



City Research Online

City St George's, University of London

Citation: Tasiu Abubakar, A. (2026). Cyber and Information Campaigns in Africa. In: Sambaluk, N. M. (Ed.), De Gruyter Handbook of Cyber Conflict and Warfare. (pp. 327-341). Berlin, Germany: De Gruyter Brill. ISBN 9783111612577 doi: 10.1515/9783111613031-022

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: <https://openaccess.city.ac.uk/id/eprint/38312/>

<https://doi.org/10.1515/9783111613031-022>

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to [City Research Online policy](#).

Cyber and Information Campaigns in Africa

Abdullahi Tasiu Abubakar

Abstract

The centrality of information in statecraft and geopolitical and ideological competitions makes information warfare a preoccupation of several state and non-state actors. Advances in communications technologies enhance its universality and prominence in cyberspace. Africa is experiencing this in many ways, with the relentless targeting of its populations on multiple fronts by various actors. This chapter examines the nature and impact of cyber-enabled information campaigns in Africa. It looks at the factors that fuel the rapid rise of the phenomenon, the forces driving it, and the directions it takes. Document analysis and media investigations show that foreign powers such as Russia and the People's Republic of China (PRC), domestic governments and violent extremist groups are the key sponsors of the campaigns while Western social media platforms are among the main tools of perpetrating them. Drawing on Philip Taylor's "munitions of the mind" model as conceptual framework and analyzing documents, social media and online content, the study highlights the patterns and consequences of cyber-enabled information operations in Africa.

Keywords: *Cyberspace, digital disinformation, foreign powers, influence operations, propaganda, social media, TikTok terrorists*

Introduction

The Nigerian government was stunned in August 2024 when anti-government protests partly turned into pro-Russian rallies, with protesters waving Russian flags and calling for the overthrow of the "pro-Western" regime of President Bola Tinubu. Security forces arrested and charged 76 of them, including 30 minors, with treason¹ – an offense that carries the death penalty in Africa's most populous nation. Media reports say the protests followed economic hardships caused by government policies and that those caught waving Russian flags were merely victims of the Kremlin's influence operations largely run via TikTok and Telegram channels.² This came at the time when violent extremist groups in the country had just renewed their own cyber-enabled information campaigns. And it was barely a year after Nigeria had held divisive elections characterized by influence operations engaged by politicians and social media influencers.³ The latter happened despite the scandal surrounding the involvement of a

¹ Camillus Eboh, "Nigeria charges 76, including minors, with treason after August protests," *Reuters*, November 1, 2024, <https://www.reuters.com/world/africa/nigeria-charges-76-including-minors-with-treason-after-august-protests-2024-11-01/> (accessed 2 October 2025).

² Silas Jonathan, "How Telegram, TikTok aided Russian disinformation that led to the incarceration of Nigerian minors," *Premium Times*, November 14, 2024, <https://www.premiumtimesng.com/news/headlines/754117-how-telegram-tiktok-aided-russian-disinformation-that-led-to-incarceration-of-nigerian-minors.html> (accessed 2 October 2025).

³ Temple Uwalaka, Fred Amadi and Stella Enyindah, "Social media influencers and political influence operations: The Data Boys example in Nigeria," *Public Relations Inquiry*, 14/1 (2025), 89-115.

British firm, Cambridge Analytica, in information manipulation in previous Nigerian elections.⁴

The diversity of those few examples illustrates the widening scope of influence operations in Nigeria. And the country is just one of several African nations where cyber-enabled information campaigns are expanding rapidly. Most of the 54 recognized sovereign states in the continent have experienced the phenomenon.⁵ From Cairo to Cape Town, from Bamako to Bangui, from Abidjan to Addis Ababa, and from Nairobi through N'Djamena to Niamey, foreign powers, domestic governments and politicians, and terror groups are increasingly engaged in cyber and information campaigns targeting Africans from multiple fronts. Advances in communications technologies and expansion of digital communications in Africa have enhanced the continent's presence in cyberspace but also turned it into a fertile ground for cyber-enabled operations. "The Internet, along with social media, makes it much easier to propagate false information at a greater speed and scale."⁶ Africans are among the most avid users of social media in the world and are increasingly relying on them for news consumption, making them easier targets.⁷ "Social media users in Nigeria and Kenya are near the top of the globe in the number of hours per day spent on social platforms. They are simultaneously the countries that report the most concern about false and misleading information."⁸ Across the world, improvement in internet connectivity and social media use has made influence operations easier, faster, wider and cheaper.⁹ "Cyberspace has enabled unprecedented access to domestic populations worldwide, which can be targeted through the topmost layer of the environment."¹⁰ This has become more pronounced in Africa, but scholarship has not paid adequate attention to it.

This study attempts to fill the gap by examining the nature and consequences of cyber-enabled influence campaigns in the continent. It addresses the following research question: What are the dominant patterns, actors, and effects of cyber-enabled information operations in Africa? Drawing on Philip Taylor's "munitions of the mind" model as conceptual framework, the study analyzes the dimensions and dynamics of the operations and the motivations of their sponsors. Analysis of documents and media investigations show that foreign powers – especially Russia and the People's Republic of China (PRC) – domestic governments and extremist groups are the main sponsors of the campaigns, and Western social media platforms serve as the key tools of the operations.

