



*Empowered lives.  
Resilient nations.*

# **Social media in Africa**

**A double-edged sword for  
security and development**

Executive summary

Kate Cox, William Marcellino, Jacopo Bellasio, Antonia Ward,  
Katerina Galai, Sofia Meranto, Giacomo Persi Paoli

## This study explores social media use and online radicalisation in Africa

Information and communication technology (ICT) in Africa is a double-edged sword: while it can promote social, political and economic development, it may also increase opportunities for radicalisation. Twitter, Facebook, YouTube and other social media platforms can arm terrorists with a low-cost tool to attract, train and communicate with followers and potential recruits. Al-Shabaab, Boko Haram, Islamic State of Iraq and the Levant (ISIL) and other violent extremist groups in Africa now use social media to share their messages and attract new recruits.

There is an on-going debate over the role of online activities in the radicalisation process. However, much of this debate has focused on Western countries, particularly in relation to ISIL's online influence of homegrown terrorism and of foreign fighter travel to Iraq and Syria. Less is known about patterns of online radicalisation in Africa and about the extent to which African national governmental strategies focus on addressing this issue.

To address this gap in knowledge, the United Nations Development Programme (UNDP) commissioned RAND Europe to explore social media use and online radicalisation in Africa. This is the first publically available study to analyse how social media is used by al-Shabaab, Boko Haram and ISIL to contribute to radicalisation in seven African countries – Cameroon, Chad, Kenya, Nigeria, Somalia, Sudan and Uganda – by applying lexical and network analysis techniques to primary Twitter data.

This report addresses the following research questions (RQ):

- **RQ1:** What trends can be observed in the use of social media in Africa to contribute to online radicalisation?
- **RQ2:** Have existing counter-radicalisation interventions by African national governments and non-African government agencies:
  - i. Focused on preventing and responding to online radicalisation?
  - ii. Built innovative technological approaches into their design?
- **RQ3:** What implications can be drawn for the improvement of existing programmes and design of future programmes aimed at countering online radicalisation?

The research team analyses these questions through the lens of three case studies focused on al-Shabaab, Boko Haram and ISIL – three of the most lethal Islamist militant groups worldwide in terms of numbers of people killed. To address RQ1, the research team draws on a combination of research interviews, a literature review and Twitter data analysis to identify how these groups use social media in their day-to-day activities and how social media users talk about each organisation. Complementing this analysis and in support of RQ2–3, the interviews and literature review also explore whether government-led strategies in the seven countries focus on countering online radicalisation.

