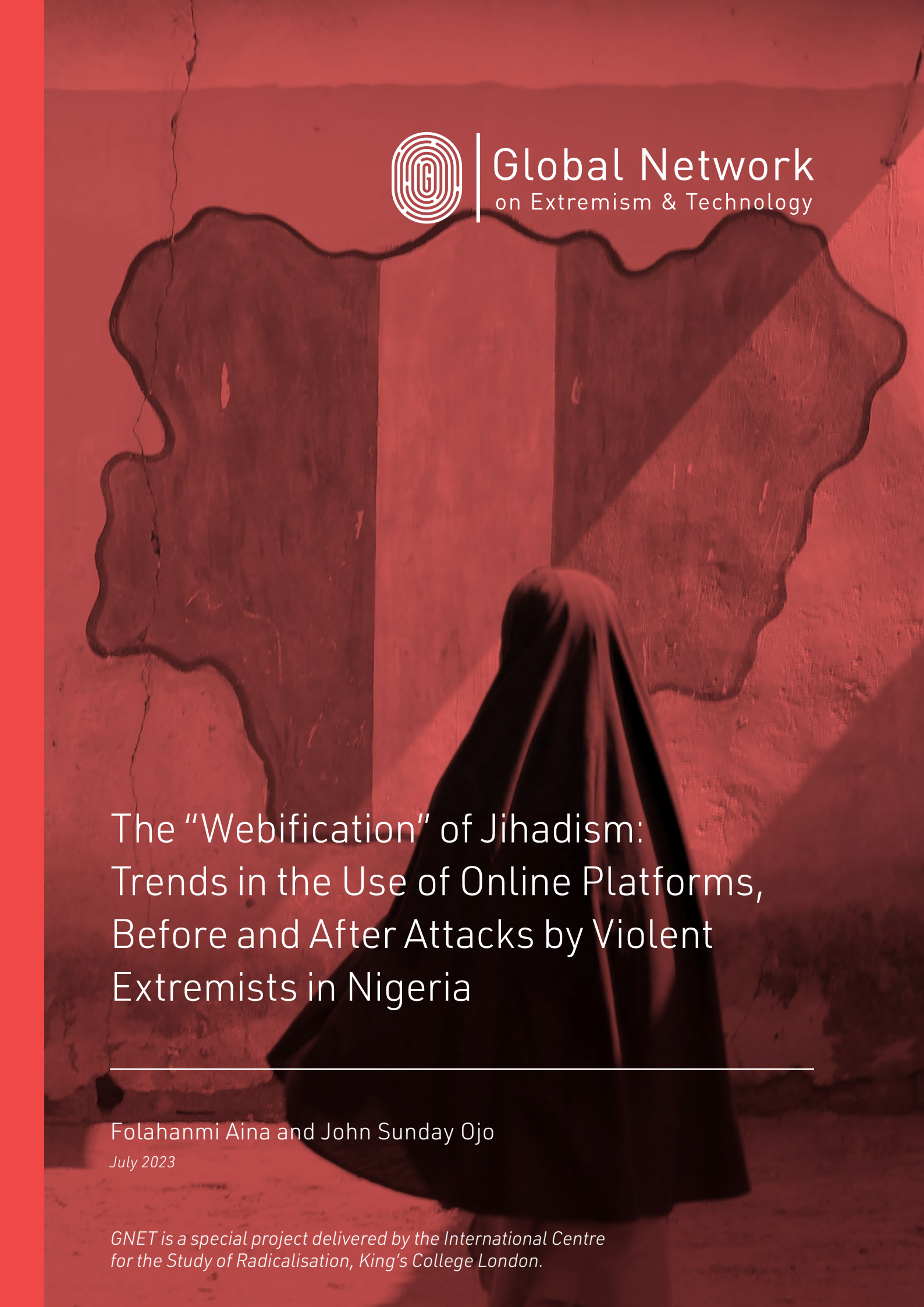

Global Network
on Extremism & Technology

The "Webification" of Jihadism: Trends in the Use of Online Platforms, Before and After Attacks by Violent Extremists in Nigeria

Folahanmi Aina and John Sunday Ojo

July 2023

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The authors of this report are Folahanmi Aina and John Sunday Ojo

Folahanmi Aina recently completed his doctoral studies at the School of Global Affairs, King's College London. His research interests include leadership in national security policy decision-making, terrorism, extremism and insurgency in the Lake Chad Basin and Sahel regions.

John Sunday Ojo is a doctoral researcher at the University of Portsmouth, United Kingdom. His research interests include conflict, peace and security in Africa.

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Recommended citation:
Aina, Folahanmi, and John Sunday Ojo.
"The 'Webification' of Jihadism: Trends in the Use of Online Platforms, Before and After Attacks by Violent Extremists in Nigeria." London: Global Network on Extremism and Technology (GNET), July 2023.
https://doi.org/10.18742/pub01-136.

Executive Summary

Violent extremist organisations (VEOs) use social media platforms to promote extremist content and coordinate agendas. The use of digital platforms to disseminate information and coordinate activities by VEOs in Nigeria has grown considerably in recent years. This report analyses the adoption of social media before and after attacks by Boko Haram, Islamic State of West Africa Province (ISWAP) and Ansaru.

In the post-attack environment, Boko Haram, ISWAP and Ansaru use platforms to claim responsibility and display their strengths against the state’s security forces. By demonstrating their capacity to attack state security forces, the three groups aim to erode the public’s confidence in the state military’s capacity to safeguard national security.

The key findings of this report are as follows:

1. Boko Haram, ISWAP and Ansaru previously leveraged popular social media platforms, including YouTube, Facebook, Telegram and Instagram. These platforms were used to promote propaganda and create awareness regarding upcoming attacks. However, all three groups have now had their use of these platforms restricted or banned.
2. ISWAP has switched to using WhatsApp as a secure platform for communication before, during and after attacks. Rocket.Chat and Telegram have also been instrumental in ISWAP’s information dissemination.
3. Boko Haram uses Telegram to share its activities in the pre-attack and post-attack environments.
4. Ansaru has yet to appear on social media platforms due to its underground activities, which are hard to monitor.
5. The recent acquisition of high-speed satellite internet has enhanced ISWAP’s communication with its audience and enabled coordinated attacks.

Combating the exploitation of social media platform by VEOs requires a multidimensional approach. Effective collaboration with technology companies becomes imperative to identify extremist content. Building technological infrastructure for the state requires synergistic collaboration with the military and intelligence agencies to enable the removal of extremism from social media platforms. Devising multilingual and specialised algorithms to detect coded extremism messages and audio-visual content is essential for effective counter-extremism digital architecture. Investing in current technology through research and algorithm development must be prioritised to identify violent extremist content in Nigeria and beyond.

