Media and Communication
2027 • Volume 15 • Article 12815
https://doi.org/10.17645/mac.12815

ARTICLE

Open Access Journal

Cyber-Militia and Digital Coercion: Online Targeting and Militarised Communication in Burkina Faso

Samba Dialimpa Badji [1] and Harouna Drabo [2]

[1] Department of Journalism and Media Studies, Oslo Metropolitan University, Norway
[2] Institut Français de Géopolitique, Université Paris 8, France

Correspondence: Samba Dialimpa Badji (sambadia@oslomet.no)

Submitted: 15 May 2026 **Accepted:** 20 August 2026 **Published:** 12 November 2026

Issue: This article is part of the issue "Digital Media in Contemporary Conflicts" edited by Kristin Skare Orgeret (Oslo Metropolitan University) and Mulatu Alemayehu Moges (University of Agder), fully open access at https://doi.org/10.17645/mac.i516

Abstract

This article examines the emergence of coordinated pro-regime digital networks in Burkina Faso through the concept of "cyber-militia." Drawing on a comparative qualitative analysis of 468 Facebook entries collected across three online targeting campaigns, the study explores how actors associated with the Brigade d'intervention rapide de la communication (BIR-C) use digital platforms to amplify hostile narratives, intimidate critics, and delegitimise individuals and organisations perceived as threats to the military regime. Combining qualitative content analysis and process tracing, the article identifies three operational logics of cyber-militia communication: escalation and intimidation, persistence and reputational delegitimisation, and institutional delegitimisation. The findings suggest that cyber-militias function as hybrid formations situated at the intersection of propaganda, participatory digital culture, and coercive state power. The article contributes to scholarship on digital media and conflict by proposing cyber-militia as a new analytical framework for understanding coordinated forms of participatory digital coercion in contemporary conflict environments.

Keywords

Burkina Faso; conflict communication; digital authoritarianism; digital media; Facebook; online harassment; propaganda

1. Introduction

Digital media have become central arenas in contemporary conflicts, profoundly reshaping how political narratives are produced, circulated, and contested (Alsharairi et al., 2025; Castells, 2009; de Bruijn, 2025;

© 2026 by the author(s), licensed under a Creative Commons Attribution 4.0 International License (CC BY).

Zeitzoff, 2017). Social media platforms no longer function merely as communication or mobilisation tools; they increasingly serve as strategic spaces where legitimacy, authority, and dissent are negotiated through coordinated online practices (Friis Hau, 2025). Digital platforms can simultaneously facilitate citizen expression and enable forms of intimidation, surveillance, and digital repression (Yingi & Benyera, 2025).

Since 2015, Burkina Faso has experienced escalating violence linked to jihadist armed groups, particularly Jama'at Nusrat al-Islam wal-Muslimin (JNIM), affiliated with Al-Qaeda in the Islamic Maghreb (AQIM). The worsening security situation contributed to two military coups in 2022, first bringing Lieutenant-Colonel Paul-Henri Damiba to power and later Captain Ibrahim Traoré. Following the second coup, the military authorities increasingly framed information control as a matter of national defence and political stability. Official discourse promoted what was described as "patriotic information," while journalists, activists, and critical voices faced mounting pressure (Chams, 2025).

Alongside restrictions imposed on traditional media, social media emerged as a crucial site of political contestation. A coordinated network of cyber-activists and pro-regime influencers commonly referred to as the Brigade d'intervention rapide de la communication (BIR-C) became increasingly visible online. Through coordinated publications, amplification strategies, and hostile engagement directed at critics of the regime, the BIR-C appeared to function as a digital extension of the regime's broader communication and security apparatus (Ouedraogo, 2026).

This article introduces the concept of cyber-militia not as a completely distinct concept from electronic armies, state-sponsored trolling, or computational propaganda, but rather as a pertinent extension of the current literature on these themes. It underscores the militarisation of networked support systems employed by regimes in conflict-affected regions, where online targeting frequently employs operational language and strategies that symbolically (and at times temporally) connect digital intimidation with offline coercive practices.

Using cyber-militia as an analytical framework, this study seeks to contribute to the scholarship on digital authoritarianism by elucidating the role of semi-formal digital actors operating alongside state institutions.

This article addresses the following research question:

> How do coordinated pro-regime digital networks operate as cyber-militias within contemporary conflict-related information environments?

This overarching research question is divided into four specific research questions:

> RQ1: What coordination mechanisms characterise the communication practices of the BIR-C on Facebook?
>
> RQ2: How are hostile narratives constructed and amplified against individuals and organisations perceived as opponents of the regime?
>
> RQ3: What role does participatory engagement play in the reinforcement of cyber-militia communication?

RQ4: How does militarised digital discourse contribute to the normalisation of coercive practices online?

Drawing on a comparative analysis of three Facebook-based targeting campaigns involving two individuals and one organisation, the study examines the operational logics, communication strategies, and coercive dimensions associated with cyber-militia activity.

In 2025, Burkina Faso had 5.42 million internet users, including 3.90 million social media users (Kemp, 2026). Facebook overwhelmingly dominates the country's social media landscape, accounting for nearly all active social media users, particularly among the youth ("Burkina Faso Digital Report 2025," 2025; Kemp, 2026). The platform has become both a major source of news consumption and a key arena for political debate, mobilisation, and civic engagement. Its political influence has been visible since the 2014 popular uprising that led to the fall of Blaise Compaoré, during which Facebook played a central role in coordinating protest narratives and citizen mobilisation (Gouba, 2024; Sawadogo, 2015). The widespread accessibility of Facebook and related applications such as WhatsApp has further reinforced the strategic importance of digital platforms in shaping political communication and information struggles in Burkina Faso (Yameogo, 2020).

2. Political and Security Context: Burkina Faso Under Ibrahim Traoré

In April 2026, Yousra Elbagir, a journalist with the British television channel Sky News, became the target of a significant wave of online harassment following the publication of a report on Burkina Faso (Beraud, 2026; Elbagir, 2026). Posts and comments accused her of being a "mercenary of the pen" and alleged that she came from a family of "influence agents serving Western hegemony" ("Une journaliste de Sky News," 2026). A British telephone number purportedly belonging to her was also circulated, accompanied by calls for coordinated harassment. The campaign illustrates the increasingly confrontational character of Burkina Faso's digital information environment, where journalists and other perceived critics can become targets of networked denunciation and intimidation.

The episode occurred after the present research had begun and is, therefore, not included in the analysed corpus. It is nevertheless illustrative of the continuing evolution of the targeting practices associated with the BIR-C. Elbagir is not an isolated target: The BIR-C has been associated with several other digital campaigns directed at individuals and organisations portrayed as hostile to Burkina Faso's military authorities. The episode, therefore, provides a contemporary entry point for understanding the political and security environment in which the BIR-C emerged, while also raising questions about the potentially gendered dimensions of such attacks, which fall beyond the scope of the present analysis.

Burkina Faso's political instability is closely intertwined with an increasingly protracted armed conflict. Since the escalation of jihadist violence in the mid-2010s, large parts of the country have experienced persistent insecurity, displacement, and disruption of state authority. The deteriorating security situation contributed to two military takeovers in 2022, culminating in Captain Ibrahim Traoré's seizure of power in September ("Coup d'État au Burkina Faso," 2022). Under the transitional military authorities, the fight against armed groups has remained central to political legitimacy and public discourse. The regime has increasingly promoted narratives centred on sovereignty, patriotism, anti-imperialism, and national resistance, while framing the defence of the nation against both armed and perceived ideological enemies as a central political imperative.