Manipulation of the Minds

In his seminal work *Munitions of the Mind*, Philip Taylor conceptualizes propaganda as a key component of power relations and dissects it in its various forms, trajectories and

⁴ Samantha Bradshaw and Philip Howard, *Challenging Truth and Trust: A Global Inventory of Organised Social Media Manipulation* (Oxford: 2018).

⁵ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa* (Washington, DC, 2024), <https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/> (accessed 2 October 2025).

⁶ Jelena Vičić and Erik Gartzke, "Cyber-enabled influence operations as a 'center of gravity' in cyberconflict: The example of Russian foreign interference in the 2016 US federal election." *Journal of Peace Research*, 61/1 (2024), 10-27, p. 12.

⁷ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*.

⁸ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 2.

⁹ Herbert Lin and Jaelyn Kerr, "On cyber-enabled information warfare and information operations," in Paul Cornish (ed.) *The Oxford Handbook of Cyber Security* (Oxford: 2021), pp. 251-272.

¹⁰ Jelena Vičić and Richard Harknett, "Identification-imitation-amplification: Understanding divisive influence campaigns through cyberspace," *Intelligence and National Security*, 39/5 (2024), 897-914, p. 900.

ramifications.¹¹ He traces its long history from ancient time to contemporary period, detailing the changes it has undergone and the main intent that remains constant: influencing the recipient's mind. He defines propaganda as "the *deliberate* attempt to persuade people to think and behave *in a desired way*."¹² There exists accidental, unplanned and unconscious propaganda, he argues, but the focus is on "the conscious, methodical and planned decisions to employ techniques of persuasion designed to achieve specific goals that are *intended to benefit those organizing the process*."¹³ Taylor's work precedes the latest wave of cyber-enabled information operations around the world but it captures their essential elements and intents. His concept of "munitions of the mind" could provide proper grounding to the concept of "hacking human mind" put forward by Vičić and Erik to explain the use of cyber capabilities to influence "human minds."¹⁴ They are all focused on what we can describe as "manipulation of the minds." And although "cyber operations only became a common tool of statecraft in the twenty-first century," Lilli has noted that "states have been using cyberspace against each other at least since the late 1960s"¹⁵ – a period adequately covered by Taylor's research. Regardless of the time and tools deployed for propaganda, the intention has always been to influence recipients' minds. The "'munitions of the mind' may have become ever more sophisticated in their application and methods of dissemination but they have always had one thing in common: they are directed at human beings."¹⁶ So, information campaigns in cyberspace reflect the advances Taylor has envisaged.

For clarity, cyber-enabled information operations are defined here as organized communication activities by state or non-state actors, using manipulative behavior with cyber tools, "to achieve a specific effect among a target audience."¹⁷ The interdisciplinary nature of the subject causes terminological confusions that make many scholars to use the term "influence operations" interchangeably with the terms "information operations," "propaganda" and "information warfare."¹⁸ In this chapter, "information operations" is used interchangeably with "information campaigns" and "influence operations." The centrality of information in it reinforces Taylor's argument that those who control the flow of information wield power over the recipients. "Propaganda is thus a powerful tool for perpetuating power relationships,"¹⁹ but the recipients also have the power to "reject the messages – provided they can be detected."²⁰ An ability to deliver messages that cannot be detected as propaganda is often seen as a viable way of enhancing the efficacy of information operations. "While many influence operations may contain falsehoods," Vičić and Gartzke argue, those that "rely on information that is factually correct are arguably far more effective."²¹ This perhaps explains why influence campaigners are now increasingly using factual information, in manipulative way, to execute their work.²²

¹¹ Philip Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day* (3rd edition) (Manchester, 2003).

¹² Taylor, *Munitions of the Mind* (italics original), p. 6.

¹³ Taylor, *Munitions of the Mind*, p. 6.

¹⁴ Vičić and Gartzke, "Cyber-enabled influence operations," pp. 11-23.

¹⁵ Eugenio Lilli, "How can we know what we think we know about cyber operations?" *Journal of Global Security Studies*, 8/2 (2023), 1-18, p. 6.

¹⁶ Philip Taylor, "'Munitions of the mind': A brief history of military psychological operations," *Place Branding and Public Diplomacy*, 3/3 (2007), 196-204, p. 196.

¹⁷ Jonathan Morley-Davies, Jem Thomas and Graham Baines, *Russian Information Operations Outside of the Western Information Environment* (Riga: NATO Strategic Communications Centre of Excellence: 2024), p. 18.

¹⁸ Vičić and Harknett, "Identification-imitation-amplification," p. 898.

¹⁹ Taylor, *Munitions of the Mind*, p. 9.

²⁰ Taylor, *Munitions of the mind*, p. 9.

²¹ Vičić and Gartzke, "Cyber-enabled influence operations," p. 13.

²² Vičić and Gartzke, "Cyber-enabled influence operations".

Despite this, however, disinformation campaigns remain an integral part of information operations in Africa, as seen in various cases described below.

