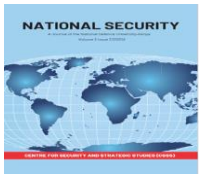


NATIONAL SECURITY

A Journal of the National Defence University-Kenya

Volume: 3
Issue: 2

Research Article Open Acces

Youth, Digital Communication and National Security in Kenya: The Gen-Z Protests (2024–2025)

Samuel Juma Ouma[1] *

[1]St. Paul's University- sammyayal68@gmail.com

* Corresponding author

Abstract

This paper explores the intersection of digital communication, youth activism and national security, drawing on the case of the 2024/2025 Gen-Z protests in Kenya. Beginning with protests against the Finance Bill 2024, these protests quickly became the most widespread youth mobilisation and protest in Kenyan history since the early 1900s. Social media platforms served as mobilisation venues on one side and contest venues on the other. The research builds on the theory of securitisation and the notion of networked publics to construct a Digital Securitisation Cascade, aiming to understand how viral online communication both inflates and limits states' responses to dissent. The methodological approach involves a convergent mixed-methods design, combining computational social science and qualitative methods, including network analysis and cross-platform content time-series modelling, with critical discourse analysis of government statements, media attention and 25 semi-structured interviews with activists, journalists and policymakers. Results indicate that surges in online presence were powerful predictors of securitising rhetoric by state actors and viral transmission of visual representations of police violence created international suspicion, which softened coercive state strategies. At the same time, misinformation and disinformation also made it difficult to trust any side of the protesters or the government, provoking further conflict online. It contributes in 3 ways: theoretically, the study is a reconceptualisation of securitisation as a digitally networked public contest into a large-scale form of mobilisation; empirically, the study presents a rare example of a large-scale mobilisation of youth in East Africa; and methodologically, the study is a multimodal approach to the study of protest communication in the Global South. The article concludes by offering policy recommendations on the governance of platforms, transparency in the security sector and youth empowerment in democratic processes