This context has intensified struggles over information. Government authorities, pro-regime actors, journalists, civil-society organisations, and other political actors compete to define the nature of the security crisis and the legitimacy of the state's response. Pressure on critical media has also increased. Several international media outlets have been suspended, while local journalists, civil-society actors, and online commentators critical of the authorities have faced intimidation, surveillance, and other forms of repression ("Burkina Faso: Disparition forcée," 2025; "Burkina Faso: Liberté d'expression," 2025). Public communication has increasingly been framed around the notion of "patriotic information," encouraging media and citizens to align their narratives with what is presented as the national interest.

Against this backdrop, social media, particularly Facebook, has become an important arena of political confrontation. Digital platforms provide spaces not only for mobilisation and the circulation of conflict narratives, but also for discrediting perceived opponents and contesting competing interpretations of the war. It is within this environment of political instability, armed conflict, and intensified struggles over information that the BIR-C emerged as a network of cyber-activists, influencers, and pro-regime digital supporters operating in support of the military authorities' broader political narrative.

The emergence of the BIR-C also echoes the creation of the Bataillons d'intervention rapide (BIR) in November 2022 ("Burkina: Création de six bataillons," 2022). Established to strengthen the Burkinabè military's offensive capabilities against jihadist armed groups through mobility and rapid deployment, the BIR operate on the physical battlefield. The BIR-C, by contrast, invokes similar militarised imagery in the informational sphere, treating communication as another theatre of confrontation. Its discourse includes references to operations, missions, fronts, apprehension, and continued mobilisation, thereby transferring elements of military vocabulary into political communication.

The phenomenon also evokes historical parallels with the Comités de défense de la révolution (CDRs) established during Thomas Sankara's revolutionary government between 1983 and 1987. The CDRs were conceived as grassroots structures for mobilising citizens in support of the revolution, but also became associated with surveillance, denunciation, intimidation, and social control directed at perceived opponents (François, 2023; Lalsaga, 2020; Ziegler & Rapp, 1986). Although the historical and technological contexts differ substantially, the comparison is analytically useful because both formations connect political mobilisation with ideological enforcement and participatory control. Whereas the CDRs operated through neighbourhood structures and physical mobilisation, the BIR-C operates through digital networks, amplification, and participation on social media.

Taken together, these developments suggest that the BIR-C should not be understood simply as a communication network. It emerged within a political environment in which the boundaries between military mobilisation, political loyalty, and information warfare have become increasingly blurred. The militarisation of political communication in contemporary Burkina Faso can, therefore, be understood as a reconfiguration of older practices of mobilisation, surveillance, denunciation, and ideological enforcement through digital infrastructures.

3. Literature Review

Digital media have fundamentally transformed the dynamics of contemporary conflict by reshaping the production, circulation, and contestation of information (Castells, 2009; de Bruijn, 2025; Zeitzoff, 2017). Social media platforms and messaging applications have become key arenas where political legitimacy, public opinion, and conflict narratives are negotiated (Alsharairi et al., 2025; Caled & Silva, 2022). As a result, modern conflicts are increasingly fought not only through military operations but also through struggles over narratives, visibility, and symbolic power (Andrew & O'Loughlin, 2010; Barikov & Suleimenov, 2025; Marangé & Quessard, 2021; Velchev, 2025; Yarchi, 2025). Digital platforms simultaneously facilitate mobilisation, propaganda, surveillance, and resistance, while also accelerating misinformation, polarisation, and violence (Poupin, 2025; Tufekci, 2017). In conflict settings, they have become strategic instruments in the broader *weaponisation of information* (Douzet et al., 2014; Rid, 2020).

A growing body of scholarship examines computational propaganda and digital authoritarianism as mechanisms through which political actors shape online information environments. Woolley and Howard (2018) define computational propaganda as the strategic use of algorithms, automation, and coordinated communication to manipulate public opinion. While early research focused on bots, more recent studies emphasise the importance of coordinated human actors, influencers, and networked supporters (Boyer, 2025; Quessard, 2025). Similarly, research on digital authoritarianism demonstrates how governments use digital technologies for surveillance, censorship, and political control (Erixon & Lee-Makiyama, 2011; Feldstein, 2021; MacKinnon, 2011; Polyakova & Meserole, 2019), particularly during periods of political instability (Achinivu, 2025; Bosco et al., 2025; Hunter et al., 2026; Kermani, 2025).

African scholarship highlights similar dynamics. Mare (2020) analyses internet shutdowns and surveillance in Zimbabwe, while comparable practices have been documented in Chad, the Democratic Republic of Congo, Gabon, and Ethiopia (Ayalew, 2019; CIPESA, 2019). Across the continent, governments increasingly employ digital surveillance, biometric technologies, and restrictive regulatory frameworks to monitor communications and constrain dissent (CIPESA, 2022). Yet this literature primarily examines formal state mechanisms, paying less attention to politically aligned digital formations operating between state institutions and citizen participation.

Relevant insights emerge from studies of electronic armies and patriotic hackers. Leber and Abrahams (2019) show that online influence during the 2017 Gulf diplomatic crisis combined state intervention, influencers, automated accounts, and supportive publics (see also Abrahams & Leber, 2021). Jones (2019) similarly demonstrates that authoritarian influence operations involve diverse mixtures of trolls, bots, influencers, and coordinated amplification. Conduit (2024), examining Syria's patriotic hackers, argues that authoritarian digital mobilisation may be partly devolved to semi-autonomous actors whose relationship with the state remains ambiguous. These studies caution against equating textual similarity with centralised coordination, since repeated narratives may also emerge through imitation, affective mobilisation, or shared political vocabularies.

Another important strand of research concerns online harassment and digital violence. Digital platforms facilitate coordinated insults, threats, doxxing, and reputational attacks with significant social and political consequences (Citron, 2014; Goik, 2025; Posetti et al., 2021; Schoenebeck et al., 2023; Sekone, 2024).

Research shows that hostile campaigns are frequently collective rather than individual (Lewis et al., 2021; Marwick, 2021; Marwick & Caplan, 2018). Marwick and Lewis (2017) demonstrate how networked actors coordinate harassment through amplification, while Calloni (2025) highlights participation itself as a mechanism of coercion.

These dynamics can be understood through Papacharissi's (2015) concept of affective publics, whereby politically engaged users become connected through shared emotions and narratives rather than formal organisation. Related research on affective polarisation shows how emotional hostility deepens political divisions and legitimises antagonism toward opponents (Berntzen et al., 2024; Ferreira & Ferreira, 2025; Gidron et al., 2023; Iyengar et al., 2019). Likewise, the concept of cyberbalkanisation and research on echo chambers demonstrate how digital environments reinforce ideological clustering, shared identities, and hostile narratives (Chavalarias, 2022; Cinelli et al., 2021; Sunstein, 2008, 2009). In conflict settings, such environments encourage the emergence of coded expressions and militarised narratives that normalise hostility toward perceived enemies (Abondo Ndo, 2024; Etaywe & Giles, 2025; Morales, 2023; Villines, 2025).

Recent research on digital transnational repression further shows how surveillance, harassment, impersonation, and coordinated intimidation increasingly target exiled critics across borders (Brown et al., 2026; Freedom House, 2025; Michaelsen & Thumfart, 2023). At the same time, platform governance shapes the effectiveness of these practices. Facebook's infrastructural role in African information ecosystems (Nothias, 2020) and uneven trust, safety, and moderation enforcement illustrate how platform affordances can facilitate the circulation of context-specific coercive narratives (Research ICT Africa, 2023).

Existing concepts, including information disorder (Wardle & Derakhshan, 2017), propaganda (Cialdini, 2021; Ellul, 2008; Matz et al., 2017; Snow et al., 2024), digital authoritarianism, and networked harassment, illuminate important aspects of online political conflict but do not fully explain the configuration observed in Burkina Faso. The empirical evidence points to a hybrid formation that combines coordinated amplification, participatory harassment, militarised discourse, and symbolic coercion through a network of politically aligned actors operating between formal state authority and decentralised online participation. To capture this configuration, the article proposes the concept of cyber-militia.