Contents

1 Introduction

The activities of violent extremist organisations (VEOs), such as Boko Haram and its breakaway factions, the Islamic State in West Africa (ISWAP) and Ansaru, threaten peace and security in Nigeria and the wider region. Attacks by these groups significantly increased in 2014, with attacks occurring almost daily.[1] According to the United Nations Development Programme, violence committed by Boko Haram and ISWAP has killed about 350,000 people since 2009.[2] As of February 2023, violence perpetrated by the three groups has resulted in at least 2.3 million internally displaced persons in Adamawa, Borno and Yobe, the most affected states situated in the northeast of Nigeria.[3]

The use of technology by VEOs in Nigeria is not new. As far back as 2010, Boko Haram members used Ansar al-Mujahideen, a jihadist web forum, to propagate their agendas and seek recruits. ISWAP’s media team, headed by Abba Yusuf (also known as Abu Rumaisa), use satellite and Android phones, high-speed printers, laptops, high-definition digital cameras, clip-on microphones, walkie-talkies, data compression and archiving software.[4] The proliferation of electronic messaging platforms, including social media platforms, has seen VEOs take advantage of these tools. Social media platforms dominate almost every aspect of human interaction, from interpersonal relations to the global economy; VEOs are no exception.[5]

The three groups have continued to exploit online media platforms to promote their attacks including suicide bombings, kidnappings, mass killings and laying ambushes for the Nigerian military. Over time, Boko Haram, ISWAP and Ansaru have continued to adopt and utilise different online platforms before and after staging their attacks. Understanding the trends in the usage of these platforms is critical to unpacking the motives and operational developments related to attacks perpetrated by these jihadist groups.

This report seeks to answer the following research questions:

i. What do the trends in the use of online electronic platforms reveal about the evolution of the operational tactics before and after attacks carried out by jihadist groups in Nigeria?

ii. How could the trends in the use of online electronic platforms before and after attacks carried out by jihadist groups better inform counterterrorism policy?

1 Counter-Terrorism Guide, Boko Haram. Available from: https://www.dni.gov/nctc/groups/boko_haram.html.
2 UNDP, “Assessing the Impact of Conflict on Development in North-east Nigeria,” United Nations Development Programme, 2021. Available from: https://www.ng.undp.org/content/nigeria/en/home/library/human_development/assessing-the-impact-of-conflict-on-development-in-north-east-ni.html.
3 International Organization for Migration (IOM), DTM Nigeria – Displacement Report 43 (February 2023).
4 Malik Samuel, “ISWAP’s use of tech could prolong Lake Chad Basin violence,” ISS Today, last modified 13 April 2023, https://issafrica.org/iss-today/iswaps-use-of-tech-could-prolong-lake-chad-basin-violence.
5 Samantha Bradshaw, “Influence Operations and Disinformation on Social Media,” Centre for International Governance Innovation, last modified 23 November 2020, https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/.

VEOs in Nigeria disseminate information regarding their intentions before and after attacks using online videos on social media platforms, particularly Telegram and Facebook. Ansaru, the first breakaway faction from Boko Haram,[6] initially used Telegram. However, since its re-emergence between 2012 and 2015, Ansaru transitioned to using Facebook to communicate its intent before and after its attacks. Boko Haram, meanwhile, is known to release videos before and after staging its attacks primarily through Telegram and Facebook. This dissemination is done chiefly through the accounts of individual members. In the past, Boko Haram disseminated videos through an online news platform in Nigeria called Sahara Reporters. Prior to its direct adoption of social media platforms, Boko Haram also relied on journalists with Agence-France-Presse, to whom it sent its videos.[7] ISWAP, like Boko Haram, also operates Facebook and Telegram accounts to disseminate information before and after its attacks, such as showing kidnapped hostages and making demands.

This report is divided into five sections. First, we provide an overview of VEOs’ use of online platforms and an overview of the research design. Second, we provide a synopsis of Boko Haram and its splinter groups, ISWAP and Ansaru. Third, we analyse the use of online platforms by VEOs and the distinct trends before and after attacks. Fourth, we present the research findings and implications for Nigeria’s national security policies before presenting our conclusions and recommendations.

6 Jacob Zenn, “Electronic Jihad in Nigeria: How Boko Haram Is Using Social Media,” Jamestown, last modified 9 December 2017, https://jamestown.org/program/electronic-jihad-nigeria-boko-haram-using-social-media/.
7 ibid.

2 Use of Online Platforms by Violent Extremist Organisations

Across the world, VEOs use a range of online platforms for radicalisation, recruitment, propaganda, psychological influence operations and general communications.[8] Propaganda remains one of the most common elements in many, if not all, terrorist incidents. VEO propaganda is designed to instil fear in target populations, win associate approval and inspire new adherents.[9]

VEOS attempt to create an atmosphere of terror using various disinformation tactics and strategies.[10] The threat posed by terrorists to both states and their societies is less the physical damage they inflict than their adverse psychological influence.[11] Some of these tactics pre-date modern media coverage as evidenced in the activities of ancient terrorist groups, such as “the Assassins”, who operated in the Middle East in the tenth century, and “the Zealots”, who campaigned against the Roman occupation of what is now Israel.[12]

In more recent times, VEOs’ use of social media platforms has proved successful in recruiting foreign terrorist fighters, especially in war zones.[13] Notably, Islamic State used narrative advertising – stories that appeal to emotions and desires – to establish a strong connection with its target audience.[14] Al-Qaeda produced military instruction manuals and videos online in multiple languages.[15] These online strategies offer an opportunity better to understand the trends of VEOs’ internet use.

While trend data provides valuable insights into the foundational values of these terrorist groups, that information adds little connecting attitude and opinion formation regarding behavioural intent.[16] Instead, the use of online platforms by VEOs serves as a force multiplier, increasing their striking power without necessarily increasing their size.[17] As James Forest contends, the global proliferation of

8 John R. Vacca, ed., *Online terrorist propaganda, recruitment, and radicalization*, CRC Press, 2019; Charlie Winter, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino and Johanna Fürst, “Online extremism: Research trends in internet activism, radicalization, and counter-strategies,” *International Journal of Conflict and Violence (IJCV)* 14 (2020): 1–20; Ryan Scrivens, Paul Gill, and Maura Conway, “The role of the internet in facilitating violent extremism and terrorism: suggestions for progressing research,” *The Palgrave handbook of international cybercrime and cyberdeviance* (2020): 1417–1435; Anne Aly, Dana Weimann-Saks, and Gabriel Weimann, “Making ‘noise’ online: An analysis of the say no to terror online campaign,” *Perspectives on Terrorism* 8, no. 5 (2014): 33–47.

9 Norman E. Emery, Robert S. Earl and Raymond Buettner, “Terrorist use of information operations,” *Journal of Information Warfare* 3, no. 2 (2004): 14–26.

10 ibid.

11 Robert J. Johnson, and Stevan E. Hobfoll, “Mental Health and Terrorism” in *A Handbook for the Study of Mental Health: Social Contexts, Theories, and Systems*, edited by Teresa L. Scheid and Tony N. Brown, 2nd ed., 384–406. Cambridge: Cambridge University Press, 2009.

12 N. Johnson, “How ISIS is waging a ‘war of ideas’ through social media,” The Daily Signal, 28 July 2015, http://dailysignal.com/2015/06/08/how-isis-is-waging-a-war-of-ideas-through- social-media/

13 ibid.

