JOURNAL OF POLICING, INTELLIGENCE AND COUNTER TERRORISM
2026, VOL. 21, NO. 1, 52–69
https://doi.org/10.1080/18335330.2025.2486659

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

The regulation of terrorist online content in Africa: an overview of the applicable regional instruments and the legal frameworks of South Africa, Kenya and Nigeria

Brenda Mwale

Post Doctoral Research Fellow, Faculty of Law, University of Pretoria, Pretoria, South Africa

ABSTRACT

The rapid advancement in technology has made society increasingly dependent on information and communication technology (ICT). Unfortunately, this dependence has also created new opportunities for terrorist groups to use the Internet for their activities. Over the years, there has been a significant rise in terrorist online activity, with these groups using the Internet for various purposes, including the dissemination of terrorist content. This is particularly concerning for African countries, where Internet use by terrorist groups and dissemination of terrorist content is increasing. However, the complexity of regulatory measures within the continent due to diverse legal frameworks, as well as capacity and implementation challenges, complicate efforts to address this issue. In this context, this article explores how existing regional instruments and national laws address terrorist online content. It proposes a unified and multifaceted approach to improve the regulatory measures in Africa.

ARTICLE HISTORY
Received 16 July 2024
Accepted 26 March 2025

KEYWORDS
Content moderation; online platforms; prohibited speech; terrorism; terrorist online content

Introduction

The advent of information and communication technology (ICT) presents both opportunities and risks for Africa. While ICT promotes social, political, and economic development, it also creates new risks. Increasingly, online platforms, such as social media platforms, are used to disseminate terrorist content for recruitment, propaganda, and coordinating activities. Indeed, Tech Against Terrorism, a leading organisation in disrupting terrorist activity online, claims that al-Shabaab, a violent extremist group based in Somalia, is 'essentially the largest single producer of terrorist material on the Internet', responsible for around 20–25% of the terrorist content they find (Tech Against Terrorism, 2024).

The African Union (AU) Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace (2024) reaffirms that African states shall ensure that ICT is not misused for, among other purposes, inciting violence, terrorism and violent extremism. This duty may require states

CONTACT Brenda Mwale mwale17@gmail.com

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

to take necessary actions, including adopting legal and practical measures to counter the use of ICT for terrorist purposes, including the dissemination of online terrorist content. Although some states have introduced regulations to address the problem, efforts are complicated by diverse regional, subregional and national laws and a lack of clear legal provisions at these levels. Furthermore, online platforms responsible for taking down such content rely on their terms of service and community standards to determine which content is classified as terrorist, frequently without clear regulatory guidance on how to apply such classifications.

A key challenge is that the lack of clarity on what constitutes 'terrorist online content' and what measures should be taken by relevant stakeholders can result in the improper classification of online content. Potentially, non-terrorist content may be flagged as terrorist, and legitimate expressions could be criminalised by states, raising human rights concerns. Indeed, the African Declaration on Internet Rights and Freedoms (2014) highlights that:

> Although there is a legitimate desire by governments to curb criminal activities online, particularly … terrorist activities, there are also clear instances where the pursuit of these apparently legitimate objectives has been used as a pretext to introduce provisions to curtail criticism of governments. (The African Declaration, p. 4)

This article provides an overview of terrorist online content regulation in Africa, describing the problem of terrorist online content in the region and highlighting key regulatory measures and laws. It focuses on key regional instruments, including the Organization of African Unity (OAU) Convention on the Prevention and Combating of Terrorism and the African Union Declaration of Principles of Freedom and Access of Information in Africa which address terrorism and online speech respectively. It also focuses on subregional cybercrime instruments developed by the East African Community (EAC), Economic Community of West African States (ECOWAS) and the Southern African Development Community (SADC), as well as the national laws in South Africa, Kenya, and Nigeria —which are parties to the OAU Convention on Terrorism and members of these subregional bodies.

Each of these three countries has a unique context in terms of levels of Internet access, experiences with terrorism and approaches to countering terrorist online content. In all three countries, Internet access is rapidly increasing, and there is a strong social media presence. However, Kenya and Nigeria have a history of terrorist threats and attacks, while South Africa has not faced significant terrorism challenges. Additionally, South Africa provides a unique case study due to its attempts to explicitly prohibit terrorist online content within its counter-terrorism law. By selecting various regional and subregional instruments, as well as the above three countries, this article conducts a comparative analysis to understand how terrorist online content is addressed through legal instruments at different levels and in different locations in Africa. It does so by exploring how these instruments address terrorist online content, highlighting their implications and limitations. It also analyses the policies of online platforms regarding terrorist online content and proposes practical steps for ensuring regulatory frameworks in Africa are more robust.

Defining terrorist online content

Before exploring the existing legal frameworks, it is essential to understand what 'terrorist online content' entails, as there is no universally accepted definition of the term. In

contrast to other regions like Europe, where definitions of terrorist online content are explicitly stated in some instruments, many African countries tend to lack this level of specificity and do not define the term. Thus, to explore what 'terrorist online content' entails, this section will focus on the explicit and oft-quoted definition provided by the European Union (EU) regulation on addressing the dissemination of terrorist content online (European Union, 2021). The regulation defines 'terrorist content' as content which:

a. Incites the commission of a terrorist offence;
b. Solicits a person or a group of persons to commit or contribute to the commission of a terrorist offence;
c. Provides instruction on how to carry out terrorist acts;
d. Constitutes a threat to commit a terrorist offence (European Union, 2021, Article 2(7)).

Material disseminated for 'educational, journalistic, artistic or research purposes or for awareness-raising purposes against terrorist activity' does not qualify as terrorist online content (European Union, 2021, Preamble). This exemption establishes safeguards for lawful activities that may contain content linked to terrorism.

While the above definition highlights the general characteristics of terrorist online content, there are concerns regarding the broad definition of the term. Primarily, it covers not only content that incites or solicits the commission of a terrorist offence but also content that provides instructions to commit such an offence or constitutes a threat to commit an offence (Rojszczak, 2023, pp. 191–193) with no intent requirement (Bellaert, Selimi, & Gouwy, 2021, p. 165). Thus, it is argued that the broad definition could potentially open doors to violations of the right to free speech and abuse by authoritarian regimes (Bellaert et al., pp.164, 179).

