, 9 Jan 2015.

26 Meleagrou-Hitchens/Maher/Sheehan 2012, n. 16, pp. 10-12.

27 Hassan, Abdullahi Ali 2025: The Somali Diaspora Are Digital Remitters of Violence, Africa at LSE, London School of Economics, 23 Oct 2025, in: https://blogs.lse.ac.uk/africaatlse/2025/10/23/the-somali-diaspora-are-digital-remitters-of-violence/ [21 Sep 2026].

28 Ibid.

29 Ibid.

30 Somali Guardian 2026: Al-Shabaab Issues Sharp Rebuke over Somaliland's New Jerusalem Embassy, 17 Jun 2026.

31 Hoffman, Bruce/Rosenau, William/Curiel, Andrew J./Zimmermann, Doron 2007: The Radicalization of Diasporas and Terrorism: A Joint Conference by the RAND Corporation and the Center for Security Studies, ETH Zurich, RAND Conference Proceedings CF-229, Santa Monica, in: https://www.rand.org/pubs/conf_proceedings/CF229.html [21 Sep 2026].

32 GSDRC 2015: Radicalisation of Diaspora Communities, Helpdesk Research Report, University of Birmingham, in: https://gsdrc.org/publications/radicalisation-of-diaspora-communities/ [21 Sep 2026].

33 Al Raffie, Dina 2013: Social Identity Theory for Investigating Islamic Extremism in the Diaspora, Journal of Strategic Security 6: 4, pp. 67-91.

34 Congressional Research Service 2015: European Fighters in Syria and Iraq: Assessments, Responses, and Issues for the United States, Report R44003, Washington, D.C., in: https://www.everycrsreport.com/reports/R44003.html [21 Sep 2026].

35 Reuters 2019: Europeans Who Joined Islamic State, reproduced in: Kuwait Times, 20 Feb 2019, citing Europol data, in: https://www.pressreader.com/kuwait/kuwait-times/20190220/281771335466256 [21 Sep 2026].

36 Foreign Policy Research Institute 2020: The Enduring Legacy of French and Belgian Islamic State Foreign Fighters, 27 Feb 2020, in: https://www.fpri.org/article/2020/02/enduring-legacy-french-belgian-isis-foreign-fighters/ [21 Sep 2026].

37 The Irish Times 2019: Europe Confronts Problem of Returning ISIS Fighters, 21 Feb 2019, citing data of the German Federal Office for the Protection of the Constitution (BfV), in: https://www.irishtimes.com/news/world/europe/europe-confronts-problem-of-returning-isis-fighters-1.3799392 [21 Sep 2026].

38 Reuters 2019, n. 35.

39 Renard, Thomas/Coolsaet, Rik (eds.) 2018: Returnees: Who Are They, Why Are They (Not) Coming Back and How Should We Deal with Them?, Egmont Paper 101, Brussels, in: https://egmontinstitute.be/app/uploads/2018/02/egmont.papers.101_online_v1-3.pdf [21 Sep 2026]; see also Coolsaet, Rik 2016: Facing the Fourth Foreign Fighters Wave, Egmont Paper 81, Brussels.

40 European Institute of the Mediterranean: Radicalization in Europe, in: https://www.iemed.org/publication/radicalization-in-europe/ [21 Sep 2026].

41 Bisserbe, Noemie 2016: European Prisons Fueling Spread of Islamic Radicalism, The Wall Street Journal, 31 Jul 2016, in: https://www.wsj.com/articles/european-prisons-fueling-spread-of-islamic-radicalism-1470001491 [19 Sep 2026].

42 Mufson, Steven 2016: How Belgian Prisons Became a Breeding Ground for Islamic Extremism, The Washington Post, 27 Mar 2016, in: https://www.washingtonpost.com/world/europe/how-belgian-prisons-became-a-breeding-ground-for-islamic-extremism/2016/03/27/ac437fd8-f39b-11e5-a2a3-d4e9697917d1_story.html [19 Sep 2026].