14 Anna Kruglova, “‘I will tell you a story about Jihad’: ISIS’s propaganda and narrative advertising,” *Studies in Conflict & Terrorism* 44, no. 2 (2020): 115–37.

15 James J. F. Forest, “Influence Warfare and Modern Terrorism,” *Georgetown Journal of International Affairs* 10, no. 1 (2009): 81–89, https://www.jstor.org/stable/43134193.

16 Paul S. Lieber and Peter J. Reiley, “Psychological Operations to Counter Online Radicalization”, in *Special Operations: Out of the Shadows*, eds. Charles Marsh, Joseph D. Kiras and Peter J. Blocksome, Boulder, CO: Lynne Rienner Publishers, 2020, 125–37.

17 Jonathan R. White, *Terrorism and homeland security*, Cengage Learning, 2016.

information technology provides a new tool for influencing populations’ perceptions and emboldens terrorists and insurgents like never before.[18] Engagements within the “narrative space” by VEOs have become a growing concern for security forces and intelligence services tasked with countering the spread and effects of these strategies. Some of the most common online platforms VEOs and jihadist groups use include Twitter, Telegram, YouTube and Facebook. Less common applications include Google Drive, Sendvid, Google Photos and the Web Archive, among others.[19]

The messaging warfare embarked upon by VEOs across the globe has also allowed groups to leverage the capabilities of affiliate groups. While terrorism is not new to the world, the concept of information operations, increasingly adopted by terrorist groups, remains relatively new.[20] It is believed that information operations entail using information-related capabilities to influence, disrupt, corrupt or usurp the decision-making of a target audience.[21] Beyond operating their underground television studios, print media production and websites, VEOs also rely on traditional media houses as proxy couriers to distribute and transmit specific messages within society. By utilising online platforms, VEOs can amplify their quest to harness the power of information in a manner that not only sways public attention but also puts pressure on decision-makers to act in ways favourable to VEO objectives.[22]

The discourse on the usage of online platforms in promoting extremist propaganda, recruitment processes and funding has been explored by various scholars.[23] Social media architecture has also played a fundamental role in mobilising violent extremists worldwide.[24] Individuals employing these online platforms to promote extremist content have increased, constituting about 90% of extremists, as estimated by PIRUS data.[25] Several schools of thought have highlighted that online platforms are potent weapons for propagating jihadism.[26] Numerous academic approaches have failed to establish how violent extremists employ online platforms in the pre- and post-attack environments.

18 See Forest, “Influence Warfare and Modern Terrorism”.
19 Maura Conway, Moign Khawaja, Suraj Lakhani et al., “Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts,” *Studies in Conflict & Terrorism* 42, no. 1-2 (2018): 141–60.
20 See Emery et al. “Terrorist use of information operations”.
21 Joint Concept for Operating in the Information Environment (JCOIE) “Distribution Statement A Approved for Public Release” (2018), available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.
22 Leigh Armistead, *Information operations matters: best practices*, Potomac Books, 2010; Emery et al., “Terrorist use of information operations”.
23 See Conway, “Disrupting Daesh”; Scrivens et al., “The role of the internet”.
24 Jytte Klausen, “Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq,” *Studies in Conflict & Terrorism* 38, no. 1 (2015): 1–22; Katie Cohen, Fredrik Johansson, Lisa Kaati and Jonas Clausen Mork, “Detecting linguistic markers for radical violence in social media,” *Terrorism and Political Violence* 26, no. 1 (2014): 246–56.
25 Michael Jensen, Patric James, Gary LaFree, Aaron Safer-Lichtenstein and Elizabeth Yates, “The use of social media by United States extremists,” *National Consortium for the Study of Terrorism and Responses to Terrorism* (2018).
26 James A. Piazza, and Ahmet Guler, “The online caliphate: Internet usage and ISIS support in the Arab world,” *Terrorism and political violence* 33, no. 6 (2021): 1256–75.

3 Methodology

This report utilises a qualitative research design of a single case study of VEOs in Nigeria. The project focuses on jihadist groups driven by political ideology in Nigeria, including Boko Haram, ISWAP and Ansaru. Data collection took place over five months between November 2022 and March 2023. Collected data covers the periods from 2009 to 2023. Data was obtained from secondary sources, which include academic journal articles, reports and local and international online news reports. Adopting an in-depth case study of Nigeria allowed us to provide a more detailed analysis with the intent that these empirical findings can then be generalised to other jihadist VEOs.

The research design for this project is descriptive, utilising process tracing. The overall strategy adopted for the research is exploratory in nature rather than confirmatory or disproving.

Data Analysis

This research analyses the collected data using thematic analysis. Braun and Clarke define thematic analysis as “a method for identifying, analysing, and reporting patterns (themes) within data”.[27] One significant advantage of this method is that “thematic analysis can be a method that works both to reflect reality and to unpack or unravel the surface of ‘reality.’” A theme is defined as capturing “something important about the data in connection with the research question, which represents some level of patterned response or meaning within the data set.”[28] The available materials were reviewed while considering the initial themes of interest: jihadist groups in Nigeria penetrate internet to coordinate attacks; Boko Haram’s use of online platforms to disseminate information; Nigerian jihadist groups employed social media before and after attacks. Further themes were highlighted and extracted from the existing data using qualitative analysis.

27 Virginia Braun and Victoria Clarke, “Using thematic analysis in psychology,” *Qualitative research in psychology* 3, no. 2 (2006): 77–101.
28 ibid.

4 VEOs in Nigeria: Boko Haram, ISWAP and Ansaru

The emergence and historical trajectories of VEOs in Nigeria are complex and multi-dimensional. We highlight four core contributors to the rise of VEOs in Nigeria. First, the region of Northern Nigeria, where the VEOs under investigation emerged, has long been considered the centre of a socio-economic deficit constituting chronic poverty, unemployment and educational underdevelopment.[29] VEOs in this region leveraged these socio-economic conditions to justify the emergence and resurgence of violence against the state. Second, VEOs in Northern Nigeria utilise a religious ideology embedded in a misinterpretation of Islam. VEOs in Northern Nigeria have rejected the dominance of Western education throughout the country.[30] Third, historical factors that facilitate tensions between ethnic and religious groups, aggravated by economic competition among diverse social groups, triggered violence and radicalised youths towards extremism.[31] Fourth, the external forces of transnational VEOs, such as Al-Qaeda in the Islamic Maghreb (AQIM) and Islamic State, facilitated the rise of VEOs in Nigeria.[32] In this section, we provide an overview of the three VEOs under investigation: Boko Haram, ISWAP and Ansaru.

