African Journal of Security and Strategic Studies
Volume 1, Issue 1, February 2026

*Date Received: 24th July 2025; Date Accepted: 13th January 2026*

# Use and Misuse of Social Media and National Security in Africa: A Delicate Balance between Order and Liberty in Kenya

*June R Ruto, Emily Okuto & Israel Nyadera*

**Abstract**

Social media activism in Africa presents both opportunities and risks. It promotes transparency, accountability, and civic engagement, but also generates misinformation, polarization, and security threats. In Kenya, campaigns such as #RejectFinanceBill2024 have demonstrated how online mobilization can strengthen democratic participation but also escalate to unrest when fueled by disinformation and incitement. This study examines the impact of social media activism on national security in Kenya between 2014 and 2024, focusing on three objectives: how social media facilitates activism that threatens security, the correlation between online activism and security breaches, and the effectiveness of government interventions. Anchored in Social Movement Theory, Network Theory, and Securitization Theory, the study employed a descriptive design, random sampling of 384 social media users and purposive sampling of 10 experts, and mixed data collection through semi-structured questionnaires and interviews. Descriptive and thematic analysis revealed that platforms such as X, TikTok, Facebook, and WhatsApp are central to both civic mobilization and the spread of hate speech, propaganda, and cyber threats. Correlation tests showed strong associations between online activism and violent protests as well as between activism and the unintentional spread of misinformation. While government responses, ranging from legislation to digital surveillance, aimed to contain these risks, they have often sparked public contestation for undermining freedoms. The study concludes that safeguarding Kenya's national security requires balanced regulatory frameworks, platform-specific co-regulation, digital literacy initiatives, and real-time crisis communication, measures that address genuine threats without eroding constitutional rights.

**Keywords:** Social Media, Misinformation, Activism, National Security, Kenya

## Introduction

The media as the public watchdogs and the Fourth Estate have the core responsibility of reliably informing the public, and providing citizens with the information needed to make informed decisions about leadership and policy (Mpofu, 2023; Collins, 2025). As public informers and educators, the media sets the agenda for public discussion, and provides a platform for political expression (McCombs & Valenzuela, 2020). Information dissemination has largely been dictated by traditional mass media institutions' agenda-setting and gate-keeping powers, especially in print and television journalism. These media were viewed as the twentieth century's "public sphere," where political discourse occurs and public opinion is created (Çela, 2015; Kaiser et al., 2018).

However, the influx of social media in the 21st-century has significantly revolutionized communication regarding access, freedom of information, and promotion of public discourse.

[1] **Contact:** zuri.chiri@gmail.com: National Defence University-Kenya.

Nonetheless, these positive gains have come with several challenges, particularly with respect to context-bound governance domains both within and among states.

Since the Arab Spring phenomenon in the early 2010s, contentious debates and concerns regarding the use and/or abuse of digital space and the likely implications of the same on national security and stability have emerged (Haj, 2016). Against this background, this paper critically examines ways through which social media-based activism can have potentially harmful outcomes for national security. It further explores actionable strategies for regulating social media and AI usage to ensure national security, in a manner that protects human rights, civil liberties and other democratic gains in Kenya.

**Methodology**

The study adopted a descriptive research design that integrated quantitative and qualitative strands in a convergent approach. This choice was informed by the need to capture both measurable patterns of social media use and activism, as well as deeper experiential insights from experts and documentary sources. The quantitative component entailed a structured survey of 384 social media users, which provided the basis for descriptive statistics and correlation analysis between online activism and national security outcomes. The qualitative component consisted of semi-structured key informant interviews with ten purposively selected subject-matter experts, supplemented by a systematic desk review of scholarly and policy literature using the PRISMA framework.

This design ensured that the study combined the strengths of numerical generalization and thematic interpretation, thereby aligning with the stated objectives and addressing the complexity of the social media–security nexus.

The study focused on the decade between 2014-2024. This is an important period for this study because it covers two successive governments and an increase in social media use especially by youths for political activism. Our focus was mostly on Facebook, X (Formerly Twitter, Instagram and Telegram, which are the leading social media platforms for youths in Kenya. The study population comprised of youths (above 18 but below 35) social media users in Kenya who were active on at least one major platform during the twelve months preceding the study, with Nairobi serving as the focal site due to its high internet penetration, concentration of civic mobilization, and relevance to national policy debates. The data was drawn from publicly available Facebook groups, X hashtag streams, and Telegram or Instagram forums dealing with civic or political issues. For this group, probability sampling was applied: a list of eligible accounts was compiled, duplicates were removed, and systematic random sampling with a fixed interval was used to generate invitations. Where initial contacts failed to respond, pre-identified alternates were substituted to preserve randomness. To determine the sample size for social media users using simple random sampling, the study applies the widely used sample size formula (Krejcie & Morgan, 1970):

$$n = \frac{Z^2 * p * (1 - p)}{e^2}$$

where:

- n = required sample size,
- Z = Z-score associated with the desired confidence level (for 95% confidence level, Z≈1.96Z),

- p = estimated proportion of the population possessing the characteristic of interest (we use 0.5 when the proportion is unknown, to maximize sample size),
- e = margin of error (often set at 5%, or 0.05 for this study).

Calculation:

1. Plugging the values into the formula:

$$n = \frac{(1.96)^2 * 0.5 * (1 - 0.5)}{0.05^2}$$

2. Simplifying further:

$$n = \frac{3.8146 * 0.2}{0.0025}$$

$$n = \frac{0.9604}{0.0025}$$

n = 384.16

3. Rounding up, we get a sample size of approximately 384 social media users.

The qualitative sample of subject-matter experts was identified purposively to reflect diverse perspectives relevant to the study. These included two digital space experts such as regulators or industry practitioners, two national security personnel including officers from cybercrime or policy units, two policymakers or regulators, two social media activists with a history of civic mobilization, and two media or communication scholars. Selection was guided by professional experience of at least three years in roles directly linked to digital communication, security, or governance. This purposive approach recognized that expertise rather than representativeness was central to the qualitative inquiry, in contrast with the probability procedures applied to the quantitative survey.

Data collection methods and instruments were clearly distinguished. For the survey, the method was a cross-sectional online survey while the instrument was a structured questionnaire composed of closed and open-ended items, including Likert-type scales. For the qualitative strand, the method was key informant interviewing and the instrument was a semi-structured interview guide that allowed probing while retaining comparability across respondents. For the desk review, the method was systematic documentary analysis and the instrument was a PRISMA extraction form used to screen, select, and code peer-reviewed articles, government reports, and policy documents. This clarification avoids conflating methods with tools, a common weakness in poorly specified methodologies.

Survey administration was conducted via online platforms such as Google Forms, with invitations distributed to the sampled accounts. Measures such as captcha filters, IP checks, and duplicate elimination were employed to minimize bot responses or multiple entries. The key informant interviews were conducted either face-to-face or through secure online platforms, lasting between 45 and 60 minutes. All interviews

were audio-recorded with prior consent, transcribed verbatim, and anonymized through role codes rather than names to ensure confidentiality. The PRISMA-based review proceeded through identification, screening, eligibility, and inclusion phases, with a transparent audit trail maintained for replicability.

Data analysis followed a dual track aligned with the mixed-methods design. Quantitative data were coded and analysed using statistical software, generating descriptive statistics and Pearson correlation coefficients to test associations such as between online activism and violent protest participation, and between activism and inadvertent spread of misinformation. Qualitative data were analysed thematically following Braun and Clarke's six-step approach: familiarization, coding, theme generation, review, definition, and reporting. Dual-coder checks were applied to a portion of transcripts to enhance intercoder reliability, and themes were triangulated with quantitative patterns and documentary insights. The integration of both strands occurred at the interpretation stage, where quantitative findings were explained, qualified, or challenged by qualitative narratives.