Some commentators have opted not to explicitly define the term 'terrorist online content' but rather categorise such content. For instance, Davey, Comerford, Guhl, Baldet, and Colliver (2021, p. 7) developed a framework for classifying terrorist content into three broad categories:

1. Instructional material which contains guidance on operational aspects of terrorist activity.
2. Ideological material which is designed to further terrorist worldview by explaining why the world is a certain way.
3. Inspirational material designed to reinforce a terrorist mindset, such as material intended to provoke hate towards a particular group of people.

From the above, it could be argued that the metrics to consider in defining terrorist online content include the type and purpose of the content. Thus, this article defines terrorist online content as any material uploaded, shared, or distributed online by an individual or group to (a) depict terrorist acts and how to conduct such acts, (b) share the ideologies of a terrorist group, or (c) incite, support or solicit a person to commit a terrorist act. Material for 'educational, journalistic, artistic or research purposes' is exempt from this definition.

Terrorist online content in Africa

Building on this definition, this discussion now focuses on Africa, where terrorist groups such as al-Shabaab, Boko Haram, the Islamic State of Iraq and the Levant (ISIL) affiliated groups, and other violent extremist groups are increasingly using social media for various purposes. First, they use social media to disseminate propaganda. Research published by the Institute of Strategic Dialogue in 2022 revealed that within a period of two years, there were numerous posts on Meta (formerly Facebook) containing propaganda linked to al-Shabaab and Islamic State (Ayad, Harrasy, & Abdullah, 2022, pp. 6–7, 16). Beyond such 'mainstream' platforms, research also shows an increased use of anonymous online platforms to share propaganda. For example, al-Shabaab uses the anonymous platform JustPaste.it to spread their propaganda videos (Weimann & Vellante, 2021, p. 45).

Second, terrorist groups use social media to inspire and recruit followers. Groups like al-Shabaab have employed this tactic since the early 2000s, producing videos aimed at recruiting 'youth, the Somali diaspora and Western foreign fighters' (Cox et al., 2018, p. 12). These videos were shared across various online news media networks (Cox et al., 2018, p. 12, 16). Third, these groups turn to social media to broadcast messages asserting their power and aiming to intimidate law enforcement authorities. For instance, it is alleged that Boko Haram's messages are targeted towards members of the Nigerian armed forces to 'convince them of the futility of fighting against a superior force' (Ogbondah & Agbese, 2018, p. 329). Fourth, terrorist groups use social media to solicit funds from their target audiences. The International Crisis Group (2018, pp. 5–6) highlights that some of the videos posted by al-Shabaab often conclude with requests for funding. Last, as part of their messaging strategy, groups, such as Boko Haram, display ongoing attacks or claim responsibility for attacks on online platforms (Mahmood, 2017, p. 3, 8).

As technology continues to evolve, terrorist groups are beginning to use generative artificial intelligence to create and publish material (Nelu, 2024). The advancement in tactics highlights the ability of these terrorist groups to adopt new technologies to effectively disseminate their messages. Beyond that, content posted online can remain available for years (Ayad et al., 2022, p. 9). Researchers found, for example, that in October 2021, a Somali-language 'media outlet' shared videos carrying al-Shabaab 'branding' (Ayad et al., 2022, p. 4). The videos remained on the platform for several months, attracting 53,300 views and 17,800 shares. Allowing such content to remain online for long periods enables wider spread of the material.

These challenges are compounded by practical content moderation hurdles somewhat particular to the continent. First, it is alleged that terrorist groups are leveraging language moderation gaps to bypass content moderation. For instance, Ansaru, a jihadist group in Nigeria, posts content in Hausa (Dahiru, 2023). It is also alleged that supporters of groups such as al-Shabaab and Islamic State are capitalising on ineffective moderation in East African languages to build stronger networks (Ayad et al., 2022, p. 5). According to the Institute for Strategic Dialogue:

> … the most active, networked, and multilingual ecosystem of support for al-Shabaab and the Islamic State existed on Facebook, where profiles and pages classified as 'media outlets' were sharing terrorist content openly, and eschewing private groups and profiles. The content … is often linked to 'media' and 'media personality' pages in Somali, Kiswahili and Arabic, and … points to language moderation blind spots … (Ayad et al., 2022, p. 4).

Terrorist content proliferates because social media companies are 'short of moderators who speak local languages and understand cultural context' (Debre & Akram, 2021).

Second, terrorist groups are increasingly moving to use smaller or encrypted platforms to bypass content moderation measures (Allen, 2022) and propagate their agendas 'largely unchecked'(Romaniuk, Fabe, & Nandy, 2023). While it might be easy to delete an account or content associated with a terrorist or terrorist organisation on a larger platform, a terrorist group can simply move to smaller, less regulated platforms. For instance, in 2019, after instant messaging service Telegram Messenger (Telegram) cracked down on several jihadist channels, al-Qaeda engineered a new Rocket.Chat server, a decentralised social media platform where developers cannot act on content stored on 'user-operated servers' or spread across 'the user community' (Aina & Ojo, 2023, pp. 15–16; King, 2019, p. 4). It is also alleged that al-Qaeda in the Islamic Maghreb (AQIM) uses 'beacon' websites to drive Internet traffic to smaller sites and 'aggregators' to provide users with a collection of links that go to the same terrorist content (Allen, 2022).

In African countries such as Kenya and Nigeria that experience domestic terrorism and have high Internet access and social media use, the likelihood of terrorist content spreading online is high. In countries such as South Africa that have high online engagement but little direct experience of terrorism, the risks are more moderate. On the other hand, countries with less digital presence and minimal experience with terrorism face a low risk. However, as Internet access increases across the continent, the presence and accessibility of such content will likely increase. This highlights the need to examine terrorist online content regulation in Africa while remaining alert to the ways in which borders both shape online legislation and are made porous by the online world. This is most usefully approached by differentiating between regional, subregional and national levels of response.