Boko Haram

The words “Boko Haram” stem from the Hausa language and denote the prohibition of Western education. The group of the same name is a radical Islamic group founded in 2002 by Mohammed Yusuf in Borno State, northeastern Nigeria. Known originally as *Jama’atu Ahlus-Sunnah Lidda Awati wal Jihad* (JASJ), the group was founded on the principles of Islam, seeking to establish an Islamic state and Sharia law as a framework to replace the governance system within Nigeria. The group claimed that the existing governance system was beset by corruption and economic inequalities. In 2009, the group transformed from a peaceful organisation to an insurgent organisation managed by Islamic extremists. This epoch marked the radical transformation of the group from a mere Islamic group to a terrorist organisation that carried out attacks against civilians, religious centres, international organisations and government institutions.[33] The gruesome attacks by the group drew government attention, which led to the arrest of its

29 Ojochenemi J. David, Lucky E. Asuelime and Hakeem Onapajo, *Boko Haram: the socio-economic drivers*, Switzerland: Springer International Publishing, 2015.
30 Akinola Olojo, “Nigeria’s troubled north: Interrogating the drivers of public support for Boko Haram,” Retrieved 12 August 2013: 2014.
31 Peter Mbah, Chikodiri Nwangwu and Herbert C. Edeh, “Elite Politics and the Emergence of Boko Haram Insurgency in Nigeria,” *TRAMES: A Journal of the Humanities & Social Sciences* 21, no. 2 (2017).
32 Usman Ladan, “Transnational Terrorism Revisited: Is Boko Haram an al-Qaeda Affiliate?,” *African Conflict & Peacebuilding Review* 12, no. 1 (2022): 105–26.
33 John Sunday Ojo, “Governing ‘ungoverned spaces’ in the foliage of conspiracy: Toward (re) ordering terrorism, from Boko Haram insurgency, Fulani militancy to banditry in northern Nigeria,” *African Security* 13, no. 1 (2020): 77–110.

leader.[34] Yusuf was killed in police custody after his arrest in 2009. Yusuf's death triggered anger from his followers and violence erupted between the group and the Nigerian security forces. This period experienced the most destructive and fatal engagements between Boko Haram and the Nigerian security forces.[35]

On 7 March 2014, Abubakar Shekau, who replaced Yusuf as a leader, pledged allegiance to Abu Bakr al-Baghdadi, the caliph of the Islamic State in Syria and Iraq (IS), transforming Boko Haram into an international terrorist network.[36] This period saw the transition of multiple groups from local jihadists to international terrorist networks across the Lake Chad region. This network of VEOs covered Nigeria, Chad, Cameroon and Niger. The relationship between al-Qaeda and Boko Haram has become a regional and transnational security dilemma for Lake Chad countries. Since its affiliation with the global jihadist network, Boko Haram has adopted operational modes that have been reinforced by al-Qaeda's financial, technical and operational backing.[37] Such franchised operational reinforcement guaranteed Boko Haram's intelligence-gathering capabilities, recruitment, guerrilla warfare strategies and logistical advancements. Boko Haram has stated: "Boko Haram is just a version of al-Qaeda, which we align with and respect … We support Osama bin Laden, and we shall carry out his commands in Nigeria until the country is totally Islamized."[38]

Boko Haram employs different strategies, including kidnapping for ransom to finance its active engagement, bombings, assassination and ambushing and killing vulnerable targets.[39] The most prominent kidnapping operation was that of female students from Chibok Government Girls Secondary School, where Christians constituted 70% of the student population.[40]

In 2015, a video circulated by Boko Haram affirmed its allegiance to IS, stating that "we announce our allegiance to the caliph … and will hear and obey in times of difficulty and prosperity. We call on Muslims everywhere to pledge allegiance to the caliph."[41] Boko Haram's affiliation with IS automatically enhanced its operational capacity, as such affiliation had for other terrorist groups in Algeria, Egypt, Tunisia, Libya and Morocco.[42] Boko Haram has exploited the Sahelian region's political crises and fragile conditions to build networks with non-state armed groups and advance its operational capacity. In May 2021, Boko Haram leader Shekau was killed by the splinter group ISWAP during a face-off over territorial and ongoing leadership control of the group.[43]

34 ibid.
35 ibid.
36 John Sunday Ojo, "Franchising Terrorism and Insurgencies: From Al-Qaeda, ISIS to Boko Haram," In R. Scott, *Handbook of Terrorist and Insurgent Groups: A Global Survey of Threats, Tactics, and Characteristics* (forthcoming) CRC Press; Virginia Comolli, "Boko Haram and Islamic State," in Simon Staffell and Akil Awan (eds), *Jihadism Transformed: Al-Qaeda and Islamic State's Global Battle of Ideas* (2016).
37 Jacob Zenn, *The Al-Qaeda Accelerant in Boko Haram's Rise*, United States Naval War College, Center on Irregular Warfare and Armed Groups, 2017.
38 Isaac Kfir, "The Boko Haram Reader: From Nigerian Preachers to the Islamic State," *Journal of Islamic Studies* 30, no. 3 (2019): 435–7.
39 See Ojo, "Governing 'ungoverned spaces'".
40 Jim Muir, "Nigeria's Boko Haram pledges allegiance to Islamic State," *BBC News*, 7 March 2015.
41 ibid.
42 Martin Ewi, "What does the Boko Haram-ISIS alliance mean for terrorism in Africa?," ISS Today, last modified 17 March 2015, https://issafrica.org/iss-today/what-does-the-boko-haram-isis-alliance-mean-for-terrorism-in-africa.
43 John Campbell, "Nigerian Terrorist Abubakar Shekau: Dead or Alive – and Does it Matter?," Council on Foreign Relations, 2021, last modified 24 May 2021, https://www.cfr.org/blog/nigerian-terrorist-abubakar-shekau-dead-or-alive-and-does-it-matter.

Islamic State in West Africa Province (ISWAP)

The indiscriminate killing of civilians under Abubakar Shekau’s leadership created tension within Boko Haram’s organisational structure. This tension led to fragmentation, with Abu Musab al-Barnawi forming the Islamic State in West Africa (ISWAP) in 2016.[44] ISWAP’s operational domain is along the four geographical axes of Lake Chad: Cameroon, Nigeria, Niger and Chad. In contrast, Boko Haram became primarily limited to the Sambisa Forest in northeastern Nigeria.

ISWAP’s foot soldiers are estimated to number between 4,000 and 5,000 fighters,[45] a figure believed to surpass that of Boko Haram. Many of the members of the Shekau-led Boko Haram joined ISWAP following his demise in 2021.[46] Boko Haram and ISWAP have leveraged the political crises in North Africa, Central Africa and the Sahel due to the lack of government presence in these regions and the easy access to illicit flows of arms.[47] ISWAP’s unrelenting attacks on military targets and its varied funding sources – kidnappings for ransom, taxation on fishing, livestock and farm produce, foreign donations, cattle rustling, looting and other commercial engagements with the local populace in less governed environments where state presence is limited – have proven its resilience and operational sustainability.[48] These revenue sources generate about £5 million per month for ISWAP.[49] Establishing a resilient economic supply chain within the local populace effectively guarantees ISWAP’s revenue flows.[50] Cementing relationships with the local populace was one of the instruments adopted by ISWAP to maintain its dominance in the Lake Chad region. ISWAP has increasingly leveraged its social base to promote friendly relationships with local communities, replacing the state as a social provider in ungoverned areas, thereby contributing to the group’s resilience in the region.[51]