## Literature Review

### *Social Media in Perspective: A Global View*

Social media has revolutionized global political and civic life by offering direct, mass communication and interactive platforms that connect individuals and communities at unprecedented scales (Chami, 2025; Boulianne, 2019). Platforms such as Facebook, X (formerly Twitter), TikTok, Instagram, WhatsApp, and Telegram provide users with easy access to information and the ability to circulate images, videos, and commentary in real time, thereby amplifying agendas and inspiring political movements (Chakma, 2024; Klinger et al., 2023). Youth are the largest demographic of users, capitalizing on smartphones and globalized communication networks to spearhead digital activism and challenge entrenched political structures (Hngokchai, 2025; Imoka, 2023).

Globally, social media has fuelled major civic and political protests that have reshaped governance debates. The Arab Spring (2010–2011), Hong Kong's Umbrella Movement (2014), Zimbabwe's "This Flag" protests (2016), France's Yellow Vests (2018–2019), Black Lives Matter (2020), and Nigeria's End SARS (2020) exemplify movements coordinated online to mobilize against injustice (Jost et al 2018; Chinemerem, 2025; Nwakanma, 2022). In Kenya, the #RejectFinanceBill2024 protests in June 2024 followed a similar trajectory, demonstrating how online spaces increasingly serve as civic infrastructure for collective action (Mwangi, 2025; Arzani, 2025). Beyond protests, digital campaigns have propelled anti-establishment political leaders such as Barack Obama, Donald Trump, Jair Bolsonaro, Boris Johnson, Giorgia Meloni, Javier Milei, and William Ruto, all of whom harnessed social media to galvanize popular support (Flew & Iosifidis, 2020).

Social media has also proven effective in advocacy and online petitions, where hashtag campaigns have directly shaped policy reforms and justice outcomes. The #MeToo movement in the US produced millions of posts, led to workplace harassment reforms, and established legal defence funds for victims, while #JusticeforGeorgeFloyd catalyzed protests and prosecution for racial injustice (Heydemann & Tejani, 2019). Similarly, #BringBackOurGirls drew global attention to Boko Haram's kidnappings in Nigeria, pressuring both national and international actors to respond (Oriola, 2024). These cases illustrate social media's ability to amplify civic voice and pressure institutions into action.

However, this transformative potential is accompanied by darker risks. Extremist and terrorist groups such as Al Qaeda, ISIS, and Al Shabaab have exploited social media to radicalize and recruit vulnerable youth, undermining national and global security (Darden, 2019; Menkhaus, 2013). Online spaces have also facilitated the spread of misinformation, hate speech, and conspiracy theories, exacerbating ethnic and religious polarization and eroding social cohesion (Arifah et al 2025). Governments, especially in multicultural societies, have adopted regulatory frameworks to compel social media companies to moderate harmful content, though such efforts often generate tensions over free speech and censorship.

Despite originating in the United States and Europe, social media's reach has expanded eastward through platforms such as TikTok, WeChat, and Telegram, with global adoption now standing at 69 percent of the world's population and 95 percent of internet users (Kamath et al, 2012). The largest platforms include Facebook (2.26 billion users), TikTok (2.05 billion), YouTube (1.9 billion), WhatsApp (1.33 billion), Instagram (1 billion), and Telegram (700 million), reflecting their centrality in modern life (Binitie & Odetayo, 2024). Africa, however, remains the least penetrated region, with only 10 percent coverage in Eastern Africa compared to 75 percent in Asia, 71 percent in North America, and 80 percent in Europe, though penetration is rising in Southern and Northern Africa (Cariolle, 2021).

***Evolution of the Social Media Space in Kenya***

Social media, emerging in the early 2000s with pioneers such as MySpace, Hi5, and Friendster, has since transformed into a global ecosystem dominated by platforms like Facebook, YouTube, X (formerly Twitter), WhatsApp, Instagram, and TikTok (Singh & Singh, 2025). These platforms revolutionized communication by enabling entertainment, networking, and large-scale information sharing, connecting diverse communities across the globe. Kenya quickly integrated into this wave, with online communities originally centred on personal sharing and leisure evolving into spaces for civic and political engagement. From 2013 onwards, Kenyan social media shifted decisively toward politics, with parties recruiting bloggers, fundraising online, and running targeted digital campaigns during the 2013, 2017, and 2022 elections (Abboud et al., 2024). Kenya's comparatively advanced economy in the region supported this expansion, with 13 million active users, 24 percent of the population, despite internet coverage reaching 41 percent (Otieno & Anyuor, 2024).

Kenya's democratization gains have further empowered both political actors and citizens to harness digital platforms for mass communication and mobilization (Opiyo et al 2017). President William Ruto's 2022 victory illustrated the growing centrality of social media campaigns, while civil society and ordinary citizens increasingly seized digital spaces to push for accountability. Notably, youth-driven online activism surged during the COVID-19 pandemic and intensified during the 2024 anti-Finance Bill protests, where "Gen Z" mobilized leaderless digital movements that spilled into the streets with disruptive force (Osman, 2025).

Indeed, these movements were marked by online sloganeering, caricatures of leaders, and targeted cyberbullying, indicating both the democratizing and destabilizing potentials of social media. The proliferation of artificially generated or manipulated content, breaches of privacy, and even treasonous messaging reflect escalating governance challenges. As such, Kenya's experience demonstrates how social media activism can enhance participation and accountability while simultaneously presenting significant risks to national security, requiring nuanced strategies that balance regulation with democratic freedoms.

### *The Delicate Terrain of 'Governing' the Internet and Social Media*

Regulatory approaches to internet and social media governance vary across political systems (Rochefort, 2020). Consolidated democracies such as those in Western Europe have prioritized frameworks for content regulation and moderation, compelling social network companies to comply while preserving participation, transparency, and security (Flew et al., 2019). In contrast, authoritarian regimes often resort to disruptive measures including censorship, surveillance, crackdowns on dissent, and outright internet shutdowns, which undermine rights to free speech and access to information. While regulation is necessary to curb abuses, repressive approaches freeze democratic ideals, harm economies, and erode accountability. Taxation on social media use, arbitrary arrests, and invasive surveillance discourage civic discourse and compromise privacy (Głowacka et al., 2021). Yet the unregulated use of digital platforms has facilitated criminality, misinformation, and threats to critical infrastructure. Globally, 156 countries have enacted cybercrime legislation, with Europe leading at 91 percent adoption, while Africa lags at 72 percent. Notably, nine of the world's 13 countries without cybercrime laws are in Africa (Council of Europe, 2025, February).

Enforcement in democracies illustrates balanced accountability. France's September 2024 arrest of Telegram CEO Pavel Durov prompted reforms aligning the platform with EU rules against extremist content (Berchin, 2025). Similarly, in the UK, inflammatory social media posts fueling the 2024 Southport riots led to mass arrests and prosecutions, which indicates the delicate balance between safeguarding freedoms and protecting national security (Casciani, 2024).

### *On the State of Social Media Regulation in Kenya*

Kenya has made notable progress in developing cyberspace laws to govern online activity and protect digital rights. The Computer Misuse and Cybercrimes Act (2018) criminalized cyberterrorism, harassment, fraud, and identity theft while safeguarding the availability, integrity, and confidentiality of data and computer systems. This was followed by the Data Protection Act (2019), which strengthened privacy protections and established regulatory oversight through the Office of the Data Protection Commissioner. Complementing these is the Kenya Information and Communications Act, which regulates telecommunications and digital media. These laws apply broadly, to private citizens, journalists, researchers, and organizations, underlining Kenya's intention to ensure safe and accountable online spaces (Mutua & Yanqiu, 2021).

Despite this progress, gaps remain in regulating harmful political activity online. Current laws primarily treat the internet as a communication space, not a locus of political mobilization. As such, thresholds for prosecuting "offensive" or "distasteful" political content remain ambiguous, while boundaries around legitimate activism versus unlawful extremism are ill-defined. This ambiguity has contributed to tensions between security agencies and activists, including allegations of arbitrary arrests, which fuel public mistrust. The rise of the Gen Z movement in 2024 exemplifies these shortcomings. Kenya's securitization trajectory highlights the urgent need to balance freedoms with security through clear, consensus-driven frameworks that protect rights while addressing extremist misuse (Kizito, 2024).