Foreign Powers Campaigns

Analysis of information campaigns conducted on the continent by various actors, along with a review of relevant literature, reveals that selective dissemination of correct information, disinformation, misinformation, and mal-information were all used in these operations. Disinformation (deliberate dissemination of erroneous information to influence people to achieve specific ends) and mal-information (selective use of correct information to inflict harm) have always been part of propaganda techniques—and so is misinformation (accidental or unwitting dissemination of falsehoods). But they are sometimes skillfully mixed with dissemination of accurate information in executing cyber-enabled influence operations in Africa. Research by the Africa Center for Strategic Studies shows that every region of the continent has been targeted for disinformation campaigns, with at least 39 countries affected, half of them targeted repeatedly. “African countries experiencing conflict are subject to much greater levels of disinformation – facing a median of 5 campaigns – highlighting the connection between instability and disinformation.”²³ Multiple actors are involved in the campaigns, some of them amplifying one another while others clash or take different directions. “Nearly 60 percent of disinformation campaigns on the continent are foreign state-sponsored – with Russia, China, the United Arab Emirates (UAE), Saudi Arabia, and Qatar as the primary sponsors.”²⁴ It is unclear why the report didn’t mention any Western country for involvement in disinformation campaigns in Africa. This omission warrants further investigation, particularly regarding the potential invisibility or sophistication of Western-led operations. It is possible that the Africa Center, a think tank of the United States (US) Department of Defense, chose to focus only on the campaigns of non-Western nations. Western colonial powers had used propaganda before to advance their imperial interests in Africa and Western intelligence agencies have carried out many influence operations in the continent.²⁵ Bradshaw and Howard, for instance, point to the United States’ “active campaigns of influence” as well as counter-propaganda activities and anti-jihadist campaigns, among other operations.²⁶ “The United States has made perhaps the largest financial investment of any nation in foreign influence, conducting surveillance and projecting soft power through media influence.”²⁷ And most of the social media platforms being used for influence campaigns in Africa – such as Facebook, X (formally Twitter), Instagram, YouTube and WhatsApp – are owned by US firms, although Chinese-owned TikTok, Russia’s RUTUBE (an imitation of YouTube) and Telegram (founded by Russian entrepreneurs) are also rapidly gaining ground now in the continent.²⁸ The involvement of Britain’s Cambridge Analytica in elections interference in Nigeria and Kenya was also well documented – and so was the British PR agency Bell Pottinger’s role in Guptas’ influence operations in South Africa during Jacob Zuma’s regime.²⁹ But the foreign power with the biggest prominence in influence campaigns in Africa now is Russia. Africa Center’s report shows that between 2022 and early 2024 Russia sponsored 80 documented disinformation campaigns targeting over 22 African countries – which represents almost 40% of such

²³ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 2.

²⁴ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 2.

²⁵ Tony Roberts and George Karekwaivanane, *Digital Disinformation in Africa: Hashtag Politics, Power and Propaganda* (eds.) (London: 2024),

²⁶ Samantha Bradshaw and Philip Howard, *Challenging Truth and Trust: A Global Inventory of Organised Social Media Manipulation* (Oxford: 2018), p. 71.

²⁷ Roberts and Karekwaivanane, *Digital Disinformation in Africa*, p. 5.

²⁸ Jonathan, “How Telegram, TikTok aided Russian disinformation.”

²⁹ Bradshaw and Philip Howard, *Challenging Truth and Trust*.

campaigns in the continent. “These 80 campaigns have reached many millions of users through tens of thousands of coordinated fake pages and posts. Aggressively leveraging disinformation is a mainstay of Russia’s use of irregular channels to gain influence in Africa,” the report says.³⁰

West and Central Africa are the most targeted regions and Russia’s rising influence in countries such as Burkina Faso, Mali, Niger, Chad and Central African Republic appears to have emboldened Kremlin to widen its operations.³¹ The case of its operations in Nigeria, mentioned earlier, is among the latest. Russian-sponsored online portal “African Initiative” and TikTok influencers as well as Telegram and RUTUBE channels were the major tools used in that campaign.³² South Africa, Sudan, Egypt, Libya, Morocco, Mozambique and Madagascar have also been witnessing Russian operations. The Wagner Group has been the primary instrument of the campaigns, but after the death of its founder Yevgeny Prigozhin in 2023 the newly formed Russian Africa Corps and African Initiative have become the key operators. Their campaigns “employ paid African influencers, digital avatars, and the circulation of fake and out-of-context videos and photographs.”³³ However, not all the campaigns were effective. Seyoung Jeon’s study has found that the level of Russian involvement in election interference in Africa was exaggerated. “In Zimbabwe, South Africa and the DRC, despite serious domestic concern over Russian interference, in reality the level of disinformation was insignificant.”³⁴ Russian campaigns were more effective in opportunistic interference in areas affected by conflicts, as seen in Burkina Faso, Mali, Niger and Central African Republic. It capitalized on France’s diminishing influence in those countries and became an effective replacement of the former colonial power. Russia’s interest in Africa extends beyond the continent: It uses African bases to launch operations against the United States.³⁵ Part of its alleged US elections meddling operations in 2020 was reportedly run from the West African countries of Ghana and Nigeria.³⁶ Clifford and Gruzd argue that Russia outsources “the creation of content to local operators in Africa” to evade detection or get “plausible deniability should the campaign be uncovered.”³⁷

China is another foreign power that uses cyber-enabled information campaigns to advance its interest in Africa. Disinformation is found to be part of its strategy. The report of Africa Center says China “is the second most prolific Africa-wide sponsor of disinformation with five known multi-regional campaigns”—two of which “have aligned with or amplified Russian narratives.”³⁸ The two areas of common campaigns are on spreading anti-Western and anti-United Nations (UN) messages. But China’s approach is focused on promoting Chinese Communist Party “narratives through the ownership and control of [Information and Communication Technology] infrastructure as well as through licensing and training agreements with African media.”³⁹ It is far beyond disinformation campaigns; it focuses on

³⁰ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 3.