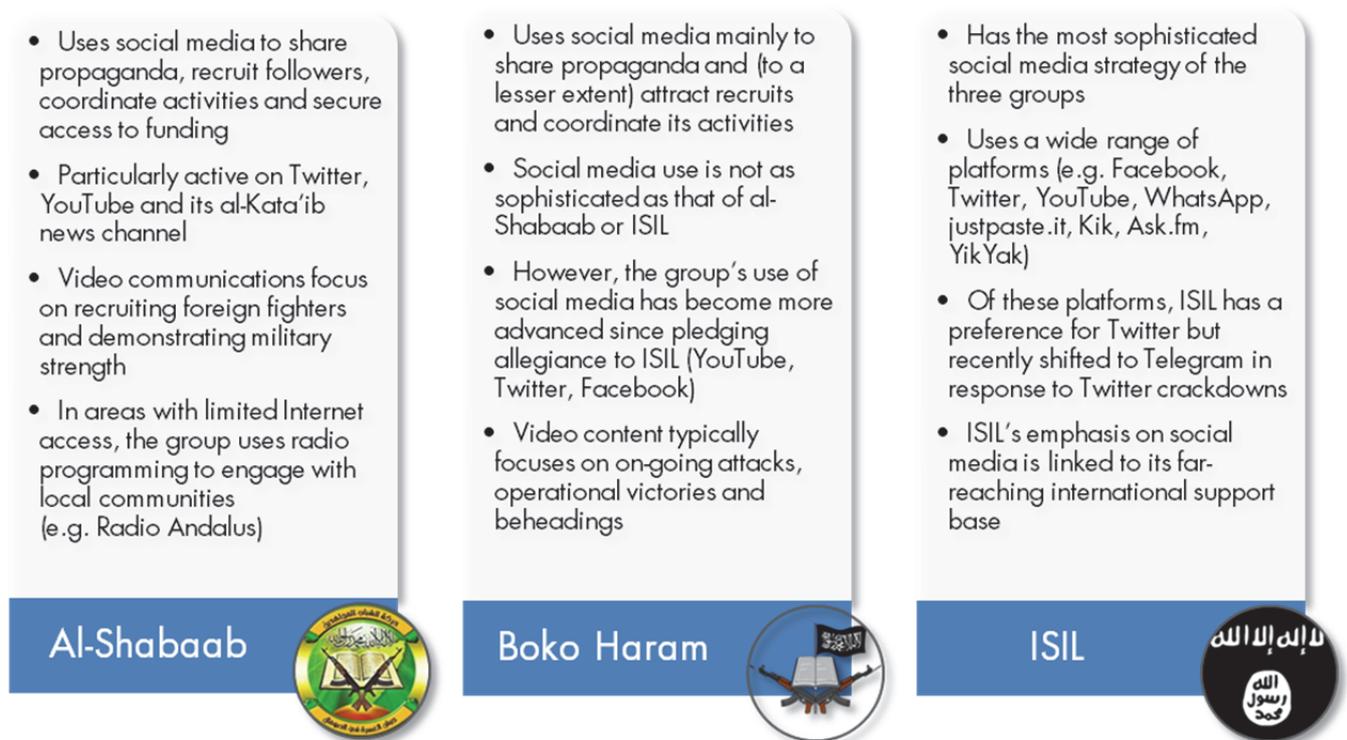
## Al-Shabaab, Boko Haram and ISIL all use social media, albeit to varying degrees and levels of sophistication

Cross-media communications are a core part of the strategies of al-Shabaab, Boko Haram and ISIL, as highlighted by the groups' dedicated branches for media planning, namely al-Shabaab's al-Kata'ib, Boko

Haram’s Media Office of West Africa Province and ISIL’s Al Hayat Media Center. Driven in part by technological advances and expanded Internet access in parts of Africa, the use of social media by all three groups has increased in recent years – although this varies by geographical area depending on the level of ICT penetration.

As Figure S-1 shows, ISIL has the most sophisticated online strategy of the three groups and makes use of the widest range of social media platforms. While Boko Haram’s use of social media is the least advanced of the three groups, it has become more sophisticated since pledging allegiance to ISIL in 2015.

**Figure S-1: Use of social media by al-Shabaab, Boko Haram and ISIL**



While all three groups use social media for propaganda and recruitment, 'offline' influences can also play a role in radicalisation

Boko Haram, al-Shabaab and ISIL all appear to use social media as a propaganda tool. For these groups, social media propaganda is used to claim or publicise attacks or kidnappings with, for example, Boko Haram's kidnapping of 276 schoolgirls in April 2014 sparking the international media campaign known as #BringBackOurGirls. They also use social media propaganda to criticise opponents, demonstrate the effectiveness of their tactics and, in ISIL's case, appeal to potential foreign fighters, their families and potential perpetrators of 'lone wolf' attacks on the West.

There is evidence to suggest that al-Shabaab, ISIL and, to a lesser extent, Boko Haram also use social media to attract recruits, both domestically and internationally. ISIL draws on a variety of platforms including Telegram, Kik and WhatsApp to engage with potential recruits. In part due to YouTube's content removal efforts, al-Shabaab engages with potential recruits through closed chatrooms involving

military commanders and diaspora fighters. While Boko Haram has made some effort to radicalise individuals online – for example, by tweeting links to recruitment videos – the group does not appear to use social media for recruitment to the same extent as al-Shabaab and ISIL.