4. Cyber-Militia: Toward a New Analytical Concept

This article introduces the concept of cyber-militia to analyse a networked and semi-structured formation of politically aligned digital actors and accounts mobilised against perceived political enemies. Such mobilisation may involve narrative amplification, targeting, intimidation, surveillance, reputational attacks, and symbolic coercion. The concept is deliberately behavioural rather than organisational. It identifies observable patterns of collective digital action without assuming that all participating accounts are authentic individuals, formally affiliated members, centrally coordinated, or operating under a defined state command structure.

This caution is important because influence operations may involve bots, pseudonymous accounts, sockpuppets, impersonation, commercially managed profiles, or actors located outside the apparent political community (Abrahams & Leber, 2021; Brown et al., 2026; Jones, 2019; Leber & Abrahams, 2019). As this study does not technically verify account authenticity, cyber-militia primarily describes observable networked behaviour rather than confirmed offline identities.

The use of cyber-militia in this article differs from Svantesson's (2023) conceptualisation of cyber militias as volunteer cyber-defence formations engaged in interstate warfare through cyberattacks, systems support, open-source intelligence, and information operations. The present study instead focuses on digitally mediated political coercion within domestic and transnational information environments. Cyber-militia, therefore, refers to actors and accounts involved in narrative enforcement, intimidation, collective denunciation, exposure of targets, and calls for punitive intervention.

The concept builds on scholarship on electronic armies (Abrahams & Leber, 2021) and patriotic hackers (Conduit, 2024). Authoritarian digital mobilisation may involve influencers, ideological supporters, trolls, automated accounts, and semi-autonomous political actors whose relationships with state institutions remain ambiguous (Conduit, 2024; Jones, 2019; Leber & Abrahams, 2019). The BIR-C occupies a similar space. Its campaigns often align with the narratives of Burkina Faso's military authorities and have received public political recognition ("Burkina: Hommage officiel," 2026; Ouedraogo, 2025); however, the available evidence does not establish a generalised state command structure.

It is, therefore, necessary to distinguish state direction, state alignment, and state legitimation. Direction implies demonstrable instruction, financing, control, or operational command. Alignment refers to convergence between digital activity and official political objectives. Legitimation occurs when authorities publicly recognise or praise pro-regime mobilisation. The evidence about BIR-C is considerably stronger for alignment and legitimation than for direct state control.

Cyber-militia should also not be understood as a formal, hierarchical organisation. The data reveal differentiated communicative roles. Some actors initiate accusations, others share and reproduce them, recurrent accounts sustain campaigns, and commenters intensify punitive demands. These roles indicate a distributed communicative division of labour, but do not prove fixed organisational positions or centralised control.

The same caution applies to coordination. Recurrent language, duplicated messages, shared framing, rapid amplification, and hostile comment threads are compatible with coordination, but may also result from imitation, organic virality, affective mobilisation, or shared political vocabulary. Demonstrating stronger orchestration would require evidence such as posting synchronisation, repetition latency, account-creation patterns, amplification networks, administrator relationships, or identifiable coordinating nodes. Cyber-militia, therefore, encompasses a spectrum from deliberate coordination to affectively mobilised participation.

The militia analogy remains useful because militias typically occupy an intermediate position between formal state forces and autonomous or anti-state actors. They may perform auxiliary functions involving surveillance, mobilisation, intimidation, policing, or the provision of support to political authority without being fully incorporated into state institutions (Møller, 2006). The analogy lies not in organisational equivalence but in a shared intermediary and coercive logic. Whereas conventional militias operate primarily in physical space, cyber-militias act mainly within informational and communicative environments.

In Burkina Faso, this logic is reflected in the name Brigade d'intervention rapide de la communication (BIR-C), which echoes the Bataillons d'intervention rapide (BIR) created after the 2022 military takeover. While the BIR operates against armed groups on the physical battlefield, the BIR-C frames the information

environment as another theatre of confrontation. Its discourse draws on vocabularies of vigilance, operations, capture, neutralisation, fronts, missions, and continuing mobilisation. Expressions such as *les opérations se poursuivent* (operations continue) and *mission accomplie* (mission accomplished) transpose the symbolic language of military action into political communication.

The analytical significance of this vocabulary lies in the militarisation of political communication, not in treating digital actors as literal soldiers. Critics, journalists, activists, exiles, and organisations are recast through a friend–enemy logic in which dissent is associated with terrorism, espionage, betrayal, foreign interference, or threats to national security. Once opponents are represented as security threats, calls for surveillance, investigation, punishment, exclusion, or apprehension can be normalised as defensive actions.

Cyber-militia thus intersects with computational propaganda, digital authoritarianism, electronic armies, affective publics, networked harassment, and participatory digital culture (Citron, 2014; Feldstein, 2021; MacKinnon, 2011; Papacharissi, 2015; Tufekci, 2017). It does not replace these concepts, but identifies a specific configuration of militarised, politically aligned networked participation organised around the identification, amplification, intimidation, and disciplining of perceived political enemies.

Cyber-militia can, therefore, be defined as a networked and semi-structured formation of politically aligned digital actors and accounts that mobilises against perceived political enemies through amplification, targeting, intimidation, surveillance, and symbolic coercion, while drawing on militarised repertoires of defence, vigilance, operations, and punishment. Its boundaries may remain fluid, and any relationship with the state—whether alignment, legitimation, or direct coordination—must be demonstrated empirically rather than assumed.

5. Methodology

5.1. Research Design

This study adopts a qualitative comparative case-study design (George & Bennett, 2005; Yin, 2018), combining digital content analysis with process tracing (Beach & Pedersen, 2019) to examine Facebook targeting campaigns associated with the BIR-C in Burkina Faso. A comparative design enables the identification of recurring mechanisms and variations across different target types rather than statistical generalisation (Ragin, 2014).

The analysis distinguishes discursive convergence from behavioural coordination. Narrative similarity alone is not treated as evidence of coordination because it may reflect imitation, organic diffusion, or shared political vocabulary. Instead, coordination is assessed through recurrent participation, parent-post/share relationships, exact-text repetition, temporal clustering, and operational vocabulary. Process tracing reconstructs the temporal relationship between online mobilisation and offline developments without assuming causality.

5.2. Case Selection and Data Collection

Three purposively selected cases represent distinct forms of digital targeting: (a) Didier Émile Kaboré, a civil-society activist (153 entries); (b) Newton Ahmed Barry, a journalist, former president of the national

electoral commission, and political exile (215 entries); and (c) the International NGO Safety Organisation (INSO; 100 entries). Together, the corpus comprises 468 Facebook entries.

Facebook was selected because of its central role in Burkina Faso's political communication. Data were collected in February 2026 from publicly accessible content. An entry refers to an original post, share, or individual comment. Corpus construction followed a case-bounded sampling strategy, limiting collection to material directly related to each campaign. Entries were retained when they contributed to accusation, amplification, delegitimisation, targeting, punitive mobilisation, or discussion of institutional or physical consequences. Duplicate captures were removed, while repeated texts appearing as separate posts, shares, or comments were retained because repetition itself constituted a potential coordination indicator.

5.3. Coding and Actor Classification

Each entry received one primary code—accusation, amplification, targeting/doxxing, delegitimisation, institutional/legal coercion, or contextual information—together with secondary indicators capturing operational vocabulary, calls to action, recurrent participation, exact-text repetition, parent-post relationships, temporal clustering, and transnational targeting where relevant.