43 NBC News 2025: Trump's Gaza Comments Hand Jihadist Terrorists a 'Rallying Cry', Experts Say, 7 Feb 2025.

44 Europol 2024: European Union Terrorism Situation and Trend Report (TE-SAT) 2024, The Hague, in: https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [21 Sep 2026].

45 Europol 2025: European Union Terrorism Situation and Trend Report (TE-SAT) 2025, The Hague, in: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat [21 Sep 2026].

46 The Conversation 2026: How Hatred of Jews Became a Common Ground for Islamic Terrorists and Left-Wing Extremists, Fuelling Domestic Terrorism, citing Anti-Defamation League data, in: https://theconversation.com/how-hatred-of-jews-became-a-common-ground-for-islamic-terrorists-and-left-wing-extremists-fueling-domestic-terrorism-278373 [21 Sep 2026]; Anti-Defamation League: The October 7th War: A Timeline of Key Events and Issues, in: https://www.adl.org/resources/backgrounder/october-7th-war-timeline-key-events-and-issues [21 Sep 2026].

47 Institute for National Security Studies 2024: The Strengthening of the Extreme Right in the West Following the October 7 Massacre, Tel Aviv, in: https://www.inss.org.il/publication/far-right-october-7/ [21 Sep 2026].

48 Vision of Humanity 2025: Gaza Conflict Leads to Rise in Antisemitism and Islamophobia, Institute for Economics and Peace, citing Council on American-Islamic Relations (CAIR) and European Islamophobia Report data, in: https://www.visionofhumanity.org/gaza-conflict-leads-to-rise-in-antisemitism-and-islamophobia/ [21 Sep 2026].

49 Istituto per gli Studi di Politica Internazionale 2024: On the Edge: The Ethiopia-Somaliland MoU, 30 Jan 2024.

50 FDD's Long War Journal 2024: Shabaab Says It Rejects Red Sea Access Deal between Ethiopia and Somaliland, 2 Jan 2024, in: https://www.longwarjournal.org/archives/2024/01/shabaab-says-it-rejects-red-sea-access-deal-between-ethiopia-and-somaliland.php [21 Sep 2026].

51 Critical Threats 2024: Salafi-Jihadi Movement Update Special Edition: Ethiopia-Somaliland Port Deal Strains Horn of Africa Counterterrorism Cooperation and Alters Red Sea Geopolitics, 4 Jan 2024, in: https://www.criticalthreats.org/analysis/salafi-jihadi-movement-update-special-edition-ethiopia-somaliland-port-deal-strains-horn-of-africa-counterterrorism-cooperation-and-alters-red-sea-geopolitics [21 Sep 2026].

52 Hassan 2026, n. 6.

53 Horton, Michael 2020: Somaliland Combats al-Shabaab, CTC Sentinel, Combating Terrorism Center at West Point, in: https://ctc.westpoint.edu/somaliland-combats-al-shabaab/ [21 Sep 2026].

54 Meleagrou-Hitchens/Maher/Sheehan 2012, n. 16, Executive Summary.

55 Ibid., pp. 23-27.

56 Felden, Esther/Müller, Mariel 2025: From Germany, 'War Influencers' Incite Violence in Somalia, Deutsche Welle, Jul 2025, in: https://www.dw.com/en/somalia-germany-war-influencers-violence-social-media-facebook-tiktok/a-73137140 [19 Sep 2026].

57 BBC News 2026: Man Went to Somalia in Attempt to Join ISIS, Aug 2026, in: https://www.bbc.com/news/articles/clyj90n30mjo [19 Sep 2026].

58 Neumann 2026, n. 3, pp. 111-119.

59 Ibid., pp. 113-114, on the lone-actor/organisational contrast; Combating Terrorism Center at West Point: Al-Hijra: Al-Shabab's Affiliate in Kenya, CTC Sentinel.

60 Neumann 2026, n. 3, p. 112, on sustained counter-terrorism pressure making physical organisational infrastructure harder to build and pushing mobilisation online.