The legal response

Regional level

The fact that terrorist content online often transcends national borders underscores the importance of regulating such content at a regional level in Africa. Despite the growing recognition of this issue, the African Union (AU) has yet to establish specific instruments or guidelines to address terrorist online content. In the absence of such tailored regulation, it is important to explore how existing regional instruments, foremost of which are the Convention on countering terrorism and the Declaration relating to freedom of speech and information, address such content. These instruments address two specific aspects of terrorist online content: terrorism and prohibited online speech.

OAU Convention on the Prevention and Combating of Terrorism

The OAU Convention on the Prevention and Combating of Terrorism, adopted in 1999 (Organization of African Unity, 1999), is the primary Convention that addresses terrorism in Africa. It reaffirms the determination of AU member states to 'eliminate terrorism in all its forms and manifestations' [preamble] and requires states to criminalise terrorist acts, as defined in the Convention, in their domestic laws. However, predating online proliferation, the Convention does not expressly address terrorist activities committed online,

so it lacks specific provisions on such content or measures to address it. Nonetheless, the Convention's relevance for regulating terrorist online content should not be overlooked. Although its primary focus is on physical acts of terrorism, two provisions of the Convention can address terrorist online content.

First, Article 3 (b) of the Convention prohibits the 'promotion, sponsoring, contribution to, aid, incitement, encouragement, attempt, threat, conspiracy, organizing or procurement of any person' to commit a terrorist act. All these activities can be conducted through the Internet, and any related content posted on digital platforms would be prohibited. Second, Article 5(1) (b) of the Convention requires states to cooperate and strengthen the exchange of information among them regarding 'the communication and propaganda methods and techniques used by the terrorist groups […].' Online distribution of propaganda clearly falls under this provision, allowing states to cooperate and exchange information about new propaganda techniques. However, the challenges of regional cooperation in counter-terrorism efforts in Africa, such as lack of adequate funding and political cooperation, may undermine such efforts.,

AU Declaration of Principles of Freedom of Expression and Access to Information in Africa

As terrorist content falls under a broad category of illegal online content, it is important to examine how an instrument that guides states in the regulation of illegal online content addresses terrorist online content. In 2019, the African Commission on Human and Peoples' Rights (2019) adopted the Declaration of Principles of Freedom of Expression and Access to Information in Africa, a soft law document that anchors the right to freedom of expression and access to information in conformity with Article 9 of the African Charter on Human and Peoples Rights (Organization of African Unity, 1981).

The Declaration contains principles that may apply to the issue of terrorist online content and its moderation. First, Principle 23 focuses on prohibited speech, noting that 'States shall prohibit any speech that advocates for national, racial, religious or other forms of discriminatory hatred which constitutes incitement to discrimination, hostility or violence.' It is well known that terrorist organisations use discriminatory speech based on national, racial, religious, or other forms of discriminatory hatred to incite hostility or violence. For example, the Institute of Strategic Dialogue found that the largest narratives in 5,509 posts by al-Shabaab and the Islamic State spanning two years were 'a call for violence' and 'the promotion of violent jihad' (Ayad, Harrasy & Abdullah, 2022, p.16).' Clearly, such content is prohibited under this principle.

Second, in terms of content moderation, Principle 38 of the Declaration provides that states shall not interfere with individuals' rights to seek, receive, and share information through any communication means, including digital technologies, unless such interference is justified under international human rights law. This Principle is in line with Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which provides that freedom of expression may be subject to certain restrictions such as the protection of 'public order' (United Nations General Assembly, 1996, Article 19). Where terrorist content that incites discrimination, hostility, or violence threatens 'public order', it is justifiable to implement restrictions.

Third, Principle 39 of the Declaration outlines the obligations of Internet intermediaries regarding content moderation. It provides that states should not require Internet

intermediaries to monitor content that they have not created or otherwise modified. This Principle aims to protect the free speech of users of online platforms while also protecting them from monitoring. The principle also allows law enforcement agencies to request the expedited or immediate removal of content deemed to pose an imminent danger or risk of serious harm to individuals. Such requests, however, shall be subject to judicial review.

Based on these three principles, terrorist online content appears to fall under the scope of the Declaration when it amounts to content that incites violence, hostility, or discrimination. While the Declaration is not legally binding on AU member states, its interpretations carry significant weight as they were adopted by the African Commission on Human and Peoples' Rights, an authoritative treaty body. For the Declaration to be effective at the national level, AU member states must integrate these principles into their domestic laws.

Subregional level

In addition to the regional level, subregional initiatives can play an important role in addressing terrorist online content, although no subregional group specifically addresses the issue through a dedicated legal instrument. While regional economic communities have developed various instruments on cyber security and cybercrime, which generally respond to various cyber threats, some provisions relate to the use of ICT for terrorist purposes, including cyber terrorism.

First, the Economic Community of West African States (2011) Directive C/DIR. 1/08/11 on fighting cybercrime within ECOWAS explicitly addresses the use of ICTs to commit terrorism. Indeed, it states that this 'shall constitute a higher degree of offence' (Article 24). Second, the East African Community (2008) Draft EAC Legal Framework for Cyberlaws notes that measures 'designed to tackle cyber-terrorist … conduct are based around the motivation of the offender rather than his conduct' which generally fall under the four main substantive offences outlined in the framework. It is important to note, however, that regulating terrorist online content requires special measures which may differ from strategies employed to address other forms of cyber crimes. Third, while the Southern African Development Community (2012) Model Law on Computer Crime and Cybercrime does not contain any provisions on the use of ICT for terrorist purposes, the establishment of the SADC Counter Terrorism Centre in 2022 allows these issues to be addressed as a regional concern. Regional bodies such as ECOWAS, the EAC and the SADC, then, have existing regulatory frameworks that appear to apply to online terrorist content and offer mechanisms through which more focused measures can be developed and coordinated.