In 2022, violence orchestrated by ISWAP in the region reduced by 27% compared to 2021. This could have been the result of a robust social contract established between ISWAP and local communities. However, this does not represent a holistic defeat of ISWAP in the Lake Chad region.[52]

Ansaru

Ansaru is an Islamist militant group that first emerged in 2012 in Nigeria. Ansaru is a splinter group of Boko Haram. “Ansaru” is derived from an Arabic word meaning helpers or supporters. It is believed that the group was sponsored by Khalid al-Barnawi, who claimed to have been trained by AQIM and several other regional networks. Some of Ansaru’s prominent attacks include the kidnapping of a French engineer in 2012, the murder of seven foreign workers in

44 See Ojo, “Governing ‘ungoverned spaces’”.
45 Congressional Research Services, Boko Haram and the Islamic State West Africa Province by Congressional Research Services, 24 February 2022.
46 ibid.
47 Alessio Iocchi, “The Boko Haram Franchise and the War on Terror in Nigeria,” *HeinOnline*, accessed 4 June 2023, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/dirquesp15&section=30.
48 See Congressional Research Services, Boko Haram and the Islamic State West Africa Province.
49 Malik Samuel, “Boko Haram’s deadly business: an economy of violence in the Lake Chad Basin,” Institute for Security Studies, 5 October 2022.
50 Samuele Zuffa, Islamic State West Africa Province (ISWAP), Grey Dynamics, 22 February 2023.
51 See Samuel, “Boko Haram’s deadly business”.
52 See Zuffa, Islamic State West Africa Province.

2013 and the killing of Italian and British citizens in 2014.[53] Following Ansaru’s split from Boko Haram, the group operated independently before it defected back into the Boko Haram faction led by Shekau[54]

When compared to Shekau’s Boko Haram, Ansaru engages in minimal civilian targeting and focuses primarily on Western targets. Of all Boko Haram attacks in 2016, only 9% were carried out by Ansaru.[55] Three primary factors triggered Ansaru’s fragmentation from Boko Haram. First were ideological differences: while Boko Haram initially opposed Western education and Nigeria’s governance model, Ansaru appealed to the global jihadist mission. Second, the indiscriminate killings of Muslim brothers by Shekau-led Boko Haram further reinforced the division between the two groups. Third, while Shekau’s Boko Haram was attracted to local attacks, Ansaru focused on international targets such as companies, international organisations and multilateral institutions. Ansaru was also unhappy with the autocratic organisational structure proposed by Shekau.[56]

In April 2016, Ansaru’s leader Khalid al-Barnawi was arrested by Nigerian security forces and between 2016 and 2019 the group remained underground. However, the recent resurgence of Ansaru in northwest Nigeria in Sokoto, Zamfara, Katsina, Kaduna and Niger states, where armed bandits operate, redefined the dynamics of the organisation.[57] Ansaru took advantage of herder-farmer conflicts that facilitated the emergence of armed banditry in northwest Nigeria.[58] Ansaru started supplying arms and weapons, training armed bandits and providing logistics for several attacks carried out by these armed groups in the northwest. Ansaru did not claim responsibility for the attacks until January 2020.[59]

53 United States Department of State, 2017.
54 Khalid al-Barnawi, “Nigeria Islamist group head ‘arrested’,” *BBC*, 3 April 2016.
55 Hilary Matfess, “The New Normal: Continuity and Boko Haram’s Violence in North East Nigeria,” Armed Conflict Location and Event Data Project (ACLED), 2019, https://acleddata. com/2019/02/11/the-new-normal-continuity-and-boko-harams-violence-in-north-east-nigeria/.
56 Jacob Zenn, Atta Barkindo and Nicholas A. Heras, “The ideological evolution of Boko Haram in Nigeria: Merging local Salafism and international Jihadism,” *The RUSI Journal* 158, no. 4 (2013): 46–53; See Matfess, “The New Normal”.
57 Jacob Zenn and Caleb Weiss, “Ansaru Resurgent,” *Perspectives on Terrorism* 15, no. 5 (2021): 46–58.
58 John Sunday Ojo, Samuel Oyewole and Folahanmi Aina, “Forces of Terror: Armed Banditry and Insecurity in North-west Nigeria,” *Democracy and Security* (2023): 1–28.
59 See Zenn and Weiss, “Ansaru Resurgent”.

5 Trends in the Use of Online Platforms before and after Attacks: The Case of VEOs in Nigeria

VEOs in Nigeria have evolved their tactics and operations, including using online platforms to disseminate information both before and after their attacks. Boko Haram, ISWAP and Ansaru have adopted various platforms to perpetrate and amplify their nefarious activities. These include Twitter, Facebook, YouTube, mobile phone text messaging, satellite phones and, in more recent times, Telegram.[60, 61] Several other elements used to support smooth communication on social media include WiFi, walkie-talkies, high-speed printers, high-resolution digital cameras and data compression.[62] While ISWAP relies heavily on WhatsApp and especially Telegram to facilitate internal and external communications, these two applications have been adopted as preferred platforms by Boko Haram and Ansaru. It is believed that ISWAP owns more than fifty Telegram accounts. Telegram is used due to minimal user monitoring and restrictions.[63]

Gaining access to these channels requires having to pass a verification process first.[64] The channel administrator verifies members’ identities through their account name. The administrator asks the name of each member’s commander (*Qaid*) and from which command (*Jaesh*) they come.[65] Those who fail these tests are denied access or removed from the group. Other ways to gain access to ISWAP’s Telegram channels include obtaining links to the Telegram channels from its broader networks.[66] For instance, in 2019, Ansaru launched two Telegram accounts, promoting content in English and Hausa, as Hausa is the dominant language in ISWAP, Ansaru and Boko Haram enclaves.

In November 2019, Telegram clamped down on several jihadist channels in cooperation with Europol. In response, al-Qaeda’s media cohort engineered a new Rocket.Chat server devoted to the activities of Ansaru and its supporters.[67] Rocket.Chat is a decentralised, encrypted social media platform.[68] As part of efforts to reduce direct interactions within these channels, thereby reducing monitoring risks, ISWAP increasingly relies on bots. Besides Telegram, ISWAP also

60 Chris Wolumati Ogbondah and Pita Ogaba Agbese, “Terrorists and social media messages: a critical analysis of Boko Haram’s messages and messaging techniques,” *The Palgrave Handbook of Media and Communication Research in Africa* (2018): 313–45.
61 Jamestown Foundation, *Electronic Jihad in Nigeria: How Boko Haram Is Using Social Media*, 9 December 2017, available at: https://www.refworld.org/docid/5b728ca2a.html.
62 Malik Samuel, “Conflict dynamics, giving violent extremists the upper hand,” ISS, 13 April 2023.
63 William Babalola, “WhatsApp, Telegram, Others Are Tools for ISWAP – Report,” 19 September 2022.
64 Aliyu, Dahiru, “Terrorists Using Local Language To Spread Propaganda On Facebook,” HumAngle, 17 April 2023.
65 ibid.
66 ibid.
67 See Peter King, “Islamic State group’s experiments with the decentralised web.” In conference paper. Hague: Europol. Retrieved 2019; Zenn and Weiss, “Ansaru Resurgent”.
68 ibid.