³¹ Morley-Davies *et al.*, *Russian Information Operations*.

³² Jonathan, “How Telegram, TikTok aided Russian disinformation.”

³³ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 4.

³⁴ Seyoung Jeon, “Are claims of Russian disinformation in Africa founded? Elections in Zimbabwe, South Africa and the Democratic Republic of the Congo,” in Tony Roberts and George Karekwivanane (eds.) *Digital Disinformation in Africa: Hashtag Politics, Power and Propaganda* (London: 2024), pp. 125-152, p. 147.

³⁵ Cayley Clifford and Steven Gruzd, *Russian and African Media: Exercising Soft Power* (Johannesburg: South African Institute of International Affairs, 2022).

³⁶ Clarissa Ward, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore and Tim Lister, “Russian election meddling is back – via Ghana and Nigeria – and in your feeds,” *CNN*, April 11, 2020.

<https://edition.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html> (accessed 2 October 2025)

³⁷ Clifford and Gruzd, *Russian and African Media: Exercising Soft Power*, pp. 12-13.

³⁸ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 4.

³⁹ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 4.

broad influence operations; and is more futuristic, with clear emphasis on dominating digital infrastructure in the continent. China leverages its Digital Silk Road scheme—part of its Belt and Road Initiative (BRI)—for this and encourages its companies to focus on controlling African digital space. From building undersea cables to supplying cybersecurity and smartphones, China and its firms have put their hands in every aspect of Africa’s digital ecosystem.⁴⁰ It has digital infrastructure projects in 47 out of the 54 African countries and its companies such as Huawei, China Mobile, ZTE, Dahua, China Telecom, Hikvision, Meiya Pico and Uniview are involved in developing communications infrastructure in different parts of the continent.⁴¹ The Chinese government always presents BRI “as a long-term, transnational and systematic global project” that “has brought remarkable and profound change to the world.”⁴² But research shows that it also uses it to advance its foreign policy objectives in Africa. “China’s digital expansionism through its Digital Silk Road (DSR) projects is promoting its geopolitical agenda in African countries,” Kumar argues. “Chinese companies, which are dominating the African digital technology space, are also setting new technology standards and norms that challenge the existing US-led global digital order.”⁴³ Involvement in digital infrastructural projects enhances China’s information operations, which it directs mostly on South Africa, Zimbabwe, Angola, Namibia, Botswana, Malawi and Ethiopia but also on the West African countries of Ghana, Mali and Liberia. The campaigns focus on promoting China’s political and business interests and on spreading anti-Western sentiments.⁴⁴

External state actors’ use of cyber-enabled information campaigns in Africa is part of their quest for power within and outside the continent, as has always been the case of foreign powers who engage in propaganda. This reinforces Taylor’s conception of propaganda as a powerful instrument of power struggles.⁴⁵ Changes brought by time and technology have not altered that basic principle. What they have brought are new tools and environment: cyberspace and digital devices. “Over the years,” Vicić and Harknett observe, “cyberspace has become one of the primary environments of inter-state struggle for power and autonomy, which allows governments to engage in geopolitics advancing their own interests while hindering those of their foes.”⁴⁶ It also offers room for greater flexibility, anonymity and durability. “The plasticity of cyberspace means that opportunities for mischief or hostility change continually,” creating new vulnerabilities.⁴⁷ However, the targeted audiences do also have their own agency: they can refuse to engage with the messages or reject them (where they are able to detect them) or interpret them in their own way, as audience scholarship suggests.⁴⁸ China’s use of anti-colonial narratives in her campaigns, for instance, has not prevented many Africans from distrusting the messages and describing her as a new colonialist in Africa. “Through its digital

⁴⁰ Yinka Adegoke, “The real reason China is pushing ‘digital sovereignty’ in Africa,” *Rest of the World*, 1 December 2021. <https://restofworld.org/2021/the-real-reason-china-is-pushing-digital-sovereignty-in-africa/> (accessed 2 October 2025).

⁴¹ Suneel Kumar, “China’s digital expansionism in Africa and the US counter-strategies,” *Insights on Africa*, 16/2 (2024), 146-165.

⁴² State Council Information Office of the PRC, “The Belt and Road Initiative: A Key Pillar of the Global Community of Shared Future,” *State Council Information Office*, October 10, 2023. http://www.scio.gov.cn/zfbps/zfbps_2279/202310/t20231010_773734_m.html (accessed 2 August 2025).

⁴³ Kumar, “China’s digital expansionism in Africa,” p. 146.

⁴⁴ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*.

⁴⁵ Taylor, *Munitions of the Mind*.

⁴⁶ Vicić and Harknett, “Identification-imitation-amplification,” p. 899.