National level case studies: South Africa, Kenya and Nigeria

At the national level, countries have individual approaches to regulating terrorist online content in their domestic counter-terrorism laws. This is also true of the case study countries, South Africa, Kenya and Nigeria, whose relevant legal provisions do not mirror those at the regional and subregional levels. For instance, South Africa, which is party to the OAU Convention on Terrorism and a member of SADC, has legal provisions that allow for orders against online platforms to take down or restrict access to such

content. Kenya, also party to the OAU Convention on Terrorism and a member of EAC, has provisions in its counter-terrorism law that focus on information that is published, distributed, or made available to incite a person to commit a terrorist act. In contrast, Nigeria, which is both party to the OAU Convention on Terrorism and a member of ECOWAS, adopts a more stringent approach, explicitly prohibiting the dissemination of terrorist information through the Internet and other digital means. These countries highlight varying approaches at the regional, subregional and national levels, demonstrating efforts to directly address the dissemination of terrorist publications, both offline and online, at the national level, as detailed below.

South Africa

The legal provisions on terrorist online content in South Africa are outlined in the Protection of Constitutional Democracy against Terrorist and Related Activities Amendment (2022). The Amendment Act aims to create offences relating to the possession and distribution of publications that contain unlawful terrorism related content and provide for the removal of such publications or restriction of their accessibility, (Preamble). While it seeks to create such offences, it does not define what 'unlawful terrorism related content' amounts to. However, before its enactment, Section 3A(1) of the Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Bill [B 15—2022] defined the term as content which directly or indirectly encourages or assists in committing a terrorist act. It included statements, articles or records that, at the time of publication, were (i) intended or perceived as an inducement to commit a terrorist act, (ii) reckless as to whether they were perceived as an inducement, or (iii) contained information that could be useful in committing an offense.

A person committed an offence related to unlawful terrorism content by: (a) publishing, distributing or circulating the content; (b) selling or lending it; (c) offering it for sale or loan; (d) providing services to access it; (e) electronically transmitting it; or (f) possessing it for any of these purposes. This included content published on the Internet and social media (section 3A(4)). From the above provision, it is clear that the purpose for which the content was posted – to induce someone to commit a terrorist act – was a key factor in determining whether the content was terrorist in nature: there was no requirement for a terrorist act to occur. Nonetheless, persons charged with the offence could raise a defence that they did not know that the publication was for the purpose of engaging in terrorist activity or that their actions or possession of the material in question was for journalistic or academic research purposes. (sections 3A(4)−3A(5)).

While South Africa has made a good attempt to define unlawful terrorism related content, the relevant provisions have significant limitations. First, the definition of terrorist content was overly broad and, as a result, would violate the principle of legality, violate the right to freedom of expression, and open doors to arbitrary abuse (Parliamentary Monitoring Group, 2022a). Second, from a practical standpoint, critics argued that the inclusion of the provision was unlikely to resolve underlying issues such as capacity and training of law enforcement as well as resource shortages. (Parliamentary Monitoring Group, 2022b). These underlying issues require comprehensive strategies instead of merely introducing legal provisions without establishing a solid framework for effective implementation.

Nonetheless, while not retaining section 3A, the Amendment Act establishes provisions for the issuance of orders against electronic communication service providers whose platforms 'host a terrorism publication' (Terrorist and Related Activities Amendment Act 2022, section 24(A)). Specifically, these orders require service providers to take down or disable access to such publications. To provide clarity on this provision, the Amendment Act lays down definitions of three key terms. First, 'terrorism publication' encompasses an electronic communication, such as speech, text, or video, that threatens the public or segment of the public with terrorist activity or incites others to commit the offences (Terrorist and Related Activities Amendment Act, section 24A(13)(c)). Second, the phrase 'host a terrorism publication' means to store a terrorism publication on an electronic communication network where it can be 'viewed, listened to, copied or downloaded' or provide a link to such publication (sections 24A(13)(a)-(c)). Third, the term 'take down' refers to deleting or removing a terrorism publication stored on an electronic communications network' (sections 24A(13)(a)-(c)).

These definitions aim to create a basis from which service providers can tackle terrorist publications on their platforms. However, a notable shortcoming of the Amendment Act is the lack of clarity on the duties and obligations of key stakeholders involved in enforcement and regulation, which may undermine collaboration in regulating terrorist online content. Moreover, implementing and enforcing these provisions may be challenging for several reasons, including limited institutional capacity and budget constraints. For instance, the socio-economic impact assessment of the Amendment Bill indicated that, to cut down costs, a monitoring mechanism for overseeing the implementation of the provisions on unlawful terrorist related content would not be considered (Department of Planning, Monitoring and Evaluation, Republic of South Africa, 2021).

Kenya

In Kenya, the Prevention of Terrorism Act (2012), amended in 2023, is the primary legislation for detecting, preventing, and criminalising terrorist activities. While the Act does not prohibit terrorist online content *per se*, it contains three key applicable provisions. First, section 27 of the Act provides that '[a] person who publishes, distributes or otherwise avails information intending to directly or indirectly incite another person or a group of persons to carry out a terrorist act commits an offence'. There are two important considerations. To begin with, the provision does not specify a particular mode of publication, distribution, or availing of such information, which suggests that it can encompass a wide range of formats, including offline and online publications. Following on, it is important to determine whether there is an *intent* to directly or indirectly incite another person to carry out a terrorist act. This can be determined from the content and context of the publication.

Second, and relatedly, section 30A of the Act prohibits the publication or uttering of a statement that directly or indirectly encourages or induces another person to commit or prepare to commit an act of terrorism. Under the Section, a statement is likely to be interpreted as in breach of this law if: (1) it is reasonable to assume that the publication was so intended given the circumstances and manner of the publication or (2) the intention is clear from the contents of the statement. Statements uttered on online platforms can fall under this prohibition. Like section 27 above, statements uttered must be made with the intent to directly or indirectly incite another person to carry out a terrorist act. Writing on the

relationship and categorisation of such language, Stuart Macdonald argues that it would be 'practically worthless' to only focus on direct and explicit speech, such as 'I encourage you to … ', because 'indirect forms of encouragement are often more persuasive' (Macdonald, 2019, p. 5). Therefore, including both direct and indirect incitement recognises the various motivations behind the publications and speech prohibited under section 30A.