### *The Digital Activism-National Security Nexus*

A major puzzle facing security agencies worldwide is how to regulate online-driven political movements without infringing on democratic freedoms. Unlike conventional protests that are organized through identifiable leaders and formal structures, digital activism is often leaderless, formless, and transnational.

Movements such as Kenya's "Gen Z" mobilizations epitomize this unpredictability, where viral, decentralized networks create both opportunities for civic participation and vulnerabilities to malicious elements spreading incitement. The Arab Spring demonstrates this paradox most vividly: online activism toppled authoritarian regimes but also unleashed chaos in Libya, Syria, and Yemen, where leaderless mobilization degenerated into militancy, civil war, and long-term instability (Frenkel et al., 2018).

Social media's borderless nature compounds the risk by creating contagion effects across regions. The viral circulation of Tarek el-Tayeb Mohamed Bouazizi's self-immolation in Tunisia on December 17, 2010, catalysed regional uprisings, with Facebook and Twitter amplifying discontent against entrenched regimes. What began as democratic aspiration devolved into violent insurgencies and counterinsurgencies in Egypt, Yemen, and Syria, illustrating how digital activism can morph into destabilization when institutions fail to channel grievances constructively. In Kenya, the June 2024 anti-Finance Bill protests mirrored these tendencies, where online mobilization by youth escalated into leaderless street demonstrations characterized by violence. Similarly, online mobilizations in 2025 have brought down governments in Bangladesh, Nepal and Madagascar.

Perhaps the gravest danger lies in the spread of hate speech, radicalization, and violent extremism through social media. Online platforms have been exploited to incite ethnic, racial, and religious hostility, eroding social cohesion. Incidents such as the 2018 Pittsburgh synagogue shooting, linked to anti-Semitic online propaganda, and the 2015 Charlie Hebdo attack in France indicate the global consequences of digital hate (Marwick & Lewis, 2017). In Africa, Al-Shabaab and other extremist groups continue to exploit Facebook, YouTube, Telegram, and Twitter to radicalize vulnerable youth, recruit fighters, and disseminate propaganda. These risks are particularly acute in Kenya, where the youth constitute the majority of social media users and remain susceptible to extremist narratives.

Governments also face the challenge of managing misinformation and disinformation that undermine policy interventions. During the COVID-19 pandemic, conspiracy theories about "depopulation" vaccines and "globalist control" spread virally online, fueling resistance to public health measures and eroding trust in institutions (de Lira, (de Lira et al., 2024). This dynamic illustrates the delicate balance. While social media enhances free expression, it simultaneously tests the resilience of law enforcement, the legitimacy of government communication, and the stability of democratic order. For Kenya, as elsewhere, the nexus between digital activism and national security thus lies in navigating this fine line, harnessing the civic potential of social media while mitigating its destabilizing effects.

***The Knowledge Gap***

The intersection of social media and national security has become an urgent field of inquiry as digital platforms increasingly shape political behaviour, societal cohesion, and the stability of state institutions. In Kenya, as elsewhere, social media is both a space for civic engagement and a domain vulnerable to exploitation through misinformation, incitement, and unrest, yet there are very few studies that have examined the nexus between social media use and national security. This study uses Kenya as a case study to examine the delicate balance between order and liberty in the evolving digital sphere. The authors argue for the broadening of interventions through content moderation and public–private collaboration, while also evaluating the variety and effectiveness of government strategies in mitigating risks posed by social media activism.

## Theoretical Framework

Three interconnected theories, that is social network theory, social movement theory, and securitization theory, adequately provide the best analytical framework for the social media phenomenon and its likely implications on national security. The social network theory accounts for the aspect of centrality, positing that social interactions have instrumentalized communication innovations to shape information sharing, the channelling of media, and personal influence, as well as behaviours and attitudes. On the other hand, the social movement theory explains the emergence of the political movement online, given that its primary focus is on how social interactions and connections or interrelationships build communities among people (Peterson, 1989; Owen, 2017).

According to social movement theory, it can be deduced that social media combines its connective and interactive to build social movements in two ways: First, it provides the internet-based communication (expression) platform as a resource for activists and organizers who suffer financial resource scarcity (Eltantawy & Wiest, 2011). Secondly, it provides an accessible form of citizen journalism (away from traditional journalism), which hands down an expression platform and information sources to individuals, activists and consumers, social movement founders and followers, respectively (Owen, 2017).

The securitization theory (Buzan & Wæver, 2009) on its part, aptly captures the struggle to identify unregulated social media usage as a security threat and to address this challenge with new legislation, policies, and regulations to ensure national security in Kenya. The theory posits that security is socially constructed; hence, a phenomenon becomes a security threat only when identified by politicians and governments and subjected to similar public debate to generate social consensus to elevate it as a security issue and manage it accordingly (Otukoya, 2024).

## Findings and Discussion

This part presents the findings of the study, integrating both **descriptive and thematic content analysis** to provide a comprehensive understanding of the collected data. Quantitative data obtained from survey responses are analysed using descriptive statistics, while qualitative data from Key Informant Interviews (**KIIs)** are examined through thematic analysis.

### *Usage of Social Media Platforms*

The findings presented in Figure 1 below provide insights into the most frequently used social media platforms among study respondents, offering a basis for assessing their role in digital activism and security risks. The findings illustrate the distribution of social media platform usage among respondents. **WhatsApp (81.6%)** emerged as the most frequently used platform, followed by **TikTok (58.0%)**, **Facebook (50.2%)**, **X (Twitter) (48.2%)**, and **Instagram (48.2%).** Other platforms such as **Telegram (26.3%)** and **alternative networks like Reddit, LinkedIn, and Pinterest (8.2%)** had lower engagement levels.

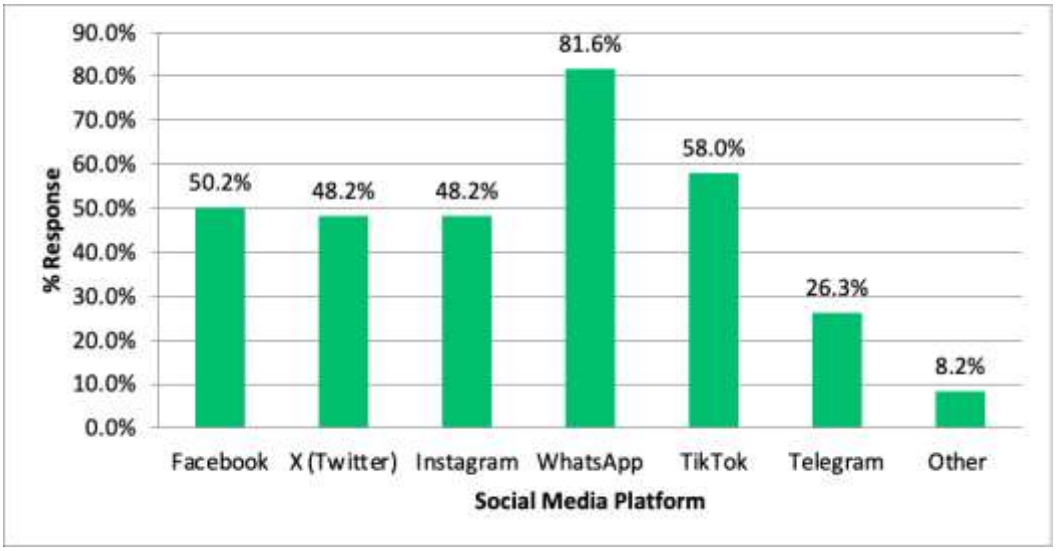


**Figure 1: Frequency of Social Media Platform Use**

The prominence of WhatsApp as the leading platform in Kenya aligns with global and regional findings that encrypted messaging applications play a critical role in grassroots (Trauthig et al., 2024). Yet the very architecture that fosters trust and rapid circulation also enables disinformation, hate speech, and extremist messaging (Kumar, & Maurya, 2024). TikTok's growing prominence (58.0%) illustrates how algorithm-driven, short-form video content energizes younger demographics, lowering participation thresholds but amplifying unchecked narratives (Abidin, 2021). Facebook (50.2%) and X/Twitter (48.2%) remain critical arenas for agenda-setting and real-time mobilization, though both have been implicated in election interference and manipulation (Bradshaw & Howard, 2019). Telegram (26.3%) plays a more specialized role in secure communication, while LinkedIn, Reddit, and Pinterest (8.2%) serve niche audiences (Scheibe, 2024).