⁴⁷ Nicholas Michael Sambaluk, *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm* (Praeger, 2020), p. 35.

⁴⁸ See Stuart Hall, “Encoding and decoding in the television discourse,” *Culture, media, language* (Routledge, 1980), pp.128-138; and David Gauntlett, *Moving Experiences: Media Effects and Beyond*. 2nd ed (Eastleigh, 2005).

infrastructure, Beijing, as it is being argued, is also spreading ‘digital authoritarianism,’ promoting an ‘illiberal political order’ and pursuing ‘data colonialism.’”⁴⁹ This is despite its insistence that its capital investment supports solid economic transformation in the continent.⁵⁰

Domestic Influence Campaigns

Domestic state actors are the other key sponsors of cyber-enabled information campaigns in Africa, deploying them mostly in areas of conflicts, political control and elections manipulation. Analysis shows that countries contending with armed conflicts and political instability experience more intense influence campaigns than those with more stable governments. Sudan, Ethiopia, Central African Republic, Libya, Mali and Burkina Faso have all witnessed a rise in such campaigns. Their governments and opposition forces as well as their respective foreign backers engage in cyber operations to advance their causes. Sudanese have been bombarded with digital propaganda, spread by the two sides of the country’s deadly conflict—the Sudanese Armed Forces and the paramilitary Rapid Support Forces. “Regional and foreign powers with vested interests in the war (Russia, the UAE, and Egypt) have also been active sponsors of disinformation in support of their respective proxy.”⁵¹ Ethiopia, too, has experienced serious cyber-enabled influence operations perpetrated mostly by the federal government and by the opposing sides in both the Tigray War and the War in Amhara. Online propaganda spread “like wildfire across social media platforms” at the peak of those conflicts, Ayalew observes. “Due to the lack of robust content regulation by social media platforms, the digital sphere in Ethiopia is increasingly filled with hateful content and propaganda against vulnerable communities in conflict situations and political [dissidence].”⁵² Protracted conflicts in Libya place the country at the center of information campaigns run by competing forces, particularly Khalifa Haftar’s Libyan National Army (LNA) and the government of national unity. The LNA is supported by Russia in its influence operations, promoting narratives against the Libyan Political Dialogue Forum. “Disinformation undermining the UN Support Mission in Libya has been widely circulated, benefiting the LNA.”⁵³ In Central African Republic, Mali and Burkina Faso, the governments and their Russian backers are also actively engaged in cyber-enabled operations to enhance their hold on power and to counter France’s propaganda against them, with disinformation constituting a key part of their campaigns.

Research on digital disinformation across ten African countries of Angola, Cameroon, Democratic Republic of Congo, Ethiopia, Kenya, Mozambique, Nigeria, South Africa, Uganda and Zimbabwe shows that it is not only conflict that drives disinformation in domestic scene in the continent; disinformation is also used in creating and maintaining social control and political power. Roberts and Karekwaivanane have analyzed “the dimensions, dynamics, drivers and directions of digital disinformation in Africa” and how it is “deployed to manipulate the beliefs and behaviours of citizens in order to serve the interests of powerholders.”⁵⁴ Deploying disinformation to suppress domestic dissent is not limited to the ten countries covered by the study. “Domestic disinformation targeting opposition political actors and pro-democracy activists has been documented in each North African country,” notes Africa Center.

⁴⁹ Kumar, “China’s digital expansionism in Africa,” p.155.

⁵⁰ Linda Calabrese, “Chinese capital and economic transformation in Africa: What has changed after Covid-19”, *Review of African Political Economy*, 52/184 (2025): 245-257, p. 245.

⁵¹ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 6.

⁵² Yohannes Ayalew, “Tackling online propaganda in internal armed conflict situation in Ethiopia” *Propaganda & Emerging Tech*, 1 August 2024. https://law.yale.edu/sites/default/files/area/center/isp/documents/mwi-yohannes-ayalew_2024-08-01_re-fin.pdf, p. 2 (accessed 2 October 2025).

⁵³ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 8.

⁵⁴ Roberts and Karekwaivanane, *Digital Disinformation in Africa*, p. 21.

“Supporters of Tunisian President Kaïs Saïed have been especially active in deploying these tools to discredit the opposition and normalize his extraconstitutional seizure of power.”⁵⁵ In Egypt, the government of Abdel Fattah El-Sisi employs a similar strategy to demonise the opposition—especially the Muslim Brotherhood “who are depicted as enemies of the nation”—while El-Sisi is presented as “the sole protector of the people.”⁵⁶