Third, the Act imposes obligations to communication service providers to intercept and retain specified communication when ordered to do so by a court. Under the Act, a police officer of or above the rank of chief inspector of police may make an ex parte application for an interception of communication order to obtain evidence of the commission of an offence (Prevention of Terrorism Act, 2012, section 36). The court may then order the communications provider to intercept and provide details of specified communication (section 36(3)(a)). The communication may relate to publications or statements envisaged under sections 27 and 30A of the Act, which relate to terrorist online content. Importantly, however, the court orders primarily focus on the interception and retention of specific information rather than the removal of content, as in the case of South Africa. While such orders are critical for preventing, detecting, investigating and prosecuting terrorist offences, their effectiveness in preventing the accessibility of terrorist online content on online platforms is limited.

This limitation highlights a broader challenge regarding the lack of precise definitions of terrorist online content and its implications for law enforcement authorities. Already, the enforcement of counter-terrorism laws in Kenya is constrained by uneven coordination between the national bodies involved in counter-terrorism, such as the National Police Service and the National Intelligence Service. In addition, 'resource constraints, insufficient training, and unclear command and control continue to hinder [counter-terrorism] effectiveness' (US Department of State, 2022). The specific measures required to regulate terrorist online content might further constrain counter-terrorism efforts in this area. However, in its statement on 'Measures to Eliminate International Terrorism' before the Sixth Committee of the 78th Session of the UN General Assembly in October 2023, Kenya emphasised the need to 'cooperate in capacity building and use of technology in knowledge management, detection and response in countering the … advancing and mutating terrorist and violent extremist strategies including through youth-targeted social media recruitment' (Kiboino, 2023, para. 11). This indicates at least an awareness at the level of national government of the need to combat emerging threats, as part of its efforts to combat terrorism effectively.

Nigeria

In 2022, Nigeria passed the Terrorism (Prevention and Prohibition) Act (2022), which provides a comprehensive legal framework for preventing and criminalising terrorist activities. The Act does not expressly prohibit terrorist online content, but section 13 prohibits soliciting and giving support to terrorist groups for the commission of acts of terrorism. The section defines support in various ways, including 'incitement to commit an act of terrorism by the dissemination of terrorist information through the Internet, other electronic or digital means, or through the use of printed materials.' Unlike Kenya, the prohibition does not focus on direct or indirect incitement; it simply provides that inciting another to commit an act of terrorism is prohibited. Besides, the provision does not require proof that the terrorist information was used in the commission of an act of terrorism.

Completing these provisions, a relevant agency, such as law enforcement, intelligence or security agency, can make an ex parte application to the court for an 'interception of communication order' to enhance the detection of offences related to the preparation of an act of terrorism (Terrorism (Prevention and Prohibition) Act, sec. 68). However, unlike South African counter-terrorism law providing for take-down orders, these orders are limited to intercepting communication transmitted over networks and are ineffective in content moderation Nonetheless, in June 2022, the National Information Technology Development Agency, a government agency tasked with implementing national information technology policy, published a Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries ('Code of Practice') setting out detailed obligations for online platforms. Specifically, the Code requires all online platforms to inform users in their terms of service not to 'create, publish, promote, modify, transmit, store or share any content or information that … promotes an act of terrorism' (National Information Technology Development Agency, 2022, part II, section 2).

The Code provides that platforms should not make such content accessible when they are informed of the presence of such materials. Once a platform is notified, it is required to remove the content within 24 hours (National Information Technology Development Agency, 2022, part IV). This requirement aims to reduce the availability, distribution, and proliferation of terrorist content as quickly as possible. While larger online platforms might be able to implement this 24-hour take-down policy, smaller online platforms might find it challenging due to limited manpower and resources. Despite these hurdles, the 24-hour removal requirement is a proactive measure to ensure online safety. In an October 2023 statement to the UN General Assembly on 'Measures to Eliminate International Terrorism,' Dakwak (2023) highlighted Nigerias commitment to 'combat the misuse of the cyberspace and new technologies by terrorists' (para. 11). This suggests that, as part of its efforts, Nigeria will likely review and enhance its efforts to specifically address terrorist use of ICT, possibly including terrorist online content. The true test lies in its implementation, however, and challenges in capacity and resources may constrain the efforts.

Regulation by online platforms

At a practical level, the regulation of terrorist online content relies heavily on online platforms like Meta (formerly Facebook) and X (formerly Twitter), where such content is posted. Generally, these online platforms have developed content moderation policies, processes, and tools to identify and remove terrorist content from their platforms. The problem is that online platforms use their terms of service and community standards to determine which content is allowed or prohibited on their platforms. These terms of service and community standards may not align with the definitions of terrorism, terrorist publications, and terrorist online content described above. For instance, Meta's community standards on 'dangerous organisations and individuals' prohibit terrorist content as follows:

> … we do not allow content that glorifies, supports or represents events that Meta designates as violating violent events – including terrorist attacks … Nor do we allow (1) Glorification, Support or Representation of the perpetrator(s) of such attacks; (2) perpetrator-generated content relating to such attacks; or (3) third-party imagery depicting the moment of such attacks on visible victims (Meta, n.d.).

In addition, individuals or organisations involved in terrorism are not allowed to have a presence on Meta's platform, and neither are symbols that represent them or content that glorifies them or their acts, including references to them (Meta). These clauses omit a critical aspect of defining terrorist related content or publications in South Africa, Kenya, and Nigeria's counter-terrorism laws: incitement to commit a terrorist act.

To take another example, X (n.d.-a) prohibits its users from threatening 'terrorism and/or violent extremism' or promoting 'violent entities' such as terrorist organisations in its 'violent and hateful entities policy, rules and policies'. The types of content that violate this policy include engaging in or promoting violent acts and recruiting, providing or distributing services, such as media or propaganda, to further stated goals on behalf of, indirectly or directly, a violent entity. In addition, under its rules, content 'containing manifestos and other content created by perpetrators [of violent attacks] or their accomplices' will be removed (X, n.d.-b). However, content for educational, documentary, or journalistic purposes is not in violation of this rule.