61 Ayad, Moustafa/Harrasy, Anisa/Abdullah, Mohammed 2022: Under-Moderated, Unhinged and Ubiquitous: Al-Shabaab and the Islamic State Networks on Facebook, Institute for Strategic Dialogue, London, 14 Jun 2022, pp. 4-9, in: https://www.isdglobal.org/isd-publications/under-moderated-unhinged-and-ubiquitous-al-shabaab-and-the-islamic-state-networks-on-facebook/ [21 Sep 2026].

62 Ibid., pp. 7-9, 13-14.

63 Ibid., pp. 4-5, 9.

64 Ibid., p. 5, citing Iyengar, Rishi 2021: Facebook Has Language Blind Spots around the World That Allow Hate Speech to Flourish, CNN, 26 Oct 2021, in: https://edition.cnn.com/2021/10/26/tech/facebook-papers-language-hate-speech-international [21 Sep 2026].

65 Global Network on Extremism and Technology 2026: Propaganda as Financial Infrastructure: How Islamic State and al-Qaeda Media Ecosystems Enable Terrorist Finance, GNET Insights, 7 Apr 2026, in: https://gnet-research.org/2026/04/07/propaganda-as-financial-infrastructure-how-islamic-state-and-al-qaeda-media-ecosystems-enable-terrorist-finance/ [21 Sep 2026].

66 Manohar Parrikar Institute for Defence Studies and Analyses 2025: The Resilience and Internationalisation of ISIS Somalia, Issue Brief, New Delhi, in: https://idsa.in/publisher/issuebrief/the-resilience-and-internationalisation-of-isis-somalia [21 Sep 2026].

67 U.S. Department of the Treasury 2024: Fact Sheet: Countering ISIS Financing, 27 Feb 2024, in: https://home.treasury.gov/system/files/136/Fact-Sheet-Countering-ISIS-Financing-2-27-24.pdf [21 Sep 2026]; U.S. Department of the Treasury 2023: Treasury Designates Senior ISIS-Somalia Financier, 27 Jul 2023, in: https://home.treasury.gov/news/press-releases/jy1652 [21 Sep 2026].

68 Chainalysis 2025: The 2025 Geography of Cryptocurrency Report, Oct 2025, in: https://www.chainalysis.com/blog/subsaharan-africa-crypto-adoption-2025/ [15 Sep 2026]; CNBC Africa/Paybis Research 2026: Regional Crypto Market Growth, Jun 2026, in: https://financefeeds.com/cnbc-africa-crypto-trends-regional-market-growth/ [15 Sep 2026].

69 Chainalysis 2025, n. 68; BusinessDay 2025: Kenya, South Africa, Ghana Pull Ahead as Nigeria Risks Losing Crypto Leadership, in: https://businessday.ng/news/article/kenya-south-africa-ghana-pull-ahead-as-nigeria-risks-losing-crypto-leadership/ [15 Sep 2026].

70 Financial Action Task Force 2023: Jurisdictions under Increased Monitoring, Paris, Feb 2023; see also: ScienceDirect 2026, May 2026, in: https://www.sciencedirect.com/science/article/pii/S2212473X26000763 [15 Sep 2026], on weaknesses in virtual asset service provider supervision as a key listing factor.

71 Polity 2025: Virtual Assets Regulation in East and West Africa: A Regional Comparative Guide, 4 Nov 2025, in: https://www.polity.org.za/article/virtual-assets-regulation-in-east-and-west-africa-a-regional-comparative-guide-2025-11-04 [15 Sep 2026]; Priviet Social Sciences Journal 2026, Jul 2026, in: https://journal.privietlab.org/index.php/PSSJ/article/view/1990 [15 Sep 2026].

72 Ibid.

73 El-Qorchi, Mohammed/Maimbo, Samuel Munzele/Wilson, John F. 2003: Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, IMF Occasional Paper No. 222, Washington, D.C., in: https://www.imf.org/external/pubs/nft/op/222/index.htm [21 Sep 2026].

74 Ibid.

75 Financial Action Task Force 2013: The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing, Paris, in: https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf [21 Sep 2026].

76 Financial Action Task Force: Recommendation 10 (Customer Due Diligence), The FATF Recommendations, Paris; Financial Crimes Enforcement Network 2003: Informal Value Transfer Systems, FinCEN Advisory No. 33, Washington, D.C.