Elections offer even greater opportunities for state actors in Africa to engage in cyber-enabled information campaigns. The case of the ruling elites in Kenya and Nigeria employing Britain’s Cambridge Analytica to use dirty digital tricks in cyberspace to manipulate elections in 2013, 2015 and 2017 is well known. What is less known is that the scandal didn’t deter the two countries’ ruling elites – and to some extent their opponents—from using influence operations to manipulate subsequent elections. Kenya’s elections of 2022 and Nigeria’s in 2019 and 2023 were equally marked by manipulative information campaigns, but this time relying mostly on local agents. “Influence operations during Kenya’s 2022 presidential elections were largely indigenous [...]. They tapped into existing fears, social cleavages and conspiracy theories based on mistrust of the state, and amplified them online.”⁵⁷ In Nigeria, they deployed various tactics including using social media platforms to smear political opponents. Social media influencers were also paid to promote “political leaders by equivocation of identities, exaggerating the performance of their principals, falsifying corruption allegations against their principals’ competitor and concealing the transgressions of their principals.”⁵⁸ Fake social media accounts and doctored videos and still pictures were used to spread falsehoods, including linking certain candidates to terror groups and elections rigging. Other countries such as Angola, Cameroon, Democratic Republic of Congo, South Africa, Uganda and Zimbabwe do all have cases of using cyber-enabled information operations during elections, with some of them employing foreign consultancy firms to run them on their behalf. “One private Israeli group, dubbed ‘Team Jorge,’ has reportedly implemented disinformation campaigns to disrupt over 20 African elections since 2015.”⁵⁹ Election contests are essential part of power struggles and the prevalence of propaganda in them reinforces Taylor’s theory of propaganda as a powerful tool of mediating power relations.

Extremists’ Information Operations

The other major actors involved in cyber-enabled information campaigns in Africa are violent extremist groups—defined here as organizations that deliberately use violence to pursue their ideological, political and/or religious goals. The term is used interchangeably with terrorist groups as terrorism is part of their activities. From Boko Haram and its splinter outfits, *Ansaru* and the Islamic State’s West African Province (ISWAP) in Nigeria, to several terror groups in the Sahel and Al-Shabaab in East Africa and Islamic State in Mozambique,⁶⁰ violent extremist groups have, for many years, been waging cyber-enabled campaigns in different parts of Africa. The al-Qaeda in the Islamic Maghrib (AQIM) and Islamic State’s units in North Africa

⁵⁵ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 8.

⁵⁶ Majd Abuamer, “Disinformation as an authoritarian strategy: The populist playbook in Egypt and Tunisia,” *British Journal of Middle Eastern Studies* (2025), DOI: 10.1080/13530194.2025.2479515, p. 12.

⁵⁷ Karen Allen, Jean Roux and Bonface Beti, *A Question of Influence? Case Study of Kenyan Elections in a Digital Age* (Pretoria: 2023), p. 2.

⁵⁸ Uwalaka *et al.*, “Social media influencers and political influence operations” p. 89.

⁵⁹ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 3.

⁶⁰ The group has other names – ISIS-Mozambique, *Ahlu al-Sunnah wal-Jamaah* (ASJ), *Ansar al-Sunnah* and *Al-Shabaab*, although it is not linked to East Africa’s *Al-Shabaab*. Boko Haram, too, has its original name – *Jama’atu Ahlis-Sunnah Lidda’ati wal-Jihad* – and there are several other extremist groups in Africa with various names.

were originally the dominant groups in violent extremism messaging, but after they were degraded in the region, extremist groups in sub-Saharan Africa become more active in influence operations in the continent. Analysis of documents, social media, and online audio-visual contents shows that they deploy the digital tools at their disposal to promote their ideology, intimidate their adversaries and recruit new members. Of all the state and non-state actors that engage in influence operations in Africa, violent extremists seem to be the ones who are most dependent on cyberspace as a primary operational and recruitment vector due to spatial displacement and asymmetric capabilities. This is mainly because they have been forced to operate underground and it is increasingly becoming the only main means of campaign available to them. Cyber-enabled campaigns are largely operated covertly even by legitimate groups and it is the covertness that makes it more viable to violent extremists.

When Boko Haram was forced to go underground following sustained military campaigns against it in Nigeria, Niger, Chad and Cameroon, it shifted its operations to cyberspace and its members quickly specialized in digital production and dissemination of their messages. “From uploading their videos and audios on the internet to opening and operating social media accounts, the insurgents have demonstrated adequate technical skill to help transform them into ‘digital terrorists.’”⁶¹ Their social media accounts are often suspended and YouTube always removes their offensive materials but usually after the newsworthy ones have been picked and publicized by the news media. The Nigerian military regularly counters Boko Haram and its splinter groups by engaging in cyber campaigns against them.⁶² Numerous anti-Boko Haram videos—“some of them purporting to come directly from the group or showing the capture and killing of its leader [when he was still alive]”—were uploaded on the internet apparently by security services.⁶³ The constant suspension of the extremists’ social media accounts and regular removal of their materials from YouTube are the result of the security services’ work. However, Boko Haram and the splinter groups, including bandits that are associating with them in Nigeria, are increasingly finding ways to evade this by using closed networks, especially Telegram. They are also using TikTok so much now that they could be described as “TikTok terrorists.”⁶⁴

Al-Shabaab in Kenya and Somalia had earlier got the tag “Twitter terrorists” when they turned the platform into one of their tools of terror activities. They used it to provide running commentaries on their attack of Nairobi’s Westgate Shopping Centre in 2013, justifying their actions and taunting Kenyan security forces.⁶⁵ “Al Shabaab and the Islamic State in Somalia (ISS) have been early and innovative adopters of disinformation in East Africa, setting up pages that pose as media outlets on Facebook and using those pages to spread extremist ideology in African languages.”⁶⁶ In Mali, Burkina Faso and Niger, extremist groups – who have recently gained more strength – are intensifying their information operations on the internet and social media platforms to propagate their ideology and spread anti-state narratives in the region. The

⁶¹ Abdullahi Tasiu Abubakar, “Strategic communications, Boko Haram, and counter-insurgency,” *Defence Strategic Communications*, 3/Autumn (2017), 139–169, p. 155.