Both Meta and X do not define 'terrorist content', but list and describe the type of content that is prohibited on their platforms. A key concern in this regard is the lack of definitional clarity and transparency on how content removal is implemented across different platforms. In 2018, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlighted that '[c]ompany prohibitions of threatening or promoting terrorism, supporting or praising leaders of dangerous organisations and content that promotes terrorist acts or incites violence are, like counter-terrorism legislation, excessively vague' (United Nations General Assembly, 2018, April 6, p. 10).

In contrast, online platforms argue that the fragmented online regulatory landscape, lack of a common approach, and limited guidance on what actions they should take in terms of regulating terrorist online content require them to take measures based on their own terms of service (Tech Against Terrorism, 2022, p. 28). However, Macdonald, Correia, and Watkin (2019) argue that amid diverging approaches, 'publicly defining' what constitutes terrorist online content would guide individual reviewers and reduce the risk of inconsistent or inappropriate decisions about content removal (Macdonald et al., 2019, p. 190). In agreement, this article further argues that as the de facto regulators of terrorist activities, the responsibility falls on states, and not online platforms, to 'publicly define' what constitutes terrorist online content.

It is important to reiterate that while regulating terrorist online content may not be a high-priority concern for some African countries, the cross-border nature of the threat means that it can directly impact many nations. The challenge for online platforms and content moderators is to consider the diverse legal, political social and cultural contexts across Africa, addressing challenges such as lack of adequate legal provisions and frameworks and regional cooperation, as well as language moderation blind spots.

Regulatory challenges in Africa

Despite progress in establishing laws on terrorism, cybercrime, and online speech, several challenges emerge regarding the regulation of terrorist online content across the continent. First, there is significant fragmentation in approaches at the regional, subregional, and national levels which may result in inconsistent application of the laws, posing

challenges for content moderation. As demonstrated, regional and subregional instruments, as well as national provisions found in South Africa, Kenya, and Nigeria's counter-terrorism law, differ significantly and lack cohesive alignment. Some of the legal provisions do not consider the complexities of terrorist usage of ICTs. For instance, counter-terrorism provisions at the regional level do not envision terrorist usage of ICTs or the prominence of private actors who regulate the digital environment. In contrast, recently amended counter-terrorism laws at the national level, such as those in South Africa and Nigeria, include specific legal provisions to address terrorist-related online content but these provisions differ in terms of their scope. Besides, there remains a lack of clarity regarding the specific measures that law enforcement authorities should take to regulate such content.

Second, the legal provisions discussed above lack clarity on what constitutes 'terrorist online content.' As a result, content moderators may face interpretational challenges leading to 'a fragmented collection of data on terrorism and violent extremism online' (UNICRI and United Nations Office of Counter-Terrorism, 2021, p. 40). Furthermore, the broad and vague nature of the definitions of terrorist publications, statements, or information highlighted above may give national authorities the power to restrict a wide range of speech, including legitimate expression. This raises concerns about fundamental human rights, such as freedom of expression, which should be guaranteed both offline and online.

Third, the existing domestic laws on counter-terrorism lack clear obligations for online platforms regarding terrorist content. This ambiguity makes it difficult to define their roles and responsibilities and leads to inconsistent enforcement policies and inconsistencies in content moderation. As Tech Against Terrorism notes, 'lack of global consensus around who should be responsible for disrupting or removing such sites has hindered the effective management of the threat to date' (Tech Against Terrorism, 2022, p. 4).

Fourth, at a practical level, while there is an increase in terrorist online content in Africa, perceptions of the threat might differ between nations. This variation can directly influence a country's decision on whether to prioritise the regulation of terrorist online content and allocate resources for this purpose. Countries that are perceived as low risk – particularly those with less internet access and/or limited firsthand exposure to terrorism – may not invest heavily in regulating what they view as a minimal threat. Even those that recognise the threat may prioritise other issues such as education, health, infrastructure and unemployment due to limited resources. This may limit efforts to regulate the threat within the continent.

Last, challenges in capacity and digital infrastructure may hinder effective responses. In 2021, Nathaniel Allen estimated that Africa needed an additional 100,000 certified cybersecurity professionals (Allen, 2021, January 19). He also notes that governments often struggle to 'monitor threats, collect digital forensic evidence, and prosecute computer-based crime' stemming from insufficient cybersecurity and technical skills in the public sector. To address this critical gap, law enforcement authorities and counterterrorism agencies should cooperate with the private sector, with stronger capacity to develop the necessary tools to combat terrorism online (UNICRI and United Nations Office of Counter-Terrorism, 2021, p. 42). In this regard, a multifaceted approach that encompasses various dimensions of tackling terrorist online content is required.

Conclusion and recommendations

This article has explored the ways in which terrorist groups in Africa are leveraging online platforms, such as social media, anonymous online platforms, and encrypted messaging services, to disseminate their content, which is increasingly widespread. It finds that while regional and subregional instruments on terrorism, online speech and cybercrime, as well as various national laws on terrorism, can address terrorist online content to various extents, significant legal and practical challenges impact their practical application. The main issue, therefore, is what course of action states should take, considering these legal and practical challenges. Some commentators suggest that states should examine the extent to which existing laws can be repurposed for online space before developing new laws (Berntsson & Janin, 2021). However, this article contends that the emergence of terrorist online content presents new challenges that existing laws struggle to address. As a result, it is necessary to either amend existing laws or develop new laws designed for the digital landscape, all anchored within a comprehensive regulatory framework.