Social network theory helps explain why WhatsApp and Telegram are so effective, whereby dense, trust-based networks accelerate circulation but reduce verification and transparency (Mlika et al, 2024). Social movement theory clarifies TikTok's and Facebook's appeal, showing how low-cost, high-visibility platforms sustain "connective action" without formal leadership (Eltantawy & Wiest, 2011; Rucht, 2023). Finally, securitization theory explains why governments frame these platforms as existential threats, citing hate speech, cyber mobilization, and covert coordination as justifications for surveillance, regulation, and content moderation (Buzan & Wæver, 2009).

***Participation in Social Media Activism***

The survey shows in Figure 2**,** that 73.1% of respondents have participated in or observed social media activism, confirming the centrality of digital platforms in Kenya's civic life. This mirrors wider African cases such as #FeesMustFall in South Africa and #EndSARS in Nigeria, where online mobilization has become a mainstream form of participation, challenging traditional protests while introducing governance and security dilemmas (Omilusi, 2025). Social movement theory explains this dynamic by showing how digital platforms lower resource barriers, enabling mobilization, citizen journalism, and "connective action" without strong organizational structures (Rucht, 2023). Social network theory further clarifies how influencers and viral content act as central nodes that synchronize participation across dispersed populations

(Theodorakopoulos et al., 2024). Securitization theory highlights the state's dilemma, whereby activism is a democratic right, yet its leaderless and emotionally charged nature increases risks of disorder, prompting governments to frame it as a security concern.

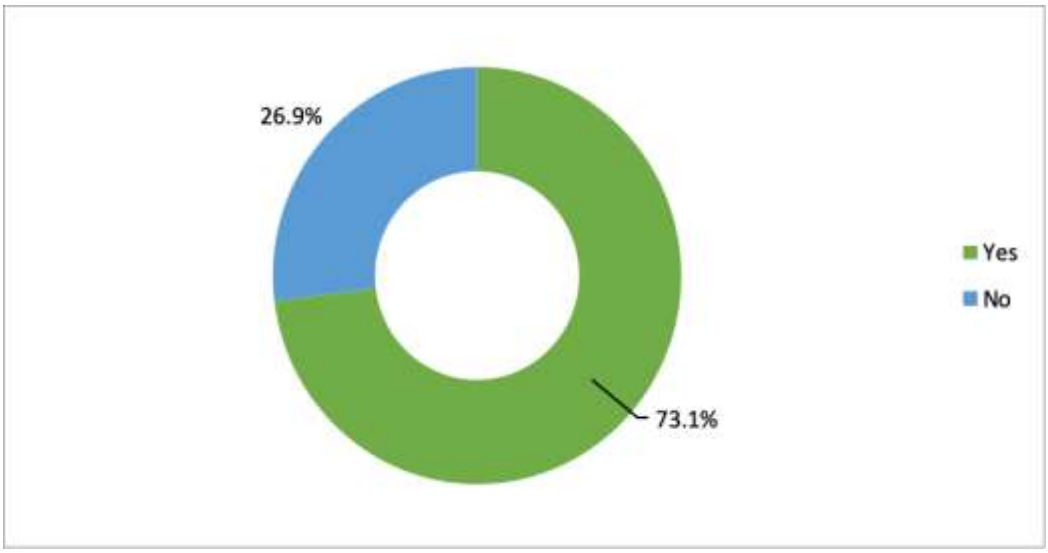


**Figure 2: Participation in Social Media Activism**

***Influence of Social Media Platforms on Public Mobilization***

The survey identifies in Figure 3, X/Twitter (52.1%) as the most influential platform for mobilization, followed by TikTok (22.5%), Facebook (8.9%), WhatsApp (7.5%), Instagram (4.2%), and Telegram (1.4%). This hierarchy reinforces scholarship describing X/Twitter as a hub for real-time activism, agenda-setting, and protest coordination (Segerberg & Bennett, 2011; Meikle, 2024). Interviews validate this perception, whereby one expert emphasized that "*Twitter and Facebook are the most instrumental; they can quickly ignite mass communication that overwhelms formal information channels*," while an activist described X as "*the megaphone of our generation, if you want people on the streets tomorrow, you start on Twitter today*." These testimonies align with literature linking Twitter to movements such as #EndSARS, #FeesMustFall, and #JusticeForKianjokomaBrothers (Mpofu, 2024; Ondimu et al., 2025). Social network theory clarifies why, whereby influencers, hashtags, and trending topics act as high-centrality nodes that synchronize dispersed actors around grievances.

TikTok's rise (22.5%) marks a generational shift. A producer noted, "*TikTok is different, it is live, it's visual, and it speaks the language of the youth in a way text cannot*." This resonates with studies showing how TikTok's algorithm amplifies emotionally charged narratives (Schellewald, 2022). Social movement theory explains this appeal, whereby TikTok lowers participation thresholds and enables "connective action" through audiovisual self-expression, especially among Gen Z, now central to Kenya's protest culture.

By contrast, Facebook (8.9%) and WhatsApp (7.5%) appear to be losing their earlier centrality. One respondent observed, "*Facebook used to be where activism lived, but now it feels slower and older, Twitter and TikTok move faster*." Literature confirms this shift, noting Facebook and WhatsApp's roles now lean toward private coordination and background communication (Donovan, 2021). Telegram (1.4%), though

marginal, raises security concerns. A security expert warned, "*Telegram and Signal are belligerent spaces… hard to monitor.*" This echoes securitization theory, where states frame encrypted platforms as risks of extremism or covert radicalization (Buzan & Wæver, 2009; Otukoya, 2024).

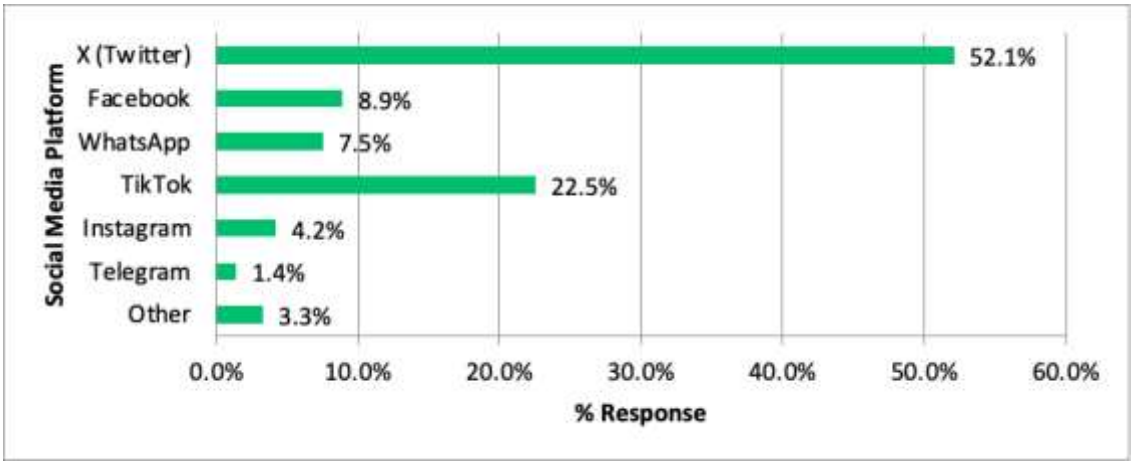


**Figure 3: Most Influential Social Media Platforms**

***Potential National Security Risks of Social Media Activism***

The study highlights multiple risks linked to social media activism in Kenya, foremost among them misinformation and disinformation. Respondents warned of "*misinformation, vendetta campaigns, deliberate agenda-setting posts*," while a civic educator noted, "*It is becoming more difficult to verify what is actual, especially with AI…the speed at which disinformation spreads is a key challenge*." These concerns echo evidence from African elections where falsehoods distorted debates and fuelled instability (Abdulazeez et al., 2025). Social network theory explains this pervasiveness, whereby dense digital communities accelerate circulation but weaken verification, amplifying unverified narratives.