Actors were classified independently of content into three categories: self-identified BIR-C actors, official institutional actors (e.g., government agencies and state media), and other or unverified participants. This distinction avoids inferring BIR-C membership solely from political alignment or participation in a campaign. Recurrent self-identified BIR-C accounts form an identifiable core, while a broader participatory periphery amplifies or reinforces campaigns without verifiable organisational affiliation.

5.4. Analytical Strategy and Limitations

Process tracing reconstructed key sequences linking online targeting with observable offline or institutional developments. The analysis identifies temporal ordering and escalation rather than causal relationships.

The study analyses observable digital behaviour rather than verified identities. It cannot determine whether accounts represent authentic individuals, bots, pseudonymous users, or externally managed profiles because no technical account-authenticity analysis was conducted. Likewise, political alignment is not treated as evidence of state direction. The findings, therefore, support conclusions about networked mobilisation and patterned amplification, but not about formal hierarchy or centralised command.

5.5. Ethics

The research relies exclusively on publicly accessible material concerning individuals and organisations already exposed to online targeting. To minimise harm, personal contact details and unnecessary identifying information were excluded, ordinary users were anonymised, and quotations were selected solely for their analytical relevance. The analysis distinguishes carefully between what the digital evidence demonstrates and what it only suggests, ensuring that claims about coordination and state involvement remain proportionate to the available evidence.

6. Results

6.1. Overview of the Comparative Corpus

The analytical corpus comprises 468 Facebook entries across three cases: Didier Émile Kaboré (153), Newton Ahmed Barry (215), and the INSO (100). Case 1 is a concentrated campaign from 13–21 April 2025; Case 2 extends episodically from June 2024 to September 2025; and Case 3 covers 7–8 October 2025. They represent three distinct targeting dynamics: rapid individual targeting, sustained reputational delegitimisation, and event-driven institutional targeting.

Across the cases, five mechanisms recur: accusation, amplification, participatory reinforcement, punitive demands, and militarised or operational vocabulary. The evidence indicates networked mobilisation and recurrent amplification rather than centralised command.

6.2. Networked Amplification and Observable Coordination

Amplification varies considerably across cases. Case 1 shows the strongest temporal concentration: All 153 entries occurred within nine days, including 112 on 20 April and 31 on 21 April. Sixteen accounts appeared repeatedly, while 44 entries reproduced identical text. These patterns demonstrate rapid networked amplification but not central orchestration.

Case 2 displays more sustained mobilisation. Its 215 entries comprise 54 original posts, 75 shares, and 86 comments. Behavioural coordination indicators appeared in 118 entries and content-level indicators in 82. Recurrent accounts, parent-post relationships, and exact-text repetition indicate continuity across successive targeting waves.

Case 3 requires more cautious attribution. Of 100 entries, eight originated from official government or public institutional accounts, two from explicitly BIR/BIR-C-associated accounts, and 90 from users or media whose affiliations could not be verified. Official accounts are not classified as BIR-C. Nevertheless, direct narrative transmission occurred when an RTB (Radiodiffusion Télévision du Burkina, the national broadcaster) publication was shared by the account BIR de l'AES and a Ministry of Security publication by the account BIR de la Communication. This demonstrates cross-actor transmission rather than institutional command.

6.2.1. Case 1: Escalation From Identification to Reported Apprehension

The targeting of Didier Émile Kaboré followed a compressed escalation sequence. On 13 April 2025, he was identified as the alleged administrator of a Facebook page critical of the military authorities. Subsequent comments discussed compiling a *dossier*, obtaining his telephone number, and placing him *hors d'état de nuire* (harmless). One participant wrote:

> *J'espère qu'il est déjà dans le sac…*
>
> (I hope he is already in the bag…)

Within the campaign, *dans le sac* referred to apprehension. On 20 April, posts circulated additional identifying information, including Kaboré's workplace, residence, and telephone number, while encouraging users to provide information to the authorities. One message explicitly linked exposure and capture:

> *Démasqué est différent de capturer. Mais une fois démasqué le processus de capturer est déclenché…*
>
> (Being unmasked is different from being captured. But once someone is unmasked, the process of capture is triggered…)

By 21 April, posts circulated claims that Kaboré had been apprehended. Expressions including *dans le sac* (in the bag), *mission accomplie* (mission accomplished), and *sac pimenté* (spicy bag) framed the reported outcome through operational and punitive vocabulary.

However, the circulation of these posts does not establish that the campaign caused Kaboré's apprehension, but demonstrates temporal and discursive proximity between digital targeting, punitive rhetoric, and subsequent claims of apprehension.

6.2.2. Case 2: Persistent Delegitimisation and Transnational Coercive Mobilisation

Case 2 differs through its duration and transnational dimension. Although Newton Ahmed Barry resides abroad, he remains a recurrent target within Burkina Faso's digital political sphere, portrayed as anti-patriotic, aligned with foreign interests, supportive of terrorism, or involved in destabilisation.

Primary coding identified 75 amplification entries, 71 delegitimisation entries, 41 accusations, 15 targeting/doxxing entries, and six instances of institutional/legal coercion. Multi-label coding additionally identified 66 accusation indicators, 21 targeting/doxxing indicators, 12 institutional/legal coercion indicators, 28 instances of operational vocabulary, 35 calls to action, and 22 transnational/Digital Transnational Rrepression indicators.

The recurrent phrase *Les opérations se poursuivent* (The operations continue) frames successive attacks as part of an ongoing undertaking. A particularly significant sequence occurred in April 2025. On 11 April, terrorism-related accusations were accompanied by questions about why arrest warrants had not been issued. On 22 April, an *APPEL AUX BURKINABÈ DE LA DIASPORA* (CALL TO BURKINABÈ IN THE DIASPORA) encouraged communities abroad to help locate targeted individuals. On 23 April, users circulated a purported official wanted list, including Barry, and again solicited diaspora assistance.

However, the dataset does not establish state direction of the BIR-C-associated campaign.

6.2.3. Case 3: Official Allegations and Networked Institutional Delegitimisation

Case 3 followed official espionage allegations against INSO and arrests involving its personnel. The 100-entry corpus comprises 19 original posts, 27 shares, and 54 comments. Eight entries originated from official state or public institutional accounts, explicitly excluded from the BIR-C network; five came from explicitly BIR/BIR-C-associated accounts; and 87 had unverified affiliations.

Official espionage narratives crossed actor categories through sharing before participants expanded suspicion from INSO to international NGOs more broadly.

Primary coding identified 32 institutional/legal coercion entries, 29 accusations, 27 amplification entries, eight delegitimisation entries, and one targeting/doxxing entry. Multi-label coding found 38 accusation indicators, 34 institutional/legal coercion indicators, 26 delegitimisation indicators, 21 instances of operational vocabulary, and 38 calls to action.

The expansion is illustrated by:

> *Il faut checker toutes les ONG inscrites à INSO.*
>
> (All NGOs registered with INSO need to be checked)

Other comments demanded investigation, suspension, expulsion, or punishment. Case 3, therefore, demonstrates how official narratives became source material for wider networked coercive mobilisation, without establishing either BIR-C-triggered state intervention or a unified state–BIR-C apparatus.

6.3. Comments, Operational Vocabulary, and Participatory Coercion

Across cases, comments functioned as active mechanisms of mobilisation. Participants repeated accusations, identified additional targets, proposed sanctions, encouraged dissemination, and intensified punitive demands. Coercive participation, therefore, did not depend on formal BIR-C membership; source posts could activate a broader participatory periphery.