For these reasons, a multifaceted approach that addresses the current legal and practical challenges is desirable. Such an approach includes:

1. Developing a harmonised legal framework. A more unified approach – potentially through initiatives by the AU – could strengthen efforts to address terrorist online content in Africa at the regional, subregional and national levels. This framework should: (i) align the definition of terrorist content with the OAU Convention on the Prevention and Combating of Terrorism to guide member states on their national definitions; (ii) set out the responsibility of states, online providers, and other relevant stakeholders in countering terrorist online content, including guidelines for cooperation; (iii) provide appropriate safeguards to protect fundamental rights such as freedom of expression and right to privacy; and (iv) consider the specific realities of the African continent with unique sociopolitical and economic realities.
2. Amending existing national laws. As new threats emerge, states should consider amending their national laws to address those threats effectively. While countries like Kenya, South Africa, and Nigeria have made efforts to address terrorist publications and content in their recently amended counter-terrorism laws, much more needs to be done. Adequate legal measures should be established to counter terrorist online content, ensuring compliance with human rights standards. Clear duties and responsibilities for content moderation, among online platforms and law enforcement agencies should also be established.
3. Investing in capacity building. African governments should invest in training law enforcement agencies to counter terrorist online content. This may involve equipping them with technical skills in digital forensics, data analytics, Open-Source Intelligence (OSNIT), among others. In situations where resources are scarce due to other pressing national issues, these nations should collaborate with international organisations and private entities to fill the capacity gaps. In addition, seeking funding from Western governments with stronger economies can provide much-needed support for these initiatives.
4. Cooperation with online platforms. As tech companies lead the way in moderating terrorist online content, governments should collaborate with these companies to improve the regulation of such content. Such cooperation may include technical

assistance to strengthen the capacity of law enforcement agencies, along with information sharing on emerging and future threats, enabling effective responses to evolving strategies used by terrorists. However, these partnerships must safeguard users' privacy rights on online platforms, particularly in the context of information sharing initiatives.

5. International cooperation. Given that the Internet is shared globally, cooperation with international organisations, regional bodies, individual states, and other relevant stakeholders is key to improving coordination in the regulation of terrorist online content at different levels. This can entail addressing Africa-specific challenges in preventing and combating terrorist online content, building capacity to address such content, sharing information on cross-border challenges, and strengthening the role of the AU, subregional bodies and individual states. However, emphasised by the AU Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace (2024, para. 67), 'capacity building and all cooperation [in the field of ICT and cyber space] should respect the integrity and security of national ICT infrastructure, and correspond to nationally identified needs and priorities, and respect and protect the confidentiality of national policies and plans.'
6. Developing tools to counter specific challenges. To address the challenge of language moderation blind spots, African states should consider collaborating with international organisations, global online platforms, or Western countries to develop tools and technologies to counter these blind spots. This may involve developing advanced tools and technologies specifically designed to identify terrorist content by analysing contextual language patterns. These tools should also address the risks of predictive bias.
7. Developing counter-narratives. At a softer level, preventive measures such as counter-narratives can play an important role in creating alternative narratives to reduce support for terrorism and its agendas. In October 2023, the AU Peace and Security Council encouraged AU member states to 'collaborate in developing and implementing effective counter-narrative strategies', including 'closely monitor[ing] the use of the Internet and social media' (African Union, 2023, october 27, para. 17). These strategies could offer a unique way to alter terrorist narratives in terrorist publications and content.

The adoption of such a multifaceted approach can greatly improve the ability of African nations to effectively address online terrorist content and mitigate preparatory acts of terrorism. African countries should also endeavour to learn from international best practices. For instance, they should examine legal instruments such as Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content to assess its strengths and weaknesses and evaluate its adaptability to the African context.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Brenda Mwale http://orcid.org/0000-0003-3438-9213

References

African Commission on Human and Peoples' Rights. (2019). *Declaration of principles of freedom of expression and access to information in Africa*. Adopted by the African Commission on Human and Peoples' Rights at its 65th Ordinary Session held from 21 October to 10 November 2019 in Banjul, The Gambia.

African Declaration on Internet Rights and Freedoms. (2014). *African declaration on internet rights and freedoms*. Retrieved from https://africanInternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf

African Union. (2023, October 27). Peace and Security Council 1182nd Meeting. Addis-Ababa. PSC/PR/COMM.1182. Retrieved from https://www.peaceau.org/en/article/communique-of-the-1182nd-of-the-psc-held-on-27-october-2023-on-the-report-of-the-chairperson-of-the-commission-on-counter-terrorism-in-africa

African Union. (2024). Common African position on the application of international law to the use of information and communication technologies in cyberspace.

Aina, F., & Ojo, J. S. (2023). *The "Webification" of jihadism: trends in the use of online platforms, before and after attacks by violent extremists in Nigeria (Global Network on Extremism & Technology)*. London: Global Network on Extremism & Technology.

Allen, N. (2021, January 19). *Africa's evolving cyber threats*. Retrieved from https://africacenter.org/spotlight/africa-evolving-cyber-threats/.

Allen, K. (2022, September 15). Terrorists' use of tech in West Africa must be contained. *ISS Today*. Retrieved from https://issafrica.org/iss-today/terrorists-use-of-tech-in-west-africa-must-be-contained

Ayad, M., Harrasy, A., & Abdullah, M. (2022). *Under-moderated, unhinged and ubiquitous: Al-Shabab and the Islamic State networks on Facebook: Why Al-Shabaab and Islamic State pages and profiles in East African languages continue to plague Facebook*. London: Institute for Strategic Dialogue.

Bellaert, W., Selimi, V., & Gouwy, R. (2021). The end of terrorist content online? In G. Vermeulen & W. Bellaert (Eds.), *EU criminal policy: Advances and challenges* (pp. 163–184). Antwerpen: Maklu-Publishers.

Berntsson, J., & Janin, M. (2021, October 14). Online regulation of terrorist and harmful content. *Lawfare*. Retrieved from https://www.lawfaremedia.org/article/online-regulation-terrorist-and-harmful-content

Cox, K., Marcellino, W., Bellasio, J., Ward, A., Galai, K., Meranto, S., & Paoli, G. P. (2018). Social media in Africa: A double-edged sword for security and development. 2018).

Dahiru, A. (2023, April 17). Terrorists using local language to spread propaganda on Facebook. Retrieved from https://humanglemedia.com/terrorists-using-local-language-to-spread-propaganda-on-facebook/

Dakwak, G. (2023). Statement by Gloria L Dakwak, permanent mission of Nigeria to the United Nations on 'Measures to eliminate international terrorism' 2nd -4th October 2023. Retrieved from. https://www.un.org/en/ga/sixth/78/pdfs/statements/int_terrorism/02mtg_nigeria.pdf

Davey, J., Comerford, M., Guhl, J., Baldet, W., & Colliver, C. (2021). *A taxonomy for the classification of post-organisational violent extremist & terrorist content*. London: Institute for Strategic Dialogue.