⁶² Abubakar, “Strategic communications”.

⁶³ Abubakar, “Strategic communications”, p. 161.

⁶⁴ Aliyu Dahiru, “Inside the propaganda world of Nigerian terrorists on TikTok,” *HumAngle*, 31 August 2024. <https://humanglemedia.com/inside-the-propaganda-world-of-nigerian-terrorists-on-tiktok/> (accessed 2 October 2025).

⁶⁵ Chris Greenwood, “The Twitter terrorists: How killers boasted of Kenyan mall carnage with live commentary as they murdered dozens of people,” *Daily Mail*, 23 September 2013. <https://www.dailymail.co.uk/news/article-2429660/Kenya-attack-How-killers-boasted-Nairobi-Westgate-shopping-mall-carnage-Twitter.html> (accessed 2 October 2025).

⁶⁶ Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, p. 6.

Islamic State in Mozambique was also found to have engaged in digital disinformation campaigns, such as using manipulated videos and false claims against the state and its security forces, to strengthen their insurgency in the country. However, the Mozambique government “through mainstream media and an army of government-aligned ‘digital firefighters’ seek to counter disinformation with their own narrative on the war.”⁶⁷ In all these cases, violent extremists and counter-terrorism forces in Africa appear to have found cyberspace well suited for their influence operations, confirming cyber capabilities to “enhance the scale and speed of information dissemination” and “to micro-target audiences to an extent that was not technologically feasible in the past.”⁶⁸ It is those capabilities that increase both the viability of cyber-enabled operations and the vulnerability of their target audiences.

Conclusion

Cyber-enabled information campaigns have risen rapidly in Africa as foreign powers and domestic state and non-state actors increasingly engage in struggles for power in the continent. Technological advances and expansion of digital communications enhance Africa’s presence in cyberspace but also turn the continent into a fertile ground for cyber-enabled operations. Russia and China appear to be the most active foreign powers using such campaigns to advance their interests in the continent and to undermine those of their Western adversaries. Domestic governments are the other major participants in influence operations, directing them against local opponents and deploying them for elections manipulation and for countering armed rebellions during conflicts. Social media platforms – mostly owned by American firms – and Western political marketing consultancies are among the major tools they use for their operations. Violent extremist groups demonstrate greater desperation to engage in cyber-enabled information campaigns not only because they are forced to go underground – which makes this tool very viable to them – but also because propaganda is at the center of their activities. They use them to recruit new members, promote their ideology and intimidate their enemies. All these actors show no sign of relenting in their campaigns. Their determination and the apparent viability of their operations suggest that the phenomenon will continue to grow, with wider ramifications, potentially increasing insecurity and political instability in the continent. This should prompt African leaders to take mitigation measures—such as improving critical digital media literacy, encouraging robust counter messaging with accurate information, exerting pressure on social media firms to police their platforms responsibly, and instituting effective regulatory regimes—to minimize the continent’s vulnerability.

Although this chapter has shed light on the patterns, dimensions, driving forces and broad consequences of cyber-enabled influence campaigns in Africa, it has only scratched the surface of this complex and expanding phenomenon. Further research is needed to explore in greater depth the specific tactics and techniques each actor employs in their operations in each country, evaluate their performances, and make comparative analyses. This study has also shown that it is mostly the powerful who use influence operations to advance their interests, often to the detriment of collective wellbeing. Future research can examine their wider consequences on society, especially their impacts on peace and stability, democracy and human rights in Africa. Exploring different strategies for countering them is another area scholars and policymakers can also focus on as a multi-faceted approach is needed to tackle a problem as complicated as manipulation of human minds.

⁶⁷ Roberts and Karekwaivanane, *Digital Disinformation in Africa*, p. 17.

⁶⁸ Vičić and Gartzke, “Cyber-enabled influence operations,” p. 11.