uses Rocket.Chat.[69] The adoption of Rocket.Chat reflects ISWAP’s concerns over regular infiltrations into its Telegram by Nigeria’s intelligence agencies.[70]

In our study, we found the following:

a. ISWAP fighters on the ground mostly use WhatsApp to communicate prior to attacks and during attacks.

b. In the past five years, ISWAP has not been able to use Facebook or Twitter because there have been clampdowns by the Nigerian security services.

c. Nigerian intelligence services have successfully infiltrated ISWAP’s Telegram channels more than once, resulting in group members regularly changing their Telegram channels and gravitating towards Rocket.Chat.

d. Ansaru does not release communications frequently, which has made it more difficult to track down its online activities. However, the group has increasingly relied on local languages, such as Hausa, in disseminating al-Qaeda propaganda, especially on Facebook.

e. Ansaru openly announced the creation of its public and private WhatsApp and Telegram channels through Facebook.

f. Ansaru’s use of Facebook is mainly intended to spread inflammatory messages as well as to incite violence.

g. Boko Haram and ISWAP mostly share information about their planned attacks through their Telegram channels. Boko Haram and ISWAP rarely issue warnings on planned attacks but occasionally claim responsibility for attacks through video releases.

h. Before the split that created ISWAP, Boko Haram sent videos directly to journalists and media houses.

i. ISWAP relies on high-speed satellite internet to communicate with IS and spends as much as $6,000 monthly as the cost of data for its Thuraya WiFi.

j. ISWAP has begun to gravitate towards using Rocket.Chat as a viable complement to Telegram.

k. Al-Qaeda-affiliated groups operating in Nigeria are more sophisticated than ISWAP-affiliated groups in the use of social media, whereas, in terms of messaging, the reverse is the case.

69 ibid.
70 ibid.

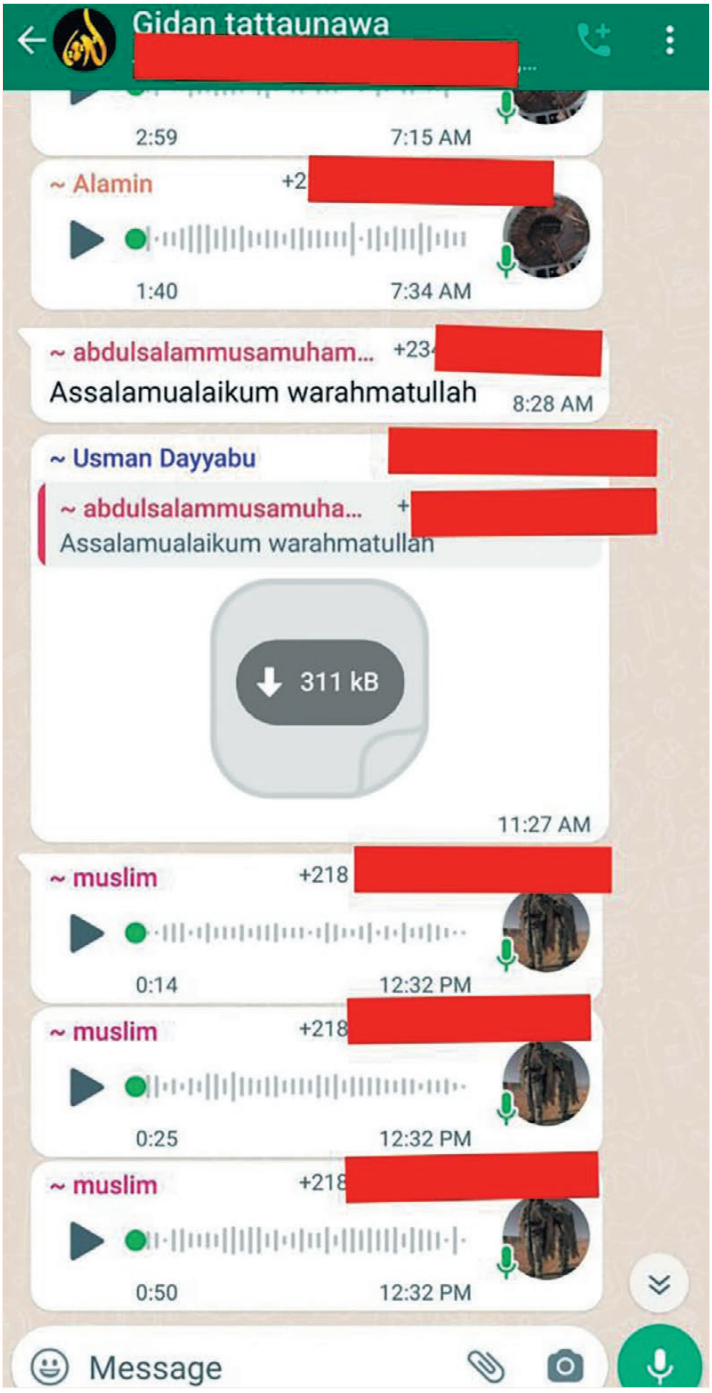

Fig 1. A screenshot of a WhatsApp group the Jihadists created for question-and-answer sessions. Taken in Jan. 2023.
Source: Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

Fig 2. A screenshot of an Ansaru propaganda video that has remained on Facebook since June 2022. Screenshot date: Feb. 14, 2023
Source: Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

Fig 3. A screenshot of an account announcing the creation of a Telegram channel where Ansaru share violent content.
Source: Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

Fig 4. Screenshot of a Facebook account saying they have taken up arms to fight “this infidel government” of Nigeria.
Source: Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

Before attacks

In the pre-attack environment, Boko Haram uses social media to promote propaganda and propagate threats of incoming attacks. For instance, in a video released on YouTube, one of Boko Haram’s leaders claimed, “I advise you to desist from following your constitution and democracy, which is unIslamic.” The man continues, reading from a script, “The only language of peace is to repent and follow Allah, but if you do not, then we will communicate it to you through the language of violence.”[71] The pre-attack environment usually informs the local population, the military and the government of threat messages. In a similar threat released via YouTube by Boko Haram, Shuibu Moni, a Boko Haram commander, threatened to attack some states. The video displays Boko Haram’s firing power in Sambisa Forest.[72]

ISWAP’s foot soldiers are known to use WhatsApp for quick communications before and while carrying out attacks.[73] ISWAP also posts videos on Telegram to convey messages to its followers.[74] The first step is to share the raw footage and pictures with IS, which then produces the propaganda material.[75] It is significant that these groups, especially ISWAP, have relied on video messaging through closed and members-only Telegram channels to convey their planned attacks and in the aftermath, including claiming responsibility for such attacks. This was the case with both the Kuje prison break in Abuja, Nigeria,[76] and the foiled prison break in Kontagora, Niger state, Nigeria.[77]

Prior to staging attacks, information is shared in coded languages on Telegram channels. After an attack, ISWAP returns to the channels to inform members what the coded messages meant. For instance, after claiming responsibility, ISWAP informed its members to be patient after the Kuje prison break, assuring them that all those in captivity would