77 Financial Action Task Force 2013, n. 75; Financial Crimes Enforcement Network 2003, n. 76.

78 KYC Hub: Hawala Money: A Complete Guide to Hawala Money Laundering, in: https://www.kychub.com/blog/hawala-money-laundering [21 Sep 2026]; Financial Action Task Force 2013, n. 75.

79 World Bank: Somali Remittance, Summary Report, on remittances at approximately 18 to 20 per cent of GDP and channel breakdowns across hawala, mobile money and money transfer operators including Dahabshiil, Amal Express and Taaj; U.S. Department of State 2025, n. 8.

80 Federal Bureau of Investigation 2011: Two Minnesota Women Convicted of Providing Material Support to al-Shabaab, press release, Oct 2011.

81 News from the States 2025: Right-Wing Reporting on Somali Money Going to al-Shabaab Is Not New, Still Misses the Mark, 25 Nov 2025; see also reporting on the underlying Minnesota public-benefits fraud investigation: Fox News, 12 Dec 2025.

82 U.S. Department of the Treasury 2001: Designation of Al-Barakaat, Nov 2001; Grey Dynamics 2024: Hawala in Somalia: Link to Money Laundering and Terrorist Financing.

83 AllAfrica 2025: Somalia: Somali Court Sentences Woman to 16 Years for Financing al-Shabaab, 18 Sep 2025.

84 Financial Action Task Force 2013, n. 75.

85 Financial Action Task Force 2025: Comprehensive Update on Terrorist Financing Risks, Paris, Jul 2025, in: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf [21 Sep 2026].

86 United Nations Security Council Counter-Terrorism Committee Executive Directorate: Trends Tracker: Evolving Trends in the Financing of Foreign Terrorist Fighters Activity, 2014-2024, New York, in: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_trends_tracker_evolving_trends_in_the_financing_of_foreign_terrorist_fighters_activity_2014_-_2024.pdf [21 Sep 2026].

87 360 Mozambique 2025: GIFiM: $7 Million Detected in Terrorism Financing in Mozambique between 2017-24, Sep 2025, reporting on the Strategic Analysis Report of the Financial Intelligence Office of Mozambique (GIFiM) published on 5 Sep 2025, in: https://360mozambique.com/economy/finance/gifim-7-million-detected-in-terrorism-financing-in-mozambique-between-2017-24/ [21 Sep 2026].

88 United Nations Security Council 2025: Thirty-Sixth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities, New York, Jul 2025.

89 Nation 2021: Trail of Ruined Lives: Aboud Rogo's Disciples of Terror, summarising Chome, Ngala: Eastern Africa's Regional Extremist Threat: Origins, Nature and Policy Options, Centre for Human Rights and Policy Studies, in: https://nation.africa/kenya/news/trail-ruined-lives-aboud-rogo-disciples-terror-3211514 [21 Sep 2026]; Foreign Policy Research Institute 2021: The Evolution and Escalation of the Islamic State Threat to Mozambique, Apr 2021, in: https://www.fpri.org/article/2021/04/the-evolution-and-escalation-of-the-islamic-state-threat-to-mozambique/ [21 Sep 2026].

90 Ayad/Harrasy/Abdullah 2022, n. 61, pp. 8-10, 19.

91 Whine, Michael 2009: The Radicalization of Diasporas and Terrorism: United Kingdom, in: Zimmermann/Rosenau 2009, n. 12, pp. 17-39.

92 Bell 2009, n. 20, pp. 41-56.

93 Meleagrou-Hitchens/Maher/Sheehan 2012, n. 16, p. 10.

94 Compare Meleagrou-Hitchens/Maher/Sheehan 2012, n. 16 (Twitter-focused); Ayad/Harrasy/Abdullah 2022, n. 61 (Facebook-focused); and Gilroy 2023, n. 13 (cross-platform: TikTok, Telegram and X).