References

- Abuamer, Majd. "Disinformation as an authoritarian strategy: The populist playbook in Egypt and Tunisia." *British Journal of Middle Eastern Studies* (2025): 1-20, DOI: 10.1080/13530194.2025.2479515.
- Abubakar, Abdullahi Tasiu. "Strategic communications, Boko Haram, and counterinsurgency." *Defence Strategic Communications*, no. 3 (2017): 139-169.
- Adegoke, Yinka. "The real reason China is pushing 'digital sovereignty' in Africa." *Rest of the World*, 1 December 2021. <https://restofworld.org/2021/the-real-reason-china-is-pushing-digital-sovereignty-in-africa/> (accessed 5 January 2025).
- Africa Center for Strategic Studies. *Mapping a Surge of Disinformation in Africa*. Washington, DC: Africa Center for Strategic Studies, 2024. <https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/> (accessed 15 February 2025).
- Allen, Karen, Jean Roux, and Bonface Beti. *A Question of Influence? Case Study of Kenyan Elections in a Digital Age*. Pretoria: Institute for Security Studies, 2023.
- Ayalew, Yohannes. "Tackling online propaganda in internal armed conflict situation in Ethiopia: An uphill task?" *Yale Information Society Project*, August 1, 2024. https://law.yale.edu/sites/default/files/area/center/isp/documents/mwi-yohannes-ayalew_2024-08-01_re-fin.pdf (accessed 13 December 2024).
- Bateman, Jon, and Dean Jackson. *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Washington DC: Carnegie Endowment, 2024.
- Bradshaw, Samantha and Philip Howard. *Challenging Truth and Trust: A Global Inventory of Organised Social Media Manipulation*. Oxford: Oxford Internet Institute, 2018.
- Clifford, Cayley, and Steven Gruz. *Russian and African Media: Exercising Soft Power*. Johannesburg: South African Institute of International Affairs, 2022.
- Calabrese, Linda. "Chinese capital and economic transformation in Africa: What has changed after Covid-19?" *Review of African Political Economy* 52, no. 184 (2025): 245—257.
- Dahiru, Aliyu. "Inside the propaganda world of Nigerian terrorists on TikTok." *HumAngle*, August 31, 2024. <https://humanglemedia.com/inside-the-propaganda-world-of-nigerian-terrorists-on-tiktok/> (accessed 1 September 2024).
- Eboh, Camillus. "Nigeria charges 76, including minors, with treason after August protests," *Reuters*, November 1, 2024. <https://www.reuters.com/world/africa/nigeria-charges-76-including-minors-with-treason-after-august-protests-2024-11-01/> (accessed 2 November 2024).
- Gauntlett, David. *Moving Experiences: Media Effects and Beyond*. 2nd ed. Eastleigh: John Libbey, 2005.
- Greenwood, Chris. "The Twitter terrorists: How killers boasted of Kenyan mall carnage with live commentary as they murdered dozens of people." *Daily Mail*, September 23, 2013.

<https://www.dailymail.co.uk/news/article-2429660/Kenya-attack-How-killers-boasted-Nairobi-Westgate-shopping-mall-carnage-Twitter.html> (accessed 24 September 2013).

Hall, Stuart. "Encoding and decoding in the television discourse." In *Culture, Media, Language*, edited by Stuart Hall, Dorothy Hobson, Andrew Lowe and Paul Willis. London: Routledge, 1980, pp. 128—138.

Jeon, Seyoung. "Are claims of Russian disinformation in Africa founded? Elections in Zimbabwe, South Africa and the Democratic Republic of the Congo." In *Digital Disinformation in Africa: Hashtag Politics, Power and Propaganda*, edited by Tony Roberts and George Karekwivanane. London: Zeb Books, 2024.

Jonathan, Silas. "How Telegram, TikTok aided Russian disinformation that led to the incarceration of Nigerian minors." *Premium Times*, November 14, 2024. <https://www.premiumtimesng.com/news/headlines/754117-how-telegram-tiktok-aided-russian-disinformation-that-led-to-incarceration-of-nigerian-minors.html> (accessed 14 November 2024).

Kumar, Suneel. "China's digital expansionism in Africa and the US counter-strategies." *Insights on Africa* 16, no. 2 (2024): 146—165.

Lilli, Eugenio. "How can we know what we think we know about cyber operations?" *Journal of Global Security Studies* 8, no. 2 (2023): 1—18.

Lin, Herbert, and Jaclyn Kerr. "On cyber-enabled information warfare and information operations." In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish. Oxford: Oxford University Press, 2021, pp. 251—272.

Morley-Davies, Jonathan, Jem Thomas, and Graham Baines. *Russian Information Operations Outside of the Western Information Environment*. Riga: NATO Strategic Communications Centre of Excellence, 2024.

Roberts, Tony, and George Karekwaivanane (eds.). *Digital Disinformation in Africa: Hashtag Politics, Power and Propaganda*. London: Zed Books, 2024.

Sambaluk, Nicholas Michael. *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm*. Santa Barbara, California: Praeger, 2020.

State Council Information Office of the PRC. "The Belt and Road Initiative: A key pillar of the global community of shared future. *State Council Information Office*, October 10, 2023. http://www.scio.gov.cn/zfbps/zfbps_2279/202310/t20231010_773734_m.html (accessed 2 August 2025).

Taylor, Philip. *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day*. (3rd edition) Manchester: Manchester University Press, 2003.

Taylor, Philip (2007) "'Munitions of the mind': A brief history of military psychological operations." *Place Branding and Public Diplomacy*, no. 3 (2007): 196—204.

Uwalaka, Temple, Fred Amadi, and Stella Enyindah. "Social media influencers and political influence operations: The Data Boys example in Nigeria." *Public Relations Inquiry* 14, no. 1 (2025): 89—115.

- Vičić, Jelena, and Erik Gartzke. “Cyber-enabled influence operations as a ‘center of gravity’ in cyberconflict: The example of Russian foreign interference in the 2016 US federal election.” *Journal of Peace Research* 61, no. 1 (2024): 10—27.
- Vičić, Jelena, and Richard Harknett. “Identification-imitation-amplification: Understanding divisive influence campaigns through cyberspace.” *Intelligence and National Security* 39, no. 5 (2024): 897—914.
- Ward, Clarissa, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, and Tim Lister. “Russian election meddling is back – via Ghana and Nigeria – and in your feeds.” CNN, April 11, 2020. <https://edition.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html> (accessed 10 August 2024).