71 Reuters, “Boko Haram threatens Cameroon with violence in video,” 7 January 2015.
72 Daily Post, “Released Boko Haram member threatens more attacks in Nigeria,” 7 March 2018.
73 Sahara Reporters, “Report Reveals How Boko Haram, ISWAP Use Facebook, WhatsApp, Telegram to Recruit, Spread Propaganda In Nigeria,” 19 September 2022.
74 Samuel, “ISWAP’s use of tech could prolong Lake Chad Basin violence”.
75 ibid.
76 N. Ayitogo “ISWAP claims responsibility for Abuja prison attack.” 2023, available at: https://www.premiumtimesng.com/news/headlines/541340-just-in-iswap-claims-responsibility-for-abuja-prison-attack.html?tztc=1.
77 Daily Post, “Minna prison break: 180 inmates escaped, 30 recaptured,” 4 June 2018.

be released eventually.[78] This was announced through a video on Telegram. Shortly afterwards, there was a foiled attempt at a maximum military prison in Kontagora, Niger state.[79] In the case of the Kuje attack, ISWAP also filmed videos during the attack, shared on its Telegram channel.[80] Just before the 2023 general elections, via a released video on Telegram, ISWAP warned that it would stage attacks to prevent the elections from proceeding.[81] However, the elections in the northeast were generally peaceful. ISWAP had dispatched fighters specifically for the purpose of disruption, but there was only an isolated case of the abduction of people in Goza, Borno state in northeast Nigeria.[82]

Ansaru has multiple social media accounts, including Facebook, and messaging apps such as Telegram and WhatsApp. However, Ansaru’s social media usage reveals it is less advanced in evading social media monitoring when compared to the other groups.[83]

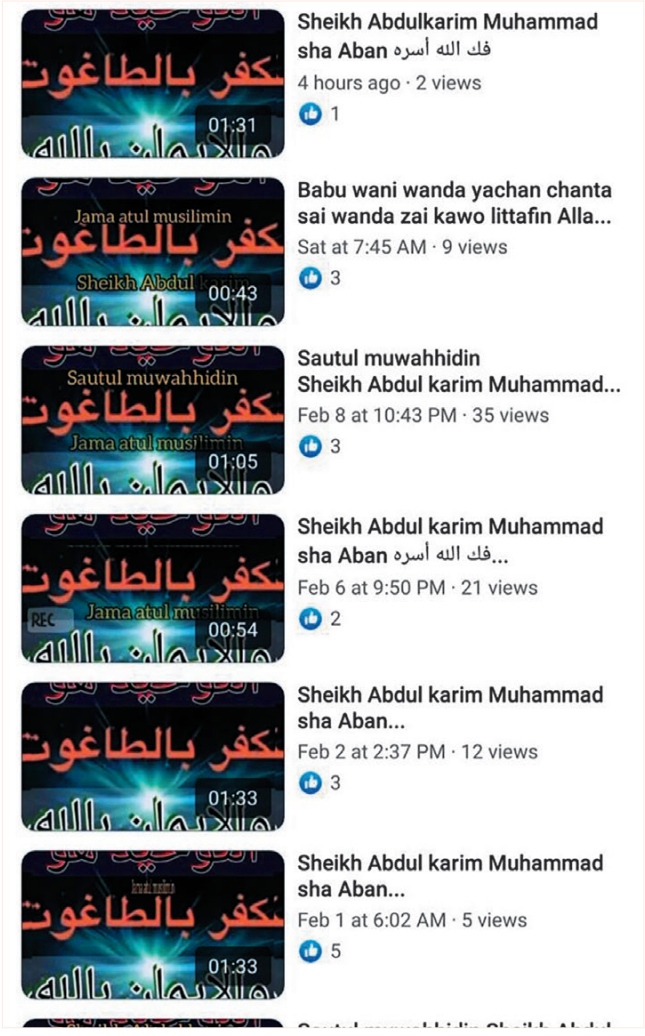

Fig 5. A screenshot showing some parts of a series of videos uploaded by an Ansaru media wing on Facebook
Source: Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

78 The Cable, “ISWAP ‘claims responsibility’ for Kuje prison attack,” 6 July 2022.
79 See Daily Post, “Minna prison break”.
80 Foundation for Investigative Journalism, “In New Video, ISWAP Claims Responsibility for Kuje Prison Attack,” July 2022.
81 Business Hallmark, “2023: ISWAP plots to derail elections,” 8 August 2022.
82 Reuters, “Suspected Boko Haram militants kidnap at least 10 people in northeast Nigeria,” 5 September 2018.
83 Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

After attacks

Boko Haram has disseminated footage of successful attacks to demonstrate its military capacity. Boko Haram also conveys messages prior to and after attacks through written terror threats. These messages are asynchronous digital communications that can be stored or archived. This allows for a re-enactment, re-invigoration and fresh perception of the illocutionary force of these threats when retrieved.[84] Emerging evidence also shows that VEOs in Nigeria use drones for propaganda, surveillance and communication.[85] For example, in April 2014, after the attack and kidnapping of 276 schoolgirls in northern Nigeria, Boko Haram posted drone footage of the attack on social media.[86]

The invasion of Kuje prison in Nigeria’s capital, Abuja, on 5 July 2022 by ISWAP resulted in a successful jailbreak. It is estimated that 879 detainees escaped, including 68 Boko Haram detainees. The attack and subsequent dissemination of propaganda demonstrated the weakness of Nigerian security forces.[87] Despite intelligence reports before the attack, the success of the operation underscores ISWAP’s operational capacity. The instrumentalisation of the internet to coordinate attacks by Boko Haram, ISWAP, Ansaru has been considered one of the most critical threats to national security.

Fig 6. Screenshot from an ISWAP member showing armed fighters in a propaganda message using Hausa language on Facebook.
Source: Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

84 Innocent Chiluwa, “The discourse of terror threats: Assessing online written threats by Nigerian terrorist groups,” *Studies in Conflict & Terrorism* 40, no. 4 (2017): 318–38.
85 See Samuel, “ISWAP’s use of tech”.
86 Cox et al., “Social media in Africa presents a double-edged sword for security and development,” RAND Corporation, 5 November 2018.
87 See Samuel, “ISWAP’s use of tech”.