Incitement and radicalization also emerged as pressing concerns. A security expert observed that platforms "*make it very easy to carry out massive political mobilization*" while fueling "*hate speech, propaganda, and communicative balkanization*." Social movement theory clarifies this paradox, whereby while platforms enable connective action, their openness also facilitates radicalizing discourses and leaderless escalation. Cybersecurity threats were another key theme. Respondents cited "*cybersecurity threat, mobilization*" and "*leakage of confidential data*," while experts described repeated attacks on Kenya's iTax system and citizen service portals. Such cases align with findings on the intersection of activism, cyberterrorism, and hostile digital operations (Bradshaw & Howard, 2019). Securitization theory illuminates why states frame these threats as existential, justifying surveillance and regulation.

***Potential National Security Benefits of Social Media Activism***

The study finds that social media activism, rather than being purely destabilizing, also generates significant security and democratic benefits in Kenya. Respondents emphasized its role in rapid information dissemination, noting that platforms "*help to pass information and create awareness*" and can serve as an "*early-warning mechanism in times of crisis*." Activists further stressed that "*activism cannot, by definition, be a threat to national security,*" indicating its role in defending rights and exposing corruption, consistent with evidence that online networks function as watchdogs of accountability (Howe & Haigh, 2016).

Social movement theory explains why these benefits emerge. Lowering barriers to participation enables platforms to enhance "connective action" where grassroots voices scale national debates, evident in Kenya's 2024 anti-Finance Bill protests (Tarrow, 2011; Tufekci, 2017). Social network theory adds that central influencers and civic bodies accelerate accountability content and alerts (Castells, 2012). Securitization theory clarifies how states, when engaging proportionately, can reframe activism as a co-producer of security using digital footprints, open-source intelligence, and citizen reporting to enhance forensic capacity and crisis management (Buchanan, 2020; Buzan et al., 1998).

***Correlation Between Instances of Social Media Activism and Specific Instances of National Security Breaches in Kenya***

The results presented in Table 1 reveal a strong and statistically significant positive relationship between participation in social media activism and participation in protests that turned violent. The Pearson correlation coefficient of r = .758, with a p-value of .000, indicates a robust association at the 0.01 significance level. This suggests that individuals who are more actively engaged in online activism are also more likely to have participated in physical protests that escalated into violent incidents. The correlation between online activism and violent protests resonates with respondents' accounts and with the wider literature. A national-security expert noted that social media "*makes it very easy to carry out massive political mobilization*," while activists stressed that platforms like X/Twitter are now the "megaphone of our generation." This finding echoes Earl et al. (2022) and Ali's (2025) analysis that digital platforms act as accelerants of collective action, compressing the time between online dissent and physical mobilization. Social movement theory adds that movements relying on loosely connected digital structures are prone to escalation, since they mobilize large numbers without robust leadership mechanisms to de-escalate tensions. The strong correlation therefore illustrates not causation but a theoretically expected pathway; rapid diffusion, fast turnout, and heightened risk of volatility when grievances lack institutional resolution.

**Table 1: Correlation between Participation in Online Activism and Engagement in Violent Protests**

| | | Participation in Social Media Activism | Participation in protests that turned violent |
|---|---|---|---|
| Participation in Social Media Activism | Pearson Correlation | 1 | .758** |
| | Sig. (2-tailed) | | .000 |
| | N | 262 | 262 |
| Participation in protests that turned violent | Pearson Correlation | .758** | 1 |
| | Sig. (2-tailed) | .000 | |
| | N | 262 | 262 |

**. Correlation is significant at the 0.01 level (2-tailed).

The correlation coefficient presented in Table 2 below ($r = .621$, $p < .001$) indicates a strong and statistically significant positive relationship between the two variables. The association between activism and the spread

of misinformation also emerged strongly in both survey data and interviews. A civic educator noted, "*It is becoming more difficult to verify what is actual, especially with AI…the speed at which disinformation spreads is a key challenge*." Another respondent warned of "*misinformation, vendetta campaigns, deliberate agenda-setting posts*." This aligns with Petratos (2021) who ranks misinformation among the top ten global risks for governance, and Mare et al, (2019), who shows how encrypted platforms have amplified disinformation in African contexts.

The strong correlation between activism and violent protest participation explains why states can be tempted to frame digital contention as a national-security issue, using a securitization lens and legitimizing surveillance, internet shutdowns, or activist arrests. Yet interviewees, particularly activists and digital content producers, counter-framed this position, arguing that "*activism cannot, by definition, be a threat to national security*" and attributing escalation to police brutality rather than online organizing. This contestation reflects the core tension in securitization. Whether civic dissent is framed as a democratic right or an existential danger. Empirically, the literature indicates how governments across Africa securitize digital contention in ways that erode trust, from internet shutdowns in Uganda to surveillance crackdowns in Ethiopia (Thumfart, 2024).

**Table 2: Participation in Social Media Activism and Unknowingly Participating in Misinformation**

| | | Participation in Social Media Activism | Participation in misinformation unknowingly |
|---|---|---|---|
| Participation in Social Media Activism | Pearson Correlation | 1 | .621** |
| | Sig. (2-tailed) | | .000 |
| | N | 262 | 262 |
| Participation in misinformation unknowingly | Pearson Correlation | .621** | 1 |
| | Sig. (2-tailed) | .000 | |
| | N | 262 | 262 |

**. Correlation is significant at the 0.01 level (2-tailed).

***Perceived Contribution of Social Media Platforms to Security Risks in Kenya***

Survey data in Figure 4 show that respondents perceived X/Twitter (59.4%) as the most risk-prone platform, followed by TikTok (41.1%), Facebook (28.6%), Telegram (22.3%), WhatsApp (18.9%), and Instagram (10.3%). These rankings map onto well-documented affordances. X/Twitter's virality and hashtag culture amplify misinformation and hate speech (Marwick & Lewis, 2017); TikTok's short-form videos encourage unverified content spread (Molina et al., 2021); Facebook has a history of election-cycle manipulation in Kenya; WhatsApp's encrypted groups facilitate unchecked rumour cascades (Ndlela, 2020); and Telegram has been linked to extremist propaganda (Walther & McCoy, 2021). KIIs reinforced these perceptions, whereby a security expert noted that "*Twitter and Facebook are the most instrumental; they can quickly ignite mass communication,*" while cautioning that TikTok and WhatsApp also magnify risks, though

YouTube is less abused due to stricter moderation. An activist, however, stressed that "*activism should not be conflated with fraudulent activities*," drawing attention to the line between advocacy and misuse.

