

Information Manipulation in Sudan

A Baseline Assessment of
actors, narratives and tactics

Executive Summary



This assessment was conducted by the Thomson Foundation as part of the FCDO-funded Sudan Digital Resilience Project.



The Thomson Foundation wishes to acknowledge **Andariya** for their contributions and commitments to this assessment. The Thomson Foundation would also like to extend its gratitude to all the organisations, journalists and individuals who participated in the research and whose invaluable input contributed to a better understanding of the Sudanese information landscape.

The material in this report discusses sensitive and potentially distressing themes, including accounts of violence against civilians, human rights violations, and sexual and gender-based violence in the context of the conflict in Sudan. Reader discretion is advised.

Thomson Foundation Lead Researcher:
Dr. Aida Al-Kaisy (Consultant)

Thomson Foundation Qualitative Researcher:
Dr. Amal Hamdan (Consultant)

Thomson Foundation Support Team:
Meriem Bahri
(Middle East & Africa Programme Manager)
Talal Salih (Sudan Project Manager)
Gary Mundy
(Director of Research, Policy and Impact)

For more information, please visit: www.thomsonfoundation.org



Executive Summary

Since April 2023, the war in Sudan has systematically destroyed not only the country's physical infrastructure but also its information ecosystem.

The following report examines how sophisticated disinformation and information manipulation campaigns have become central to the conflict, operating as organised precursors to and signs of imminent physical violence whilst perpetuating conflict, destroying social cohesion, and endangering humanitarian operations.

Through comprehensive analysis employing the ABCDE and DISARM frameworks, which combined key informant interviews and social media listening across digital platforms between September and October 2025, this baseline study presents a context where testing highly sophisticated hybrid and digital warfare methodologies has implications extending far beyond Sudan and its borders.





Sophisticated actor networks deploy distinct but equally dangerous strategies

The RSF has built a technically sophisticated disinformation apparatus, using high quality multimedia content, AI-enhanced imagery, professional public relations consultants, with foreign backing which dates back before the conflict began. RSF operations feature individual influencers and anonymous amplification accounts, with slick video production optimised for algorithm engagement across TikTok, Facebook, X, and YouTube. Their narratives centre on marginalisation of peripheral regions, anti-elite rhetoric, and psychological intimidation including explicit gendered violence threats. SAF compensates for its less technical sophistication through volume, institutional authority, diaspora mobilisation, and emotional intensity. SAF-aligned content emphasises narratives of nationalism, dignity, religious legitimacy, and the systematic denial of responsibility for civilian harm whilst amplifying RSF atrocities. Both actors are supported by coordinated inauthentic behaviour networks, influencers commanding thousands of followers, and geopolitical actors including UAE, Egypt, Russia, and Israel.



Platform-specific tactics exploit algorithmic vulnerabilities across the digital ecosystem

Between 1 September and 31 October 2025, 6,348 posts classified as information manipulation reached 890,225,854 users and generated 45,870 engagements. Facebook serves as the primary amplification platform with recommendation systems privileging divisive content. X yields disproportionate influence over political discourse through hashtag activism and coordinated campaigns. TikTok has emerged as a critical platform for video-based disinformation, with entertainment-news hybrid formats particularly potent amongst younger audiences.

YouTube functions as a content reservoir where extended videos are extracted into manipulative short-form clips redistributed across platforms. WhatsApp's encrypted group architecture and Telegram's semi-private channels enable rapid circulation of unverified content beyond external scrutiny. The monitoring revealed extensive use of AI-generated content, recycled footage from other conflicts, graphic imagery broadcast in real time, and narrative laundering where disinformation originates on one platform before being amplified across others to create the illusion of credibility.