Social media platforms such as Telegram have equipped ISIL with a free encrypted tool for coordinating its messaging and military planning. However, social media instead creates challenges for al-Shabaab's coordination efforts: the growth of the Internet appears to have led to a 'loss of control' of the narrative by leaders, with messaging becoming increasingly decentralised and independent jihadists reportedly undermining the group's messaging. With the exception of reports that al-Shabaab uses the Internet to secure funding from sympathetic Salafi networks, there is limited publicly available evidence regarding if and how the three groups use social media in order to secure funding.

It is clear that al-Shabaab, Boko Haram and ISIL use social media to share propaganda, attract recruits and coordinate their followers – all of which can contribute to radicalisation. However, a key finding of this study is that these online influences are often complemented by the 'offline' influences of family and peer networks. For example, Boko Haram operatives are said to use 'middle men' in remote areas without Internet access to share social media messaging with local communities through in-person interaction. Similarly, there is evidence to suggest that ISIL attracts young recruits through the influence of religious leaders – as seen in the case of the radicalisation of medical students in Khartoum. In this case and others, 'offline' personal relationships play a key role in the recruitment efforts of the three groups.

## Our analysis identified Twitter communities who discuss activities or attacks relating to al-Shabaab, Boko Haram and ISIL

While our interviews and literature review have focused on a wide range of social media platforms, we also conducted a deeper analysis in relation to one specific platform – Twitter – in order to explore how users based in the seven focus countries discuss content relating to the three groups. This analysis involved three steps: (1) **data crawling** through running targeted search queries aimed at scraping relevant Twitter data from selected dates before, during and immediately after significant events (e.g. major terrorist attacks) since 2012. The reason for focusing on this subset of dates was to capture the effect of these events, with a view to identifying communities of supporters, opponents or neutral observers; (2) **machine-based analysis** of the resulting Twitter dataset, involving social network and lexical analysis approaches; and (3) **research team interpretation** of the results generated through the previous steps.

Overall, the Twitter data analysis identifies 223,152 Tweets across the selected dates and terrorist groups, of which 27,741 are related to al-Shabaab, 159,095 to Boko Haram, and 36,316 to ISIL. The analysis highlights the presence of large, region-based communities engaged in the discussion of activities and events connected to al-Shabaab and Boko Haram, with a smaller community identified in relation to ISIL in the seven focus countries. In the latter case, content appears to have been generated primarily from international accounts and news outlets retweeted by local users.

The majority of news-related content identified across different communities and subsets of the data suggests that on and around key dates of terrorist attacks social media in the region had been inundated with messages posted by users talking about unfolding events. These users are likely to comprise accounts

that are normally not engaged in conversations around the terrorist groups of interest, such as news outlets. In light of this, on a platform like Twitter, wider media-driven discussions generated by occurring events are likely to overshadow slower-paced continuous messaging strategies aimed at, for example, radicalisation and recruitment.

Therefore, in the context of terrorist attacks and associated responses, social media appears to be an important source of information for users. However, a strong degree of uncertainty about the news circulating on social media appears to transpire from keywords and expressions used by users (e.g. ‘cannot verify’, ‘fake’, ‘claim’). This suggests that the establishment of trusted institutional accounts could facilitate the spreading of reliable news and carefully crafted messages in times of crisis, limiting the potential for social media to be used for fake news and terrorist dis- or misinformation.

## Countering online radicalisation is an emerging area for African governments and their overseas partners

While social media is used by all three groups to further their strategic aims, it appears that African governments and their overseas partners are only now starting to recognise and respond to this issue. At the time of writing, strategies for preventing and countering violent extremism (P/CVE) have been introduced in Somalia, Nigeria and Kenya and are under development in Chad, Uganda and Sudan. While the three existing strategies acknowledge the importance of communications and awareness-raising, countering *online* radicalisation appears to be an emerging area of focus. These strategies offer little content specifically on social media use and on which platforms – if any – are used in governmental efforts to target al-Shabaab, Boko Haram and ISIL in Somalia, Nigeria and Kenya.