95 Africa Center for Strategic Studies 2025: Combating Illicit Trafficking and Terrorist Financing in Eastern Africa, CTCVE-CTOC Workshop Guide, Jul 2025; U.S. Department of State, Rewards for Justice 2026: Al-Shabaab's Financial Network, programme profile. On the persistent evidentiary gap between designation-level financial intelligence and jurisdiction-specific diaspora fundraising pathways.

96 Virtual Key Informant Interview with a terrorism expert based in South Africa, 15 Aug 2026

97 BBC News 2026, n. 57.

98 Virtual key informant interview with a respondent based in Jerusalem, Israel, 24 Aug 2026.

99 Ibid.

100 Virtual key informant interview with a P/CVE practitioner in Singapore, 18 Jul 2026.

101 Gilroy 2023, n. 13.

102 Istituto per gli Studi di Politica Internazionale 2024, n. 49; ACLED 2024: Ethiopia's Quest for Sea Access, Jan 2024; Hassan 2026, n. 6.

103 Somali Guardian 2026, n. 30.

104 Except from a video on X, https://x.com/SuleimanElite/status/2011425371418218954 [19 Sept 2026].

105 Ibid

106 Ibid

107 Ibid

108 Ibid

109 Excerpt from a video on TikTok, https:// https://vt.tiktok.com/ZSb92RqKt/ [19 Sept 2026].

110 Ibid

111 Ibid

112 Ibid

113 Ibid

114 Ibid

115 Ibid

116 Ibid

117 Ibid

118 Excerpt from a video on X, https://x.com/chabisbuuxis/status/1644271920093835269, [19 Sept 2026].

119 Ibid

120 Ibid

121 Ibid

122 Ibid

123 Virtual key informant interview, Jerusalem, n. 97.

124 Virtual key informant interview with an an Eastern and Southern Africa Anti-Money Laundering Group official official based in Arusha, Tanzania, 24 Aug 2026.

125 Excerpt from a video on X, https://x.com/chabisbuuxis/status/1637797457084989446, [19 Sept 2026].

126 Ibid

127 Ibid

128 Excerpt from a video on X, https://x.com/chabisbuuxis/status/1644271977530630145, [19 Sept 2026].

129 Ibid

130 Ibid

131 Ibid

132 Virtual key informant interview with a terrorist financing specialist based in the U.S., 28 Aug 2026.

133 Physical key informant interview with an AML/CTF expert in Nairobi, Kenya, 26 Aug 2026.

134 Virtual key informant interview with an Eastern and Southern Africa Anti-Money Laundering Group official based in Tanzania, 24 Aug 2026.

135 Physical key informant interview with a terrorism and counter-terrorism expert in Nairobi, Kenya, 17 Aug 2026.

136 Virtual key informant interview, Eastern and Southern Africa Anti-Money Laundering Group official, n. 124.

137 Ibid.

138 Virtual key informant interview with a social media analyst based in the UK, 15 Aug 2026.

139 Virtual key informant interview with a P/CVE expert based in the U.S., 29 Aug 2026.

140 Virtual key informant interview, P/CVE practitioner, Singapore, n. 100.

The Authors

HORN International Institute for Strategic Studies

Imprint

Konrad-Adenauer-Stiftung e. V.

Jan-Ole Voß
Director of the Regional Programme Security Dialogue for East Africa
jan-ole.voss@kas.de
kas.de
Publisher: Konrad-Adenauer-Stiftung e. V., 2026, Berlin

This publication of the Konrad-Adenauer-Stiftung e. V. is solely intended for information purpose. It may not be used by political parties or by election campaigners or supporters for the purpose of election advertising. This applies to federal, state and local elections as well as to elections to the European Parliament.



The text of this publication is licensed under the Creative Commons license: "Creative Commons Attribution-ShareAlike 4.0 International", CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0/legalcode.de)

KONRAD ADENAUER STIFTUNG

Konrad Adenauer Stiftung

REGIONAL PROGRAMME
SECURITY DIALOGUE FOR EAST AFRICA

24, Kololo Hill Lane, Kololo
P.O. Box 647, Kampala, Uganda

Email: sipodi.east@kas.de
www.kas.de/en/web/sipodi-east