Debre, I., & Akram, F. (2021, October 25). Facebook's language gaps weaken screening of hate, terrorism. AP News. Retrieved from https://apnews.com/article/the-facebook-papers-language-moderation-problems-392cb2d065f81980713f37384d07e61f

Department of Planning, Monitoring and Evaluation, Republic of South Africa. (2021). Socio-Economic Impact Assessment (SEIAS). Retrieved from https://www.gov.za/sites/default/files/gcis_document/202105/4-seias-report.pdf

East African Community. (2008). *Draft EAC legal framework for cyberlaws*.

Economic Community of West African states. (2011). *Directive C/DIR. 1/08/11 on fighting cybercrime within ECOWAS*.

European Union. (2021). Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

International Crisis Group. (2018). Al-Shabaab five years after Westgate: still a menace in East Africa. Crisis Group Africa Report No 265.

Kibiono, M. (2023). *Statement on Agenda Item 109 'Measures to eliminate international terrorism' by Amb*. Michael Kiboino, deputy Permanent Representative during the 78th Session of the United Nations General Assembly, 2 October 2023. Retrieved from https://www.un.org/en/ga/sixth/78/pdfs/statements/int_terrorism/04mtg_kenya.pdf

King, P. (2019). Islamic State group's experiments with the decentralised web. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/islamic_state_group_experiments_with_the_decentralised_web_-_p.king_.pdf

Macdonald, S. (2019). Social media, terrorist content prohibitions and the rule of law. *The George Washington University Program on Extremism*.

Macdonald, S., Correia, S. G., & Watkin, A. (2019). Regulating terrorist content on social media: Automation and the rule of law. *International Journal of Law in Context*, *15*, 183–197.

Mahmood, O. S. (2017). More than propaganda: A review of Boko Haram's public messages. Institute for Security Studies. West Africa Report 20.

Meta. (n.d.). *Dangerous organisations and individuals*. Meta Community Standards. https://transparency.fb.com/en-gb/policies/community-standards/dangerous-individuals-organizations

National Information Technology Development Agency. (2022). Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries.

Nelu, C. (2024, June 10). Exploitation of generative AI by terrorist groups. Retrieved from *International Centre for Counter-Terrorism* https://www.icct.nl/publication/exploitation-generative-ai-terrorist-groups

Ogbondah, C. W., & Agbese, P. O. (2018). Terrorists and social media messages: A critical analysis of Boko Haram's messages and messaging techniques. In Mutsvairo, B *The Palgrave Handbook of Media and Communication Research in Africa*.

Organization of African Unity. (1981). *African charter on human and peoples' rights*, adopted on 1 June 1981, entered into force on 21 October 1986.

Organization of African Unity. (1999). *Organization of African unity convention on the prevention and combating of terrorism*, adopted at Algiers on 14 July 1999, entered into force on 6 December 2002.

Parliamentary Monitoring Group. (2022a). Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Bill: public hearings; SAPS 2022/23 APP Addendum; with Deputy Minister, 7 September 2022. Retrieved from https://pmg.org.za/committee-meeting/35488/

Parliamentary Monitoring Group. (2022b). Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Bill: Department response to submissions, 14 September 2022. Retrieved from https://pmg.org.za/committee-meeting/35554/

Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Act (2022).

Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Bill (As introduced in the National Assembly (proposed section 75); explanatory summary of Bill and prior notice of its introduction published in Government Gazette No. 46649 of 1 July 2022), [B 15—2022].

Prevention of Terrorism Act. (2012). Amended in 2023.

Rojszczak, M. (2023). Gone in 60 Minutes: Distribution of terrorist content and free speech in the European Union. *Democracy and Security*, *20*(2), 179–209.

Romaniuk, S., Fabe, A. P., & Nandy, D. (2023, June 23). Terrorist platform migration: The move to smaller, less regulated online spaces. *Global Network on Extremism & Technology*. Retrieved from https://gnet-research.org/2023/06/23/how-do-terrorists-utilise-and-exploit-small-covert-online-spaces/

Southern African Development Community. (2012). *SADC model law on computer crime and cybercrime*.

Tech Against Terrorism. (2022). The threat of terrorists and violent extremist-operated websites. Retrieved from https://www.techagainstterrorism.org/hubfs/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf

Tech Against Terrorism. (2024, March 21). Inside Somalia's war on al-Shabab disinformation, https://techagainstterrorism.org/in-the-news/inside-somalias-war-on-al-shabab-disinformation)

Terrorism (Prevention and Prohibition) Act, 2022.
United Nations General Assembly. (1996). *International covenant on civil and political rights*. Adopted on 16 December 1966 by UN General Assembly resolution 2200A (XXI). (23 March 1976). Entered into force.
United Nations General Assembly. (2018, April 6). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression*. UN doc A/HRC/38/35.
United Nations Interregional Crime and Justice Research Institute (UNICRI) and United Nations Office on Counter-Terrorism. (2021). *Countering terrorism online with artificial intelligence: An overview for law enforcement and counter-terrorism agencies in South Asia and South-East Asia' A Joint Report by UNICRI and UNCCT*. Retrieved from https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf
U.S. Department of State. (2022). Country reports on terrorism 2022: Kenya. Retrieved from https://www.state.gov/reports/country-reports-on-terrorism-2022/kenya
Weimann, G., & Vellante, A. (2021). The dead drops of online terrorism: How jihadists use anonymous online platforms. *Perspective on Terrorism*, *15*(4), 39–53.
X. (n.d.-a). Violent and hateful entities policy, rules and policies. Retrieved from https://help.twitter.com/en/rulesand- policies/violent-entities.
X. (n.d.-b). Perpetrators of violent attacks, rules and policies. Retrieved from https://help.twitter.com/en/rulesand- policies/perpetrators-of-violent-attacks