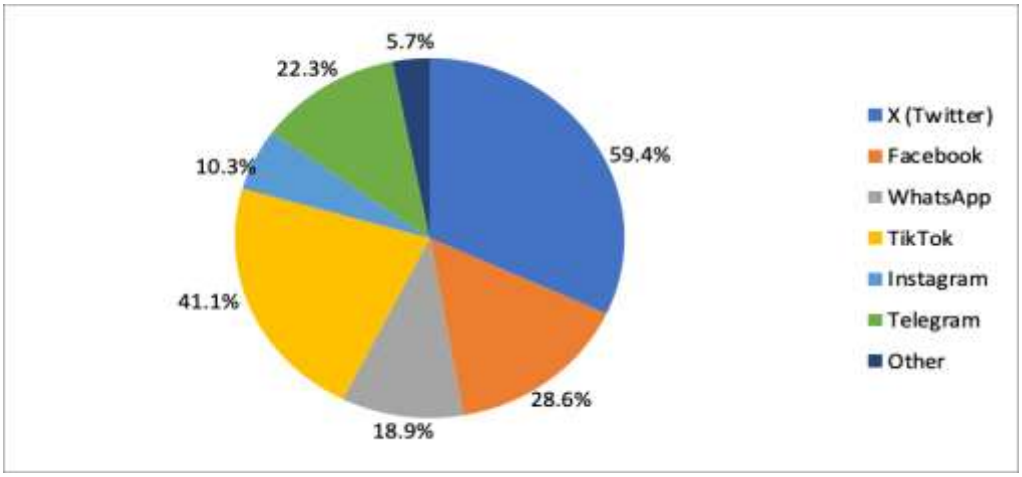


**Figure 4: Perceived Contribution of Social Media Platforms to Security Risks**

The data and testimonies highlight three sub-themes. Mass-broadcast platforms (X/Facebook) drive visibility; encrypted apps (Telegram) enable covert coordination; and contested boundaries separate activism from criminal manipulation. Social network theory clarifies why open, broadcast-oriented platforms are perceived as high-risk. Central nodes like influencers and trending hashtags accelerate diffusion, increasing the probability of incendiary content reaching critical mass. Encrypted clusters (WhatsApp/Telegram) create opacity, explaining mid-tier risk perceptions despite smaller audiences. Social movement theory adds that low-cost, connective action allows emotionally charged narratives to spread faster than verification, matching respondents' concern about "mass communication" and covert use of encrypted apps. Finally, securitization theory explains the governance dilemma. High perceived risks incentivize authorities to frame platforms as security threats, justifying surveillance and regulation. Yet, as the activist's perspective underlines, over-securitization risks collapsing legitimate dissent into criminality, undermining democratic freedoms.

***Emerging Tendencies in Social Media Use During Critical Security Incidents***

The emerging tendencies in social media use during critical security incidents in Kenya illustrate a dual-use dynamic that the quantitative results, KIIs, and empirical literature confirm. The survey showed that platforms like X/Twitter (59.4%) and TikTok (41.1%) are perceived as the riskiest, and these are precisely the platforms highlighted in interviews as channels through which live operational details are leaked or real-time mobilization occurs. The national security expert's observation that "*people even tweet…you are not helping anybody*" illustrates the operational risks of disclosure, a pattern echoed in literature that identifies Twitter's virality as both a driver of civic mobilization and a liability during crises. Conversely, the same expert acknowledged that agencies like the DCI benefit from citizen reporting and tips via social media, a finding that resonates with survey evidence of respondents highlighting platforms as early-warning and real-time reporting systems, and with literature documenting social media's positive role in horizon scanning and crisis response.

Encrypted apps such as Telegram present another challenge. Quantitatively, 22.3% of respondents perceived Telegram as a risk-prone platform, and interview data indicated its role in "*operating below the radar*," making it hard for governments to detect and track misinformation or covert coordination. This aligns with research showing how extremist groups exploit encrypted channels for propaganda and mobilization (Erbschloe, 2018). At the same time, the expert's recognition of TikTok's distinctiveness "*it does not have lag-time in communication*" corroborates the survey's finding that TikTok is rising in influence, and literature that points to its audio-visual immediacy and algorithm-driven virality as tools of youth-driven activism (Nicolla et al., 2023).

The theoretical framework helps interpret these patterns. Social network theory explains how central nodes and dense clusters in broadcast platforms like X/Facebook amplify both legitimate reporting and harmful leaks, while encrypted groups create verification deficits that fuel covert threats. Social movement theory clarifies why audio-visual, low-cost, high-visibility platforms like TikTok enable connective action during security crises, rapidly mobilizing younger demographics without formal structures. Securitization theory then accounts for the state's reactions, whereby the widespread perception of platforms as threats, for example, X at 59.4%, leads governments to frame them as security issues, thereby legitimizing surveillance, shutdowns, or regulation. Yet, as the interviews also stressed, over-securitization risks conflating legitimate activism with criminal misuse, undermining trust and eroding freedoms.

***Suggested Strategies for Better Managing Security Risks while Protecting Digital Rights***

The study finds that respondents consistently advocate a balanced, multi-pronged strategy to mitigate security risks while safeguarding digital rights. Regulation was a recurring theme, with participants urging government to "enact or strengthen laws against hate speech and misinformation" and to take "serious measures against perpetrators," yet cautioning that excessive control would only drive citizens to VPNs and proxies. This dual emphasis reflects literature showing that digital platforms both empower civic participation and destabilize politics when unchecked (Sharma et al., 2022). Securitization theory explains this tension, in that, while states may frame online harms as existential threats, proportionate regulation sustains legitimacy rather than eroding it.

Cybersecurity and digital literacy also ranked highly. Respondents insisted that "*government should invest fully in cybersecurity education*," echoing expert calls for firewalls, tele-tracking, and public education. These priorities resonate with evidence of Kenya's rising cyberattack exposure (Njoroge, 2020). Social network theory clarifies why these measures matter. In dense networks, rapid diffusion outpaces verification, so equipping citizens and strengthening infrastructure slows harmful cascades.

Mistrust in government communication emerged as another driver of unrest, as noted by a respondent: "*The problem is not social media but rather how the government communicates*." Linked calls for real-time messaging ("*Government communication must be real-time*". Public participation reinforced this message, "*Work with the people and not against them*." These perspectives reflect social movement theory, which argues that connective action is more governable when co-produced with activist networks. Other recommendations addressed root causes "*set up industries and provide employment to the youths*", is aligned with thoughts that tie socio-economic grievances to digital unrest. Finally, emphasis on ethical leadership and rights-based activism indicates securitization theory's caution that conflating activism with threats risks criminalizing dissent and undermining democratic freedoms

**Discussion**

This study affirms the dual role of social media activism as both a catalyst for civic engagement and a source of national security risks. The #RejectFinanceBill2024 protests illustrate this paradox. Indeed, this is consistent with existing literature which show that social media platforms provide unprecedented opportunities for mobilization while simultaneously amplifying misinformation, incitement, and cyber threats. Such threats are increasingly being recognised with the government of Kenya in 2023 acknowledging that social media now shapes political discourse in ways that can bolster accountability or destabilize governance.

The study also finds that cybersecurity threats emerged as a significant dimension. Respondents cited "*cybersecurity threat, mobilization*" and "*leakage of confidential data*," while the national-security expert pointed to repeated attacks on iTax and Huduma systems. What is being observed in Kenya is consistent with growing cases of extremists exploitation of these platforms from cyberterrorism with Kenya being a good case study for growing vulnerability to hacking and fraud. The Communications Authority (CA, 2023) has reported a sharp rise in cybercrime targeting activists, journalists, and state platforms. Social network theory explains why these risks proliferate. Dense, open networks accelerate diffusion, including malicious content, while encrypted channels such as Telegram amplify opacity.

Misinformation and disinformation were consistently ranked the most dangerous risks. One civic educator observed, "*It is becoming more difficult to verify what is actual, especially with AI. The speed at which disinformation spreads is a key challenge*." Respondents warned of vendetta campaigns and "*deliberate agenda-setting posts*." These perspectives are consistent with Marwick and Lewis (2017), who document how false narratives exploit algorithmic virality to distort public debates. At the same time, respondents highlighted national-security benefits. Activists emphasized that social media "*helps to pass information and create awareness*" and serves as "*an early-warning mechanism in times of crisis*." The DCI's crowd-sourced interventions in crime cases exemplify how platforms can support real-time intelligence. Social movement theory explains how low-cost, high-visibility platforms like TikTok and Twitter sustain grassroots oversight, while social network theory clarifies how centrality accelerates the diffusion of watchdog content. Securitization theory further shows that proportional engagement, transparent communication, timely updates, and collaboration with civil society can transform activism from threat to co-production of security.

Policy recommendations emerging from these findings stress balance. Respondents called for stricter regulation of hate speech and misinformation but cautioned against "serious measures that would only drive users to VPNs." They emphasized digital literacy "*Government should invest fully in cybersecurity education*" and transparency. "*The problem is not social media but government communication.*" These calls mirror global best practice emphasizing collaboration rather than censorship. Social movement theory reinforces the value of inclusive policymaking. "*Work with the people and not against them,*" as one respondent urged, reflects evidence that connective action is more governable when policies emerge from dialogue with activist networks.