Challenges to VEOs’ use of Online Platforms

Achieving a sustainable and prolonged presence on online platforms remains a monumental challenge for Nigerian VEOs. The constant removal and monitoring of their activities by social media providers and the government to censor disinformation have made it difficult to sustain their digital presence. ISWAP’s Telegram channels have also been infiltrated by Nigeria’s intelligence agencies several times, prompting ISWAP to change its Telegram channels regularly.[88]

88 Karen Allen, “Terrorists’ use of tech in West Africa must be contained,” ISS, 15 September 2022.

6 Conclusion

The internet plays a significant role in the pre- and post-attack online behaviour of Nigerian VEOs. Exploiting and manipulating the internet to promote jihadist doctrines has several implications.[89] Some of the themes and catchphrases often employed on the internet by Boko Haram, ISWAP, and Ansaru include:

- Boko Haram is rich and wealthy.
- Boko Haram is a professional military outfit.
- Boko Haram is honest, sincere and truthful.
- Boko Haram’s leader, Abubakar Shekau, is invincible and unpredictable.
- The Nigerian government is weak and feeble. Nigerian soldiers are cowardly and bumbling incompetents.
- Boko Haram is strong and powerful.[90]
- Ansaru is trustworthy, truthful, and sincere.
- Ansaru is powerful, strong, and ready to defend Muslims.[91]

These catchphrases are constructed to promote a forceful image of the organisation. As such, this propaganda risks influencing vulnerable citizens unaware of the state’s military capacity to suppress the insurgent groups’ activities.

This report has examined the usage of online electronic platforms by violent extremists in Nigeria in pre-attack and post-attack environments. It found that violent extremists in Nigeria employ popular social media platforms, including Facebook, Twitter, YouTube, WhatsApp and Telegram, to communicate and disseminate information to the public. These digital platforms have been instrumental to the insurgents’ success. However, achieving a sustainable and more prolonged presence on these platforms remains a challenge for the groups. The constant takedown and monitoring of their activities by social media platforms and the government capacity to censor disinformation have made it difficult to sustain their online presence. Preventing online terrorism requires concerted efforts that involve multifaceted strategies for combating violent extremism in Nigeria. We found that Boko Haram’s, ISWAP’s and Ansaru’s online strategies in the pre- and post-attack environments have been mechanised as a tool for propaganda, awareness creation for incoming attacks and display of powers after the attacks.

89 Branislav Todorovic and Darko Trifunovic, *Prevention of (Ab-) Use of the Internet for Terrorist Plotting and Related Purposes*, International Centre for Counter-Terrorism (ICCT), 2020.
90 See Wolumati and Agbese, “Terrorists and social media messages”.
91 Aliyu, Dahiru, Terrorists Using Local Language To Spread Propaganda On Facebook, HumAngle, April 17, 2023

Drawing on these findings, we make the following recommendations:

a. *Redefining Existing Counterterrorism Strategies:* There is a need to redefine current counterterrorism strategies. While state and transnational counterterrorism approaches against Boko Haram have focused on kinetic and non-kinetic responses, evidence shows limited digital counterterrorism measures against Boko Haram and related terrorist groups in Nigeria and the Lake Chad region. Given this deficiency, it becomes imperative that online counterterrorism strategies complement existing physical and social counterterrorism measures.

b. *Social Media Regulation:* While social media regulation could impact access to information and pose human rights violations by the state, there is a need for increased content moderation within the Lake Chad region. Such an effort requires regional coordination between Nigeria, Cameroon, Niger and Chad.

c. *Strengthening Cybersecurity Infrastructure:* Effective cybersecurity infrastructure can remove terrorist-related content. Achieving such infrastructure requires a state-led mobilisation of cyber-security experts capable of building resilience and deploying a formidable cyber-security infrastructure.

d. *Collaborating with Indigenous and Non-Indigenous Tech Companies:* The Nigerian government should consider partnering with local and foreign digital technology companies to build algorithms that detect and prevent extremist content. Platforms can therefore monitor extremist information flows and online propaganda.

Policy Section

This policy section has been authored by Dr Nicola Mathieson, Research Director, at the Global Network for Extremism and Technology (GNET) at the International Centre for the Study of Radicalisation (ICSR) at King’s College London. This section provides policy recommendations and is produced independently from the authors of this report. Recommendations do not necessarily represent the views of the authors.

This report provides an in-depth analysis of the online behaviour of the three dominant VEOs operating in Nigeria: Boko Haram, ISWAP and Ansaru. The authors confirm that, as is the case for other extremist groups, deplatforming by major social media platforms has led to the migration by the groups to smaller, more encrypted spaces. The variation in platform migration by the three groups operating under similar conditions highlights how important it is for technology companies and governments to tailor their policies to the specific behaviours of groups.

The key findings of this report carry corresponding policy implications for technology companies and policymakers. This policy section ensures that GNET reports provide actionable research outcomes that can inform and support technology companies and policymakers to identify and prevent extremist and terrorist exploitation of digital platforms. The policy section fulfils GIFCT’s core pillar of learning to improve prevention and responses to terrorist and violent extremist attacks.

1. Technology Companies

This report has identified three core areas for action by tech companies:

- While the groups under investigation did publish material in English, the dominant language used by Boko Haram, ISWAP and Ansaru on social media channels was Hausa. Tech companies need to ensure that they have the relevant linguistic expertise to manage specific national and regional threats.

- Despite the widescale deplatforming of VEOs in Nigeria, groups were able to migrate to platforms less able or less willing to remove these actors and the content they shared. In addition to removing VEOs from their platforms, social media platforms should also coordinate with other platforms to prevent successful migration. Larger tech firms should also provide support for smaller tech platforms to help them to combat terrorist and violent extremist content (TVEC) on their platforms.

- Tech companies should coordinate with states to monitor the online activities of VEOs. As highlighted in this report, there were coded messages shared by VEOs prior to attacks. These coded

messages, confirmed and explained by post-attack content, should be analysed and extracted to improve detection algorithms and improve flagging of potential violence.

2. Policymakers

In addition to the report findings and their implications for technology companies, this report has also identified three core areas for action by policymakers:

- Previous GNET reports have highlighted the regional variation in VEOs’ social media use.[92] This report identified within-country variation of platforms between VEOs. Boko Haram, ISWAP and Ansaru all responded to deplatforming from major platforms in distinct ways. While all three migrated to different platforms, the variation in destination platforms demonstrates the importance of tailored preventing and countering violent extremism (P/CVE) strategies to the hyper-local contexts in which groups operate.

- This report highlights the challenge of balancing content moderation with human rights concerns. When developing P/CVE policy, states need to ensure that fundamental human rights are protected while also removing TVEC online.

- As demonstrated in previous GNET reports, deplatforming from major platforms has led to extremist and terrorist actors moving to smaller and less regulated tech platforms.[93] All digital platforms have a responsibility to identify and remove TVEC from their platforms. As we enter a period in which there is greater support for tech companies undertaking this work, it is clearer which platforms fail to remove TVEC due to financial and technical restrictions and which are simply unwilling to do so. Policymakers should consider how they can develop strategies to apply greater pressure on those tech companies that refuse to tackle terrorist content on their platforms.

92 Suraj Ganesan and Mohammed Sinan, “Islamic State Online: A Look at the Group’s South Asian Presence on Alternate Platforms” (London: Global Network on Extremism and Technology (GNET), February 2023), https://doi.org/10.18742/pub01-114.

93 Bennett Clifford, “Migration Moments: Extremist Adoption of Text-Based Instant Messaging Applications” (London: Global Network on Extremism and Technology (GNET), November 2020), https://gnet-research.org/2020/11/09/migration-moments-extremist-adoption-of-text-based-instant-messaging-applications/; Ganesan and Sinan, “Islamic State Online.”

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.