Militarised vocabulary also recurred. Case 1 associated *démasquer* (unmasked/identified) with capture and *mission accomplie* (mission accomplished); Case 2 repeatedly invoked *les opérations se poursuivent* (the operations continue); and Case 3 employed vocabulary of vigilance, fronts, capture, and continuing operations. Such language recasts critics and organisations as security threats and makes coercive responses appear legitimate or routine. Shared vocabulary, however, remains a discursive indicator rather than proof of coordinated instructions.

6.4. Cross-Case Synthesis

Process tracing identifies three configurations, listed in Table 1.

These differences in escalation across the three cases caution against claiming that BIR-C campaigns cause state repression. Instead, they reveal a coercive information ecology in which official narratives, self-identified BIR-C actors, wider participatory amplification, digital intimidation, and formal coercive practices can intersect without evidence of hierarchical command.

The cases consequently reveal three operational logics: rapid escalation, persistent transnational targeting, and institutional delegitimisation. Across them, recurrent self-identified BIR-C actors provide evidence of continuity around an identifiable core, while a more fluid participatory periphery amplifies and intensifies

Table 1. Comparative patterns of escalation across the three cases.

Case	Escalation Pattern	Key Actions	Analytical Implication
Case 1: Didier Émile Kaboré	Identification → Exposure/Amplification → Claims of Apprehension	The target is publicly identified, personal information is circulated, online attention intensifies, and claims of apprehension are subsequently disseminated.	Demonstrates a rapid escalation from digital exposure to reported coercive outcomes, although no causal relationship is established.
Case 2: Newton Ahmed Barry	Persistent Accusation → Calls for Sanction → Diaspora Mobilisation → Wanted-List Amplification	Repeated accusations of terrorism and betrayal are followed by demands for legal action, mobilisation of diaspora communities to locate the target, and circulation of a purported wanted list.	Illustrates a transnational coercive repertoire in which digital targeting extends beyond domestic audiences without demonstrating direct state coordination.
Case 3: INSO	Official Security Allegation → BIR/BIR-C-Associated Amplification → Wider Punitive Mobilisation	Official security allegations are amplified by BIR/BIR-C-associated accounts and subsequently expanded by wider Facebook users into calls for investigation, sanctions, and broader scrutiny of NGOs.	Shows how official narratives can evolve into wider participatory coercion through cross-actor amplification, without demonstrating institutional integration or hierarchical command.

targeting narratives. This supports understanding cyber-militia as a networked and partially structured formation, while stopping short of claims of formal hierarchy, centralised command, or state direction.

7. Discussion

This study examined how digitally networked actors participate in identifying, delegitimising, and coercively targeting perceived political opponents in Burkina Faso. Across the three cases, the findings reveal an adaptive and militarised repertoire rather than a centrally organised digital army. Evidence is strongest for recurrent participation, patterned amplification, cross-actor narrative transmission, and coercive language, but does not establish formal hierarchy or direct state orchestration. Cyber-militia is, therefore, used as a relational and behavioural concept describing networked mobilisation through accusation, amplification, intimidation, surveillance, and punitive demands.

7.1. From "Electronic Armies" to Networked Cyber-Militia

The findings situate Burkina Faso within scholarship on state-aligned "electronic armies," patriotic hackers, trolling networks, and digital authoritarianism. Research from the Middle East demonstrates that authoritarian digital mobilisation can combine influencers, ideological supporters, automated accounts, semi-autonomous actors, and directly controlled operators (Conduit, 2024; Jones, 2019; Leber & Abrahams, 2019).

The Burkina Faso cases nevertheless caution against equating convergence with centralised command. Repeated narratives, exact-text reproduction, recurrent accounts, parent-linked amplification, and temporal clustering demonstrate networked mobilisation but may also reflect imitation, affective mobilisation, or shared political vocabulary. Importantly, several recurrent cross-case accounts publicly self-identify with the BIR-C, providing evidence of continuity around an identifiable core, though not of formal hierarchy.

The BIR-C thus occupies an intermediate space between formal institutions and autonomous political mobilisation. The evidence supports distinguishing state direction, state alignment, and state legitimation; direct state control is not demonstrated, whereas political alignment and public legitimation are more clearly observable.

7.2. Target Type and Differentiated Repertoires of Coercion

Cyber-militia practices vary according to target characteristics. Case 1 demonstrates rapid escalation, from Kaboré's identification and exposure to apprehension-oriented discourse and subsequent claims that he was *dans le sac* (apprehended). Case 2 involves persistent and transnational coercion, with Barry, who resides abroad, subjected to terrorism and betrayal accusations, legal–security framing, and diaspora mobilisation. Case 3 demonstrates institutional delegitimisation, as allegations against INSO expand into suspicion and punitive demands targeting international NGOs more broadly.

The repertoire is, therefore, adaptive: Domestic critics can be exposed, exiled opponents pursued across borders, and suspicion extended from individual organisations to entire institutional sectors.

7.3. Digital Transnational Repression and the Barry Case

The Barry case connects these practices to digital transnational repression, through which surveillance, harassment, doxxing, intimidation, and reputational attacks can reach exiles across borders (Brown et al., 2026; Freedom House, 2025; Michaelsen & Thumfart, 2023). Despite residing abroad, Barry remained embedded in Burkina Faso's digital political sphere. In April 2025, sustained accusations developed into explicit attempts to mobilise diaspora communities to help locate targeted individuals, producing a cross-border locating repertoire.

However, the evidence does not establish that Burkinabè authorities directed the BIR-C-associated campaign or that online targeting caused Barry's wanted-list designation. The case is better understood as an ecology of transnational repression, in which formal measures, politically aligned campaigns, recurrent amplifiers, and supportive publics may reinforce one another without demonstrable central coordination.

7.4. Participatory Coercion and Affective Publics

Comments across the cases function not simply as reactions but as mechanisms of targeting. Participants repeat accusations, identify targets, propose sanctions, intensify hostile framing, and transform narratives into punitive demands. This supports Papacharissi's (2015) concept of affective publics and research showing that networked harassment can emerge through collective participation without explicit instructions (Marwick, 2021).

The findings consequently suggest a core–periphery configuration. Recurrent self-identified BIR-C accounts constitute an identifiable core, while a more fluid periphery participates through sharing, commenting, repetition, and punitive mobilisation without verifiable organisational affiliation. Cyber-militia power may, therefore, derive partly from its ability to activate broader publics without formally incorporating them. This dynamic also resonates with research on affective polarisation (Berntzen et al., 2024; Ferreira & Ferreira, 2025; Gidron et al., 2023; Iyengar et al., 2019).

7.5. Militarised Lexicon and the Normalisation of Coercion

A distinctive cross-case feature is the militarisation of political communication. Expressions such as *les opérations se poursuivent* (operations continue) and *mission accomplie* (mission accomplished), alongside references to fronts, vigilance, and capture, recast digital participation through the vocabulary of security operations.

Such language redefines critics as targets, collaborators, infiltrators, or threats requiring neutralisation. Through repetition, humour, coded expressions, and collective endorsement, punitive responses can acquire normality and legitimacy (Abondo Ndo, 2024; Etaywe & Giles, 2025; Morales, 2023; Villines, 2025). Cyber-militia, therefore, captures the militarisation of participatory communication without implying that participants are literally soldiers.

7.6. Online and Offline Coercion: A Coercive Ecology Rather Than a Causal Chain

Process tracing demonstrates temporal and discursive relationships rather than direct causality. Case 1 progresses from identification and exposure to circulating claims of apprehension; Case 2 connects persistent delegitimisation, cross-border locating, and wanted-list designation; Case 3 reverses the sequence, with official security allegations preceding networked amplification.

These configurations constitute a coercive information ecology in which official institutions, recurrent digital actors, engaged publics, and platforms operate through distinct but potentially mutually reinforcing channels. Cyber-militia actors need not command state repression to matter politically. Their significance also lies in rendering particular individuals or organisations legitimate objects of suspicion, sanction, or exclusion.

7.7. Official Narratives and Cyber-Militia Amplification

Case 3 illustrates how official communication and BIR-C mobilisation can interact without being organisationally identical. Government information services, the Ministry of Security, and RTB (the national radio and television) are classified as official institutional actors, not BIR-C members. Yet their publications became source material for BIR-C-associated accounts and broader participants.

Participants expanded official allegations against INSO into punitive suspicion of international NGOs more generally, producing a coercive surplus beyond the original institutional narrative. This resembles Conduit's (2024) devolution of authoritarian digital activity, whereby politically useful mobilisation is undertaken by semi-autonomous actors outside formal state structures.

7.8. Facebook Affordances and Trust & Safety

Facebook actively structures these dynamics. Posts introduce accusations, shares circulate them, comments enable escalation, and persistent visibility facilitates recirculation. These affordances also create trust, safety, and moderation challenges because expressions such as *dans le sac* or *les opérations se poursuivent* acquire coercive meaning primarily through local political and linguistic context.

The study does not establish algorithmic amplification or failures by Meta to enforce particular policies. Rather, it identifies a structural compatibility between platform affordances and distributed coercive mobilisation, while highlighting the importance of contextual knowledge for detecting coded coercion.

7.9. Historical Continuities and the Specificity of Burkina Faso

The comparison with the CDRs situates the BIR-C within a Burkinabè history of participatory political defence (François, 2023; Lalsaga, 2020; Ziegler & Rapp, 1986). The argument is not that the BIR-C institutionally reproduces the CDRs, but that both mobilise citizens against actors represented as threats to a collective political project.

Digital infrastructures transform this repertoire through searchable profiles, screenshots, mass sharing, crowdsourced identification, comments, and transnational participation. The specificity of the Burkina Faso case consequently lies in the intersection of militarised rule, revolutionary historical repertoires, conflict-related security discourse, affective mobilisation, and platform-mediated participation.

8. Theoretical Contribution

Cyber-militia does not replace concepts such as electronic armies, digital authoritarianism, computational propaganda, or networked harassment. Rather, it provides a context-specific analytical extension.

Its contribution is threefold: It foregrounds the militarisation of participatory political communication; captures organisational ambiguity, whereby a self-identified core coexists with unverified amplifiers and affective publics; and locates digital coercion within a coercive information ecology connecting official narratives, semi-autonomous actors, publics, exiled targets, and platform infrastructures.

Cyber-militia thus captures a distinctive configuration of contemporary authoritarian communication: distributed coercive mobilisation that borrows the symbolic repertoire of military action while operating through the participatory infrastructures of social media.

9. Conclusion

This study examined how digitally networked actors target perceived political opponents in Burkina Faso through three comparative cases involving a civil society activist, an exiled journalist, and an international NGO. Rather than isolated instances of online harassment, the findings reveal a recurring repertoire of accusation, amplification, participatory intimidation, and militarised discourse that extends beyond persuasion to regulate the boundaries of legitimate political expression.

The article introduces cyber-militia as an analytical concept to capture politically aligned digital formations operating between formal state institutions and decentralised online participation. The evidence supports a core–periphery configuration, with recurrent self-identified BIR-C actors forming an identifiable core surrounded by a broader participatory network. However, the findings do not establish formal hierarchy, direct state command, or centralised organisational control. Instead, they point to varying degrees of state alignment and public legitimation, underscoring the importance of distinguishing these from state direction.

The study has several limitations. It examines three purposively selected cases based on publicly available Facebook content and does not include private platforms or technical analyses of bots, coordinated inauthentic behaviour, or network structures. Nor does process tracing demonstrate causal links between online campaigns and offline events.

Future research should combine network analysis, digital forensics, and interviews to better understand cyber-militia organisation and coordination. Comparative studies across Africa and the Global South, as well as research on the gendered dimensions of cyber-militia activity, would further advance the understanding of cyber-militia activities.

Funding

This work is funded by the Norwegian Research Council (NRC) as part of the Decoding Digital Media in African regions of Conflict (DDMAC) project. Project number: 325123.

Conflict of Interests

The authors declare no conflicts of interests.

Data Availability

Data are available upon request.

LLMs Disclosure

Copilot and Grammarly were used to improve and correct language, as well as translate between languages.

References

Abondo Ndo, W. S. (2024). Digital shifts and ethno-political dynamics: Examining event and actor designation in the Cameroon Boko Haram terrorism conflict through print and online platforms. *Journalism and Media*, *5*(1), 359–381. https://doi.org/10.3390/journalmedia5010024

Abrahams, A., & Leber, A. (2021). Electronic armies or cyber knights? The sources of pro-authoritarian discourse on Middle East Twitter. *International Journal of Communication*, *15*, 1173–1199.

Achinivu, C. (2025, October 28). Nigeria's government is using digital technology to repress citizens. A researcher explains how. *The Conversation*. https://theconversation.com/nigerias-government-is-using-digital-technology-to-repress-citizens-a-researcher-explains-how-267032

Alsharairi, A., Al-Souob, H. A.-R., AlQadi, M. F., & Shatnawi, S. M. (2025). Social media communication and framing of the Gaza conflict: Impact on public opinion. *Journal of Intercultural Communication*, *25*(3), 73–82. https://doi.org/10.36923/jicc.v25i3.1153

Andrew, H., & O'Loughlin, B. (2010). *War and media: The emergence of diffused war*. Polity.

Ayalew, Y. E. (2019). The internet shutdown muzzle(s) freedom of expression in Ethiopia: Competing narratives.

Information & Communications Technology Law, *28*(2), 208–224. https://doi.org/10.1080/13600834.2019.1619906

Barikov, A., & Suleimenov, I. (2025). Theoretical bases of methods of counteraction to modern forms of information warfare. *Computers*, *14*(10), Article 410. https://doi.org/10.3390/computers14100410

Beach, D., & Pedersen, R. (2019). *Process-tracing methods: Foundations and guidelines* (2nd ed.). University of Michigan Press. https://doi.org/10.3998/mpub.10072208

Beraud, B. (2026, April 17). Burkina Faso: La journaliste Yousra Elbagir accusée de "propagande" après son interview d'Ibrahim Traoré. *TV5 Monde*. https://information.tv5monde.com/international/burkina-faso-la-journaliste-yousra-elbagir-accusee-de-propagande-apres-son-interview-dibrahim-traore-2818040

Berntzen, L. E., Kelsall, H., & Harteveld, E. (2024). Consequences of affective polarization: Avoidance, intolerance and support for violence in the United Kingdom and Norway. *European Journal of Political Research*, *63*(3), 927–949. https://doi.org/10.1111/1475-6765.12623

Bosco, D., Colombo, L., & Femminis, G. (2025). Conflict, information and regime-change. *European Journal of Political Economy*, *89*, Article 102681. https://doi.org/10.1016/j.ejpoleco.2025.102681

Boyer, B. (2025). Opérations d'information et lutte informationnelle: Permanence et défis. *Revue Défense Nationale*, *876*(1), 20–26. https://doi.org/10.3917/rdna.876.0020

Brown, R., Scott, M., Michaelsen, M., Dirk, E., & Thaler, F. (2026). *Tall tales. How Chinese actors use impersonation and stolen narratives to perpetuate digital transnational repression*. The Citizen Lab. https://citizenlab.ca/research/how-chinese-actors-use-impersonation-and-stolen-narratives-to-perpetuate-digital-transnational-repression

Burkina: Création de six bataillons d'intervention rapide. (2022, November 16). *Studio Yafa*. https://www.studioyafa.bf/5756-burkina-creation-de-six-bataillons-dintervention-rapide

Burkina: Hommage officiel aux BIR-C. (2026, August 3). *APAnews*. https://fr.apanews.net/security/burkina-hommage-officiel-aux-bir-c

Burkina Faso: Disparition forcée des défenseurs de droits humains Miphal Ousmane Lankoandé et Amadou Sawadogo. (2025, May 2). *Fédération internationale des droits humains*. https://www.fidh.org/fr/themes/defenseurs-des-droits-humains/burkina-faso-disparition-forcee-des-defenseurs-de-droits-humains

Burkina Faso: Liberté d'expression en péril sous le poids de la crise politique. (2025, May 10). *Media Foundation for West Africa*. https://mfwa.org/fr/issues-in-focus/burkina-faso-liberte-dexpression-en-peril-sous-le-poids-de-la-crise-politique

Burkina Faso Digital Report 2025: Les statistiques d'internet, des médias sociaux, de la téléphonie mobile, du e-commerce et l'inclusion financière. (2025, March 10). *Digital Magazine Burkina*. https://digitalmagazine.bf/2025/03/10/burkina-faso-digital-report-2025-les-statistiques-dinternet-des-medias-sociaux-de-la-telephonie-mobile-du-e-commerce-et-linclusion-financiere

Caled, D., & Silva, M. J. (2022). Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, *5*(1), 123–159. https://doi.org/10.1007/s42001-021-00118-8

Calloni, M. (2025). Polarization and enmity in the algorithmic age. Striving for a digital ethos of relationality and pluralism. *Philosophy & Social Criticism*, *51*(4), 672–692. https://doi.org/10.1177/01914537251327724

Castells, M. (2009). *Communication power*. Oxford University Press.

Chams, S. (2025, April 7). Journalisme au Burkina Faso: Se soumettre ou disparaître. *AfriqueXXI*. https://afriquexxi.info/Journalisme-au-Burkina-Faso-se-soumettre-ou-disparaitre

Chavalarias, D. (2022). *Toxic data. Comment les réseaux manipulent nos opinions*. Flammarion.

Cialdini, R. B. (2021). *Influence: The psychology of persuasion* (revised ed.). Harper Business.

Cinelli, M., Morales, G. D., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, *118*(9), Article e2023301118. https://doi.org/10.1073/pnas.2023301118

CIPESA. (2019). *Despots and disruptions: Five dimensions of internet shutdowns in Africa*. https://cipesa.org/wp-content/files/briefs/report/Despots-And-Disruptions_March-20.pdf

CIPESA. (2022). *Digital authoritarianism and democratic participation in Africa*. https://cipesa.org/wp-content/files/briefs/Digital-Authoritarianism-and-Democratic-Participation-in-Africa-Brief-.pdf

Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.

Conduit, D. (2024). Digital authoritarianism and the devolution of authoritarian rule: Examining Syria's patriotic hackers. *Democratization*, *31*(5), 979–997. https://doi.org/10.1080/13510347.2023.2187781

Coup d'État au Burkina Faso: Le lieutenant-colonel Damiba renversé par le capitaine Ibrahim Traoré. (2022, October 3). *France 24*. https://www.france24.com/fr/%C3%A9missions/journal-de-l-afrique/20221003-coup-d-%C3%A9tat-au-burkina-faso-le-lieutenant-colonel-damiba-renvers%C3%A9-par-le-capitaine-ibrahim-traor%C3%A9

de Bruijn, M. (2025, October 14). Digital communication as a weapon: The case of Mali. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2025/10/digital-communication-as-a-weapon-mali

Douzet, F., Desforges, A., & Limonier, K. (2014). Géopolitique du cyberespace : « territoire », frontières et conflits. In F. Guérin-Pace, P. Beckouche, & Jean-Yves Moisseron (Eds.), *CIST2014—Fronts et frontières des sciences du territoire*, *Collège international des sciences du territoire (CIST)* (pp. 173–178). GIS Collège international des sciences du territoire (CIST). https://hal.science/hal-01353455v1/file/cist2014_geopolitique_du_cyberespace_territoire_frontieres_conflits.pdf

Elbagir, Y. (2026, April 10). Inside the secretive country run by a military leader with a cult following. *Sky News*. https://news.sky.com/story/the-young-military-leader-strengthening-relations-with-russia-and-china-13529478

Ellul, J. (2008). *Propagandes*. Economica. (Original work published 1962)

Erixon, F., & Lee-Makiyama, H. (2011). *Digital authoritarianism: Human rights, geopolitics, and commerce* (ECIPE Occasional Paper No. 5/2011). European Center for International Political Economy. https://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf

Etaywe, A., & Giles, H. (2025). Relational dynamics in violent extremist incitement communication: Language as bonds, obligations, and a catalyst for polarisation. *Discourse & Communication*, *19*(6), 911–950. https://doi.org/10.1177/17504813251378884

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Ferreira, G. B., & Ferreira, L. S. (2025). The polarization paradox: Social media, young voters, and the challenges to the open society. *Social Sciences*, *14*(9), Article 542. https://doi.org/10.3390/socsci14090542

François, T. (2023). Édifier l'État par la kalach. Les Comités de défense de la Révolution de Ouagadougou et le maintien de l'ordre. *Politique africaine*, *170*, 63–83. https://doi.org/10.3917/polaf.170.0063

Freedom House. (2025). *Collaboration and resistance: Tracking transnational repression in 2025*. https://freedomhouse.org/sites/default/files/2026-04/FH_TransnationalRepression2026_final%20%281%29.pdf

Friis Hau, M. (2025). Like, share, lead: The impact of social media on authority and legitimacy in the labor movement. *Social Media + Society*, *11*(2). https://doi.org/10.1177/20563051251337869

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Gidron, N., Adams, J., & Horne, W. (2023). Who dislikes whom? Affective polarization between pairs of parties

in Western democracies. *British Journal of Political Science*, *53*(3), 997–1015. https://doi.org/10.1017/S0007123422000394

Goik, A. T. (2025). Addressing cyber harm in the age of platform power: Comparative insights into legal, technical and educational responses. *Peking University Law Journal*, *13*(2), 145–164. https://doi.org/10.1080/20517483.2026.2618383

Gouba, F. (2024). Activisme numérique et engagement citoyen au Burkina Faso: Entre nouvelles opportunités et reconfigurations du rapport au politique. *Revue Ivoirienne des Sciences du Langage et de la Communication*, *18*, 590–606.

Hunter, L. Y., Topping, K., & Hosny, Y. (2026). Online government disinformation, censorship, and civil conflict in authoritarian regimes. *Media, War & Conflict*, *19*(3), 631–655. https://doi.org/10.1177/17506355225135157

Iyengar, S., Lelkes, Y., Levendusky, M., Malhotra, N., & Westwood, S. J. (2019). The origins and consequences of affective polarization in the United States. *Annual Review of Political Science*, *22*, 129–146. https://doi.org/10.1146/annurev-polisci-051117-073034

Jones, M. O. (2019). Propaganda, fake news, and fake trends: The weaponization of Twitter bots in the Gulf crisis. *International Journal of Communication*, *13*, 1389–1415.

Kemp, S. (2026). *Digital 2026: Burkina Faso*. DataReportal. https://datareportal.com/reports/digital-2026-burkina-faso?rq=Burkina%20Faso

Kermani, H. (2025). The art of delirium: Social media suppression in authoritarian regimes. *Communication Theory*, *35*(4), 197–213. https://doi.org/10.1093/ct/qtaf006

Lalsaga, K. M. (2020). *État, révolution et transition démocratique au Burkina Faso: Le rôle des structures populaires révolutionnaires de l'avènement de la Révolution Démocratique et Populaire (RDP) à la restauration de la République* [Unpublished doctoral dissertation]. Université Joseph Ki-Zerbo.

Leber, A., & Abrahams, A. (2019). A storm of tweets: Social media manipulation during the Gulf crisis. *Review of Middle East Studies*, *53*(2), 241–258. https://doi.org/10.1017/rms.2019.45

Lewis, R., Marwick, A. E., & Partin, W. C. (2021). "We dissect stupidity and respond to it": Response videos and networked harassment on YouTube. *American Behavioral Scientist*, *65*(5), 735–756. https://doi.org/10.1177/0002764221989781

MacKinnon, R. (2011). Liberation technology: China's "networked authoritarianism." *Journal of Democracy*, *22*(2), 32–46.

Marangé, C., & Quessard, M. (2021). *Les guerres de l'information à l'ère numérique*. Presses Universitaires de France.

Mare, A. (2020). State-ordered internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication*, *14*, 4244–4263.

Marwick, A. (2021). Morally motivated networked harassment as normative reinforcement. *Social Media + Society*, *7*(2). https://doi.org/10.1177/20563051211021378

Marwick, A., & Caplan, R. (2018). Drinking male tears: Language, the manosphere, and networked harassment. *Feminist Media Studies*, *18*(4), 543–559. https://doi.org/10.1080/14680777.2018.1450568

Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation online*. Data & Society Research Institute. https://datasociety.net/wp-content/uploads/2017/05/DataAndSociety_MediaManipulationAndDisinformationOnline-1.pdf

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, *114*(48), 12714–12719. https://doi.org/10.1073/pnas.1710966114

Michaelsen, M., & Thumfart, J. (2023). Drawing a line: Digital transnational repression against political exiles and host state sovereignty. *European Journal of International Security*, *8*(2), 151–171. https://doi.org/10.1017/eis.2022.27

Møller, B. (2006). *The role of militias and other paramilitaries in African (un)civil wars* (DIIS Working Paper Vol. 2006 No. 23). Danish Institute for International Studies. https://pure.diis.dk/ws/portalfiles/portal/74735/WP2006_23_web.pdf

Morales, E. (2023). Ecologies of violence on social media: An exploration of practices, contexts, and grammars of online harm. *Social Media + Society*, *9*(3). https://doi.org/10.1177/20563051231196882

Nothias, T. (2020). Access granted: Facebook's free basics in Africa. *Media, Culture & Society*, *42*(3), 329–348. https://doi.org/10.1177/0163443719890530

Ouedraogo, S. (2025, October 8). Burkina Faso-BIR-C et «Wayiyan»: Sentinelles de la Révolution en cours et piliers de la souveraineté nationale. *Aconews*. https://aconews.net/burkina-faso-bir-c-et-wayiyan-sentinelles-de-la-revolution-en-cours-et-piliers-de-la-souverainete-nationale

Ouedraogo, S. (2026, March 5). Burkina Faso/Edito: Wayignan et BIR-C, digue protectrice de la Révolution Progressiste Populaire. *Aconews*. https://aconews.net/burkina-faso-edito-wayignan-et-bir-c-digue-protectrice-de-la-revolution-progressiste-populaire

Papacharissi, Z. (2015). *Affective publics: Sentiment, technology, and politics*. Oxford University Press.

Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Posetti, J., Shabbir, N., Maynard, D., Bontcheva, K., & Aboulez, N. (2021). *The chilling: Global trends in online violence against women journalists*. UNESCO.

Poupin, P. (2025). Mobilization and dissent on blogs and social media. In F. Daucé, B. Loveluck, & F. Musiani (Eds.), *Digital authoritarianism in the making* (pp. 165–190). MIT Press.

Quessard, M. (2025). De la lutte informationnelle à l'arme cognitive: Seuils d'escalade et recompositions stratégiques dans les conflictualités hybrides. *Revue internationale et stratégique*, *140*, 113–123. https://doi.org/10.3917/ris.140.0113

Ragin, C. C. (2014). *The comparative method: Moving beyond qualitative and quantitative strategies*. University of California Press.

Research ICT Africa (2023). Digital platform governance and the challenges for trust and safety. https://researchictafrica.net/wp-content/uploads/2023/02/part-2-deals-with-the-how-with-a-focus-on-platforms-policies-and-practices.pdf

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus, & Giroux.

Sawadogo, W. (2015). Insurrection populaire et communication. *Politique Africaine*, *140*, 115–132.

Schoenebeck, S., Lampe, C., & Triệu, P. (2023). Online harassment: Assessing harms and remedies. *Social Media + Society*, *9*(1). https://doi.org/10.1177/20563051231157297

Sekone, R. J. (2024). *Radicalisation et extrémisme violent en ligne: Analyse et prévention*. Mercury Editions.

Snow, N., Jowett, G. S., & O'Donnell, V. (2024). *Propaganda & persuasion* (8th ed.). Sage.

Sunstein, C. R. (2008). Neither Hayek nor Habermas. *Public Choice*, *134*, 87–95. https://doi.org/10.1007/s11127-007-9202-9

Sunstein, C. R. (2009). *Republic.com 2.0*. Princeton University Press.

Svantesson, D. J. (2023). Regulating a "cyber militia"—Some lessons from Ukraine, and thoughts about the future. *Scandinavian Journal of Military Studies*, *6*(1), 86–101. https://doi.org/10.31374/sjms.195

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.

Une journaliste de Sky News cible d'une campagne de dénigrement par les propagandistes d'Ibrahim Traoré (2026, April 17). *France24*. https://www.france24.com/fr/afrique/20260417-journaliste-sky-news-cible-campagne-d%C3%A9nigrement-propagandistes-ibrahim-traore-burkina-faso

Velchev, A. (2025). The role of media and technology in contemporary warfare. *Journal of Information Policy*, *15*, 171–196. https://doi.org/10.5325/jinfopoli.15.2025.0007

Villines, G. (2025). *From crowds to code: Algorithmic echo chambers and the normalization of coercive suppression in political life*. SSRN. https://doi.org/10.2139/ssrn.5584211

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe. https://rm.coe.int/information-disorder-report-november-2017/1680764666

Woolley, S. C., & Howard, P. N. (Eds.). (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press.

Yameogo, L. (2020). Activisme en ligne et transformations sociopolitiques au Burkina Faso. *Communication*, *37*(2). https://doi.org/10.4000/communication.13232

Yarchi, M. (2025). Strategic narratives as an image war tool. *Place Branding and Public Diplomacy*, *22*, 531–538. https://doi.org/10.1057/s41254-025-00418-0

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.

Yingi, E., & Benyera, E. (2025). The future of democracy in the digital era: Internet shutdowns, cyber laws and online surveillance in Zimbabwe. *Alternatives: Global, Local, Political*, *50*(2), 283–297. https://doi.org/10.1177/03043754241259878

Zeitzoff, T. (2017). How social media is changing conflict. *Journal of Conflict Resolution*, *61*(9), 1970–1991. https://doi.org/10.1177/0022002717721392

Ziegler, J., & Rapp, J.-P. (1986). *Thomas Sankara. Un nouveau pouvoir africain*. Pierre-Marcel Favre/ABC.

About the Authors



Samba Dialimpa Badji is a doctoral researcher in journalism and media studies at Oslo Metropolitan University, Norway. His research focuses on disinformation and fact-checking in the context of conflicts, focusing on Ethiopia and Mali. His work also examines journalism practices and digital repression in the Sahel.



Harouna Drabo is a PhD candidate in the geopolitics of cyberspace, specialising in information-based influence operations in the Sahel. His work focuses on deciphering the geopolitical dynamics underpinning influence strategies, specifically by examining the tactics, techniques, and processes of information manipulation and analysing networks of domestic and foreign actors.