Similarly, our research identified few examples where overseas government actors have developed programmes with a focus on social media. One example is the United States Agency for International Development’s (USAID) Voices for Peace programme in Burkina Faso, Cameroon, Chad and Niger, which focuses on CVE counter-narratives shared via social media. Beyond this programme, we found limited publically available evidence of social media-related efforts by overseas government actors in the seven focus countries – although we did identify a number of radio-based counter-radicalisation efforts (e.g. the EU-funded STRIVE [Strengthening Resilience to Violence and Extremism] and USAID-coordinated ‘Dandal Kura’ programmes).

## This report presents recommendations for the governments of Cameroon, Chad, Kenya, Nigeria, Somalia, Sudan and Uganda

This study generated three overarching recommendations for the governments of Cameroon, Chad, Kenya, Nigeria, Somalia, Sudan and Uganda. These recommendations are listed in Table S-1, along with activities that could be undertaken to support their implementation.

**Table S-1: Recommendations for policy and programming**

Recommendation (R)	Supporting activities
<b>R1: Develop a bespoke national strategy for countering online radicalisation</b>	<p>Consult stakeholders including the UNDP, (social) media providers, local institutions and law enforcement.</p> <p>Undertake a consultation process through a Working Group for Countering Online Radicalisation or through dedicated workshops.</p> <p>Ensure that national strategies include context, clearly stated objectives, resource requirements, and a stakeholder engagement plan.</p>
<b>R2: After preparing a national strategy, develop counter-online-radicalisation programmes tailored to local context and needs</b>	<p>Ensure that programmes offer reactive social media responses following major attacks, as well as more continuous and preventative counter-narratives online.</p> <p>Maximise visibility by basing programmes on multiple social media platforms, using multiple languages (as relevant) and targeting campaign messaging across sectors.</p> <p>Tailor programming to local context and ensure that messaging is relatable to its audience.</p>
<b>R3: Share lessons on ‘what works’ in countering online radicalisation at the national, regional and international levels</b>	<p>Increase inter-governmental information exchange and cooperation in relation to countering online radicalisation through the creation of online communities.</p> <p>Share lessons learned regarding ‘what works’ in countering online radicalisation and discuss future collaboration opportunities at annual regional roundtables or conferences.</p> <p>Capture findings from these engagements in an annual report or compendium of conference papers.</p>

To support the uptake of these recommendations, the UNDP could develop a common blueprint for national governments to use when developing counter-online-radicalisation strategies (R1), as well as providing guidance on engaging with partners, planning for costs and timings, and understanding technology requirements. The UNDP could also play a role in coordinating the annual regional roundtables or conferences focused on counter-online radicalisation, and in producing and disseminating resulting reports or conference papers (R3).

## Future research is needed in a number of areas

Finally, the report highlights several areas that would benefit from further analysis and exploration:

- Primary research to better understand how social media contributes to individuals’ radicalisation.** Given existing data gaps on the role of social media in the radicalisation process, primary research could be undertaken and involve, for example, 10–15 individual case studies in a selected country affected by terrorist violence and with widespread social media use (e.g. Kenya or Sudan). Each case study could focus on the radicalisation ‘journey’ of former militants and draw on data from interviews with these ex-militants.

- **Mapping initiatives undertaken by local actors to counter online radicalisation in Africa.** While this report focuses on the efforts of national governments, overseas government actors and the UNDP to address online radicalisation, future work could map the efforts of non-governmental organisations (NGOs), civil society organisations (CSOs), schools, religious institutions and other community-level organisations to counter the threat from online radicalisation in Africa, exploring the extent to which social media tools have been used in the delivery of these initiatives.
- **'Deeper dive' research into online radicalisation in African countries.** While this report focuses broadly on seven countries, we recognise the importance of tailoring policy and programming to local contexts. To support understanding of local context, it is recommended that research is undertaken on the political, security and socio-economic dynamics within individual countries. This research could enhance awareness of how these dynamics can affect citizens' engagement with online or traditional media, their susceptibility to radicalisation, and their responsiveness to particular types of government intervention. Within individual countries, analysis could also focus on how these patterns may vary between urban and rural areas. To do this, further Twitter analysis could adopt a more 'bottom-up' approach by focusing on the language used by different communities (e.g. supporters and opponents of specific terrorist groups) in the country or regions of interest.