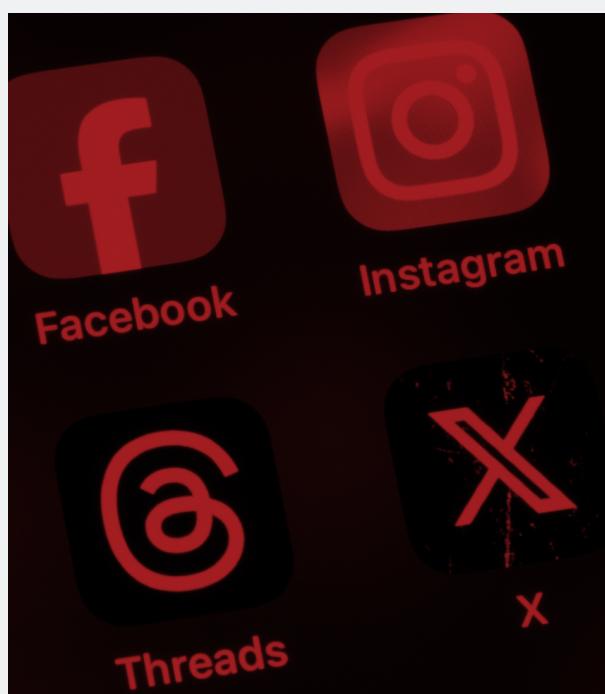


The information war directly undermines humanitarian response, targets journalists, and perpetuates conflict

Disinformation severely hinders humanitarian operations, with aid workers and Emergency Response Rooms systematically accused of being 'collaborators' or 'spies', leading to arrests, targeted attacks, and operational paralysis.

False accusations force organisations to divert resources from assistance to reputation management. Journalists face systematic targeting from both warring parties, accused of collaboration and subjected to arrest, harassment, detention, and killing. The collapse of Sudan's media infrastructure has created an information vacuum filled by propaganda rather than professional journalism.

Any individual or group calling for peace is systematically attacked and isolated, transforming peace advocacy into a social crime. The primary goal extends beyond military advantage to the deliberate fragmentation of civil society, destruction of social cohesion, and perpetuation of a conflict serving the political and economic interests of armed actors whilst devastating civilian populations.



Foreign interference shapes narratives through coordinated regional and international networks

Geopolitical actors play critical roles in Sudan's disinformation ecosystem. The UAE is strongly implicated as a major foreign actor supporting RSF through bot operations, professional communications infrastructure, and narrative laundering via Emirati platforms and influencers. Russia is involved in influence operations through Wagner Group links and corporate interests in Sudan's gold resources.

Israeli channels participate in campaigns alongside Emirati accounts, whilst Egyptian and Yemeni influencers amplify SAF-aligned narratives. Regional media platforms including Egyptian YouTube channels and UAE-based outlets function as high-reach amplification nodes for faction-aligned narratives packaged as journalism.

International platforms inadvertently launder disinformation when reputable figures without verification capacity reshare manipulated content, whilst coordinated networks operate from diverse geographies, demonstrating the globalised architecture of Sudan's information war.



Disinformation operates as a systematic precursor to mass atrocities

The repetitive pattern which links online information manipulation to offline violence is frighteningly consistent. Hate speech campaigns systematically precede military operations, working to justify future atrocities and mobilise support.

In Al-Halfa, a week-long hate speech campaign preceded the RSF's entry, immediately followed by the public execution of over 45 civilians.

In El Geneina, disinformation targeting the Masalit community directly preceded massacres resulting in over 2,000 confirmed deaths. Before violations in Al-Jazira, local populations were systematically labelled as 'collaborators' in media rhetoric.

This deliberate use of dehumanising language mirroring genocidal rhetoric on social media represents organised hybrid warfare where information manipulation functions as a weapon which is causing tangible, deadly consequences.

The report makes the following recommendations:

1. For Journalists and Media Workers

Implement comprehensive safety and verification protocols whilst resisting factional pressures and build inclusive cross-platform professional networks and collaborations that bridge geographic and ethnic divides, including journalists in exile, with equitable resource-sharing mechanisms.

2. For Technology Platforms

Designate Sudan as a crisis zone requiring enhanced Arabic-language moderation, rapid removal of coordinated inauthentic accounts, and algorithmic adjustments to reduce amplification of dehumanising content whilst prioritising verified humanitarian sources.

3. For Policymakers and Governments

Integrate information environment protection into humanitarian frameworks and early warning systems, make cessation of hate speech campaigns an explicit ceasefire condition, and provide sustained funding for independent professional Sudanese media and journalists and information literacy programmes.

4. For International NGOs and Civil Society Organisations

Develop comprehensive staff protection strategies against disinformation targeting, establish verification protocols for emergency responses, and recognise media as essential humanitarian infrastructure requiring dedicated funding and advocacy support.