The findings also confirm that social media activism in Kenya is a double-edged sword. It strengthens civic engagement and accountability, but also facilitates misinformation, incitement, and cyber threats. Social network theory explains the mechanics of rapid diffusion; social movement theory clarifies the logic of

connective action; and securitization theory situates state responses in the balance between rights and order. Regulatory frameworks that lean too heavily on suppression risk undermining democratic gains, while laissez-faire approaches threaten stability. The challenge lies in crafting governance strategies that protect freedoms, foster accountability, and mitigate risks without collapsing legitimate activism into "security threats."

**Conclusion**

This research shows that social media and emerging digital activism have both positive and negative implications on the country's national security. While on the one hand spaces provided by social media allow citizens to exercise their freedom of expression, demand accountability and call for social justices, there are other implications that negatively affect the countries national security and stability. For examples, amidst call for accountability, there has been systematic use of social media spaces to call for violence in the name of accountability. Similarly, misinformation, hate speech, fake news, cyber threats and defamation have characterized some of the social media activists approach. This was not only confirmed through our qualitative interviews with key informants, but also our correlation analysis also indicates that there is a statistically significant nexus between activism on social media platforms and both inadvertent dissemination of misinformation and engagement in violent protests. This illustrates a fragile boundary between public disorder and digital empowerment.

Of importance is the gap that exists in the current regulatory and legal frameworks in Kenya that makes it difficult to address the challenges that emerge as a result of digital activism. While there are frameworks such as the Data Protection Act (2019) and Computer Misuse and Cybercrimes Act (2018), the threats of incitement to violence, hate speech, mis/disinformation as well as fake news are not well addressed. This allows ill intended users to exploit such legal gaps to promote harmful activities while state response is likely to be seen as overreach especially if it opts for measures like arbitrary arrests, censorship or surveillance. What the country is now grappling with is increased polarization and erosion of public trust. The theories used in the study provide a unique insight. They reveal that while it is important to mitigate the challenges of social media activism, the government also needs to acknowledge that the nature of activism is changing with changes in technology and that digital activism remains a legitimate form of civic engagement.

**Recommendations**

The study proposes three interventions the government can consider while addressing the paradox between digital activism and national security. (1) amend the existing frameworks to align with current realities, including clearly defining what constitutes threats to national security through digital activism to avoid ambiguity especially with freedom of speech and expression. (2) focus on scale, speed and verification to curb the spread of disinformation, incitement and hate speech. This calls for adoption of competent technologies to flag and classify as offensive such digital activities for audiences to be alert and vigilant. (3) there is an urgent need to come up with a digital risk index for Kenya which will focus on scenario modeling but also provide clear variables and trends that point towards national security threats as a result of digital activities. This index needs to provide accurate status of the country based on a scale to show whether we are in the best or worst state in term of digital activism.

**References**


Abboud, E., Ajwang, F., & Lugano, G. (2024). Social media and politics as usual? Exploring the role of social media in the 2022 Kenyan presidential election. *Journal of Eastern African Studies*, *18*(2), 321-343.

Abdulazeez, I., Omale, Z., & Florence, C. O. (2025). Implications of Social Media Disinformation and False Narratives for Public Opinion among Nigerian Electorate. *International Journal of Sub-Saharan African Research*, *2*(4), 306-324.

Ali, M. N. (2025). Digital Activism and Collective Mobilization: A Narrative Review of Social Identity, Group Efficacy, and the SIMCA Framework. *Sinergi International Journal of Psychology*, *3*(1), 38-51.

Arifah, I. D. C., Maureen, I. Y., Rofik, A., Puspila, N. K. W., & Erifiawan, H. (2025). Social Media Platforms in Managing Polarization, Echo Chambers, and Misinformation Risk in Interreligious Dialogue among Young Generation. *Journal of Social Innovation and Knowledge*, *1*(aop), 1-33.

Arzani Ardebili, S. (2025). Tweets of Resistance: Social Media and Mobilization in Contemporary Kenya A discursive study on the Kenyan protests and online activism in 2024.

Berchin, S. A. (2025). *The Truth, Lies, and Telegram: False and Misleading Information from Telegram and Its Impact on US Perceptions Regarding the Israeli-Palestinian Conflict* (Doctoral dissertation, Brandeis University).

Binitie, A. P., & Odetayo, B. J. (2024). Evaluating the privacy issues, potential risks, and security measures associated with using social media platforms. *International Journal of African Research Sustainability Studies*.

Boulianne, S. (2019). Revolution in the making? Social media effects across the globe. *Information, communication & society*, *22*(1), 39-54.

Bradshaw, S., & Howard, P. N. (2019). Social media and democracy in crisis. *Society and the internet*, *24*, 212-227.

Buzan, B., & Wæver, O. (2009). Macrosecuritisation and security constellations: reconsidering scale in securitisation theory. *Review of international studies*, *35*(2), 253-276.

Cariolle, J. (2021). International connectivity and the digital divide in Sub-Saharan Africa. *Information Economics and Policy*, *55*, 100901.

Çela, E. (2015). Social media as a new form of public sphere. *European Journal of Social Sciences Education and Research*, *4*(1), 195.

Chakma, K. (2024). A Review of the Role of Social Media in Shaping Social Movements. *Available at SSRN 5083142*.

Chami, G. (2025). Social Media as a Conduit for Civil Society Movements. In *from Epic Tales to Digital Trails* (pp. 11-37). Routledge.

Chinemerem, O. (2025). *Digital Activism in Nigeria: The Role of Social Media in Youth Mobilization for The# EndSARS Movement* (Doctoral dissertation, Vrije Universiteit Brussels, Belgium).

Collins, R. L. (2025). *Journalists' perspectives on social media in the Fourth Estate and its impact on public trust in politics* (Doctoral dissertation, Liberty University). Liberty University Digital Commons. Accessed from https://digitalcommons.liberty.edu/doctoral/7112/

Council of Europe (2025, February). The global state of cybercrime legislation 2013–2024: A cursory overview. Cybercrime Programme Office of the Council of Europe (C-PROC). *The global state of cybercrime legislation 2013–2024: A cursory overview*. Council of Europe. https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2024-public-v6-final/1680b3ecc5

Darden, J. T. (2019). *Tackling terrorists' exploitation of youth*. Washington, DC: American Enterprise Institute.

de Lira, J. E. T., Mariz, L., & Coelho, I. M. F. C. (2024). Regulatory Challenges of Online Disinformation: Analysis of National Legislation and International Approaches to Disinformation and Fake News. *Revista de Gestão Social e Ambiental*, *18*(12), 1-21.

Earl, J., Maher, T. V., & Pan, J. (2022). The digital repression of social movements, protest, and activism: A synthetic review. *Science advances*, *8*(10), eabl8198.

Eltantawy, N., & Wiest, J. B. (2011). The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory. *International journal of communication*, *5*, 18.

Erbschloe, M. (2018). *Extremist propaganda in social media: A threat to homeland security*. CRC Press.

Flew, T., & Iosifidis, P. (2020). Populism, globalisation and social media. *International Communication Gazette*, *82*(1), 7-25.

Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, *10*(1), 33-50.

Frenkel, S., Isaac, M. & Conger, K. (2018, October 29). On Instagram, 11,696 Examples of How Hate Thrives on Social Media. *The New York Times*. Retrieved from https://www.nytimes.com/2018/10/29/technology/hate-on-social-media.html

Głowacka, D., Youngs, R., Pintea, A., & Wołosik, E. (2021). Digital technologies as a means of repression and social control. *Policy Department for External Relations, Directorate General for External Policies of the Union*, *1*, 1-106.

Haj Omar, H. (2016). *Ideology, media and conflict in political discourse and its translation during the Arab Spring: Syria as a case study* (Doctoral dissertation, University of Leeds).

Heydemann, S. D., & Tejani, S. (2019). Legal changes needed to strengthen the# MeToo movement. *Richmond Public Interest Law Review*, *22*(2), 237-268.

Hngokchai, P. W. (2025). Youth Political Participation in the Digital Era: Trends, Drivers, and Democratic Implications. *วารสาร วิชาการ สังคมศาสตร์สมัยใหม่ (Online)*, *2*(2), 53-69.

Howe, S. W., & Haigh, Y. (2016). Anti-corruption watchdog accountability: The limitations of judicial review's ability to guard the guardians. *Australian Journal of Public Administration*, *75*(3), 305-317.

Imoka, C. (2023). Digital media, popular culture and social activism amongst urban youth in Nigeria. *Critical African Studies*, *15*(2), 134-148.

Jost, J. T., Barberá, P., Bonneau, R., Langer, M., Metzger, M., Nagler, J., ... & Tucker, J. A. (2018). How social media facilitates political protest: Information, motivation, and social networks. *Political psychology*, *39*, 85-118.

Kaiser, J., Fähnrich, B., Rhomberg, M., & Filzmaier, P. (2018). What happened to the public sphere? The networked public sphere and public opinion formation. In *Handbook of cyber-development, cyber-democracy, and cyber-defense* (pp. 433-459). Springer, Cham.

Kamath, K. Y., Caverlee, J., Cheng, Z., & Sui, D. Z. (2012, October). Spatial influence vs. community influence: modeling the global spread of social media. In *Proceedings of the 21st ACM international conference on Information and knowledge management* (pp. 962-971).

Kharel, A. B. (2024). Cyber-Politics: Social Media's Influence on Political Mobilization. *Journal of Political Science*, 103-115.

Kizito, P. (2024, December 28). Kenya: Ruto breaks silence on abritrary arrests, urges parental responsibility as he pledges action. *All Africa* Retrieved from https://allafrica.com/stories/202412280016.html

Klinger, U., Kreiss, D., & Mutsvairo, B. (2023). *Platforms, power, and politics: An introduction to political communication in the digital age*. John Wiley & Sons.

Kumar, A., & Maurya, M. K. (2024). Online public sphere and threats of disinformation, extremism and hate speech: Reflections on threat-mitigation. *Journal of Communication Inquiry*, 01968599241292623.

Kwanya, T., Kogos, A. C., Kibe, L. W., Ogolla, E. O., & Onsare, C. (2022). Cyber-bullying research in Kenya: a meta-analysis. *Global Knowledge, Memory and Communication*, *71*(4/5), 208-229.

Mare, A., Mabweazara, H. M., & Moyo, D. (2019). "Fake news" and cyber-propaganda in sub-Saharan Africa: Recentering the research agenda. *African Journalism Studies*, *40*(4), 1-12.

Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. *New York: Data & Society Research Institute*, *359*, 1146-1151.

McCombs, M., & Valenzuela, S. (2020). *Setting the agenda: Mass media and public opinion*. John Wiley & Sons.

Meikle, G. (2024). *Social media: The convergence of public and personal communication*. Routledge.

Menkhaus, K. (2013). Al-Shabaab and social media: A double-edged sword. *Brown J. World Aff.*, *20*, 309.

Mlika, F., Karoui, W., & Ben Romdhane, L. (2024). Trustworthy decentralization based on blockchain tools for social network architectures. *Social Network Analysis and Mining*, *14*(1), 95.

Mpofu, S. (2023). Monitoring the Fourth Estate: A Critical Analysis of the Role of Audiences in Watchdogging Journalists. In *New Journalism Ecologies in East and Southern Africa: Innovations, Participatory and Newsmaking Cultures* (pp. 183-205). Cham: Springer International Publishing.

Mpofu, S. (2024). Violence as a Decolonizing and (De) humanizing Force, and Social Media (ted) Protests in Africa. *Media, Social Movements, and Protest Cultures in Africa: Hashtags, Humor, and Slogans*, 13.

Mutua, S. N., & Yanqiu, Z. (2021). Online content regulation policy in Kenya: Potential challenges and possible solutions. *Journal of Cyber Policy*, *6*(2), 177-195.

Mwangi, E. N. (2025). *The Twitter/X Revolution: Gen Z's Political Participation in Kenya's Digital Age* (Master's thesis, Temple University).

Ndlela, M. N. (2020). Social media algorithms, bots and elections in Africa. In *Social media and elections in Africa, Volume 1: Theoretical perspectives and election campaigns* (pp. 13-37). Cham: Springer International Publishing.

Nicolla, S., Lazard, A. J., Austin, L. L., Freelon, D., Reyes, H. L. M., & Moracco, K. E. (2023). TikToks lead to higher knowledge and perceived severity of sexual violence among adolescent men. *Journal of youth and adolescence*, *52*(12), 2449-2463.

Njoroge, G. M. (2020). *Human Factors Affecting Favourable Cybersecurity Culture-a Case of Small and Medium-sized Enterprises Smes Providing Enterprise Wide Information Systems Solutions in Nairobi City County in Kenya* (Doctoral dissertation, University of Nairobi).

Nwakanma, A. P. (2022). From black lives matter to EndSARS: Women's socio-political power and the transnational movement for black lives. *Perspectives on Politics*, *20*(4), 1246-1259.

Omilusi, M. (2025). Participatory Governance and Youth Protests in the Digital Age: Interrogating the# EndSARS Movement. *African Security*, 1-23.

Ondimu, J., Yieke, F., & Mwithi, F. (2025). Multimodal representation and ideological framing of social actors in Kenya's anti-police brutality Twitter activism. *Social Semiotics*, 1-19.

Opiyo, R., Mwau, B., Mwang'a, K., & Mwaniki, D. (2017). Attaining E-democracy through digital platforms in Kenya. In *E-Democracy for Smart Cities* (pp. 441-459). Singapore: Springer Singapore.

Oriola, T. B. (2024). *Terrorism, politics, and human rights advocacy: the# BringBackOurGirls movement*. Oxford University Press.

Osman, O. (2025). Whose Voices Shape Protest Narratives? Comparing Source Diversity in Kenya's Digital-Native and Legacy-Affiliated News Coverage. *Journalism Studies*, *26*(13), 1617-1629.

Otieno, M., & Anyuor, N. (2024). Digital newspaper contents readership in rural Kenya: Myth or reality? *Journal of Emerging Technologies*, *4*(1), 45-53.

Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research Archive*, 11(1): 1747-1755

**Owen, D. (2017). The new media's role in politics. In F. Gutiérrez Junquera (Ed.),** *The age of perplexity: Rethinking the world we know***. Penguin Random House.**

Peterson, A. (1989). Socia Movement Theory. *Acta Sociologica,* 32(4):419-426

Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, *64*(6), 763-774.

Rochefort, A. (2020). Regulating social media platforms: A comparative policy analysis. *Communication Law and Policy*, *25*(2), 225-260.

Rucht, D. (2023). *Social movements: a theoretical approach*. Oxford University Press.

Scheibe, K. (2024). *Information Behavior on Social Media: Services, Users, and Usage* (Doctoral dissertation, Dissertation, Düsseldorf, Heinrich-Heine-Universität, 2024).

Schellewald, A. (2022). Theorizing "stories about algorithms" as a mechanism in the formation and maintenance of algorithmic imaginaries. *Social Media+ Society*, *8*(1), 20563051221077025.

Segerberg, A., & Bennett, W. L. (2011). Social media and the organization of collective action: Using Twitter to explore the ecologies of two climate change protests. *The Communication Review*, *14*(3), 197-215

Sharma, S., Kar, A. K., Gupta, M. P., Dwivedi, Y. K., & Janssen, M. (2022). Digital citizen empowerment: A systematic literature review of theories and development models. *Information Technology for Development*, *28*(4), 660-687.

Singh, P., & Singh, A. K. (2025). *The digital revolution: exploring new media in the 21st century*. Crown Publishing.

Theodorakopoulos, L., Theodoropoulou, A., & Klavdianos, C. (2025). Interactive Viral Marketing Through Big Data Analytics, Influencer Networks, AI Integration, and Ethical Dimensions. *Journal of Theoretical and Applied Electronic Commerce Research*, *20*(2), 115.

Thumfart, J. (2024). Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. *Journal of global security studies*, *9*(1), ogad024.

Trauthig, I. K., Martin, Z. C., & Woolley, S. C. (2024). Messaging apps: A rising tool for informational autocrats. *Political Research Quarterly*, *77*(1), 17-29.

Walther, S., & McCoy, A. (2021). US extremism on Telegram. *Perspectives on Terrorism*, *15*(2), 100-124.