



Contextual Resources: At the Intersection of Terrorism and Technology in West Africa

March 2025

The following is a collection of Insights that explore the threat of technology-assisted and technology-enabled terrorism and violent extremism in the West African region produced by the [Global Network on Extremism and Technology \(GNET\)](#). GNET is the academic research arm of the [Global Internet Forum to Counter Terrorism \(GIFCT\)](#). GNET's mission is to publish actionable research to better understand and prevent terrorist and violent extremist exploitation of digital platforms. GNET is convened by the International Centre for the Study of Radicalisation (ICSR) based within the Department of War Studies at King's College London.

Trends in Terrorist and Violent Extremist Tech Exploitation

[The "Webification" of Jihadism: Trends in the Use of Online Platforms, Before and After Attacks by Violent Extremists in Nigeri](#)

Folahanmi Aina and John Sunday Ojo - July 2023

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.

[Digital Dunes and Shrublands: A Comparative Introduction to the Sahelian Jihadi Propaganda Ecosystem](#)

Héni Nsaibia and Rida Lyammouri - October 2020

This Insight provides an investigation into the Sahelian propaganda landscape, which has unique features and characteristics, and the ecosystem of the two main jihadi groups, JNIM and ISGS, which share common roots within the network of Al-Qaeda in the Islamic Maghreb (AQIM). A historical overview provides context that helps explain the differing media capabilities of the two entities.

Content Moderation & Evasion

[Exploit and Evade to Remain and Expand: The Cross-Platform Evasion Toolbox of Islamic State Supporters](#)

Moustafa Ayad - December 2023

This Insight provides a historical overview of Islamic State supporters' platform exploitation and evasion tactics and highlights gaps in platform moderation and current research into Islamic State ecosystems on platforms such as TikTok, Facebook, X [formerly known as Twitter], and Telegram. It focuses on what has been termed the Islamic State supporters' 'exploitation and evasion toolbox' and five new tactics that continue to confound platform moderation.



[Jihadi Media and Online Secrecy as Doctrinal Values](#)

El Mostafa Rezrazi - October 2020

This Insight outlines two key factors through which terrorist groups have shown resistance and regeneration capacities. These include the methods used to optimise their communication strategy, and to convert media activity into a doctrine.

[Hiding in Plain Site: Islamic State's 'Muslim News'](#)

Moustafa Ayad - February 2020

This Insight explores the use of the '.ml' domain by Salafi-jihadist supporters to host Islamic State-affiliated websites on the dark web in 2016, hosting a downloadable archive of IS content.

Exploitation of Financial Platforms

[Combating the Islamic State Finance: Somalia and the Pan-African Nexus](#)

Adam Rousselle - February 2025

This Insight examines the financial evolution of the Islamic State's African operations, its sources of revenue, and how the tech industry can address this growing threat. This Insight is part one of a three-part series.

[Combating Islamic State Finance: West Africa and the Sahel](#)

Adam Rousselle - February 2025

This Insight examines the office of al-Furqan, one of the Islamic State's most successful regional financial offices. It will examine the organisation's financial role in broader IS operations and the potential threat this confluence of interests could pose moving forward. This Insight is part two of a three-part series.

[Combating Islamic State Finance: Central Asia and Around the World](#)

Adam Rousselle - February 2025

This Insight explores the Islamic State's Maktab al-Siddiq financial office, which is based in Afghanistan. It analyses the global financial infrastructure IS uses to finance some of the world's deadliest terrorist attacks. This Insight is part three of a three-part series.

[From Trees to Terror: JNIM's Use of Online Rosewood Sales to Fuel Expansion](#)

Adam Rousselle - November 2024

JNIM's threat to Mali and the Sahel region stems from its direct and indirect leveraging of digital technologies, including an extensive online propaganda campaign and potential partnering with Chinese criminal groups to sell smuggled Malian rosewood indirectly. This Insight examines JNIM's online media presence and its use of illicit rosewood marketing online, which may contribute to funding its regional operations.



Exploitation of Hard Tech

Dark Signals: The Growing Threat of Satellite Internet in Extremist Networks

Gaetano Siculo - December 2024

This Insight examines the increasing adoption of satellite internet across the African continent, its potential to bridge the digital divide in Least Developed Countries (LDCs), and the role it may play in advancing or combating extremist activities.

Eyes in the Sky: The Innovation Dilemma of Drone Proliferation among Violent Non-State Actors in the Sahel

Francis Okpaleke - April 2024

This Insight delves into the innovation dilemma posed by the unchecked proliferation of drones among VNSAs in the Sahel, examining the factors behind this proliferation, how VNSAs are incorporating drones into their operations, and the resulting security implications for the region.

Opportunities for Intervention

Leveraging AI-Driven Tools for Capacity Building in Crisis Response: Enhancing Moderation and Crisis Management on Smaller Digital Platforms in Africa

Abraham Ename Minko - January 2025

This Insight investigates how AI can be leveraged to effectively empower small platforms in the Horn of Africa to counter extremist activities. By focusing on localised solutions and capacity-building initiatives, this Insight proposes a sustainable framework to enhance online safety and mitigate the misuse of digital platforms for malign purposes.

The Role and Potential of Artificial Intelligence in Extremist Fuelled Election Misinformation in Africa

Jake Okechukwu Effoduh - March 2024

In Africa, where political landscapes are often marked by instability and ethno-tribal/religious divisions, the potential for AI to be exploited by extremist groups to cause political stability poses a significant risk. These actors can harness AI to deepen societal cleavages, manipulate public opinion, and ultimately undermine the democratic fabric through disenfranchisement and misinformation. This Insight provides both legal and technical approaches to preventing this form of exploitation.

Harnessing Peacotech for Socio-Political Resilience in Benin

Jaynisha Patel - January 2024

This Insight argues that by embracing peacotech and crafting digital solutions, especially attuned to Benin's Muslim communities, the nation can forge a more resilient society less susceptible to extremist radicalisation. This approach is aligned with the prevailing optimism for democracy among Beninese Muslims and would help deliver on their preference for democratic governance.

Can 'Cyberterrorism' Really Exist in Africa?

Alta Grobbelaar - March 2023

This Insight aims to provide an overview of the use of ICT in Africa, specifically looking at how easily the term 'cyber' is used or misused in the African context. This Insight also gives way to a critical

discussion on how best to understand and eventually combat the potential threat of cyberterrorism. When considering the already contested term 'terrorism', adding another contested prefix – 'cyber' – makes the challenge of defining, analysing and conceptualisation more profound.

Further Information

For additional information about GNET, please see below:

Contact GNET: mail@gnet-research.org

Write for GNET: <https://gnet-research.org/write-for-us/>

To sign up for GNET's mailing list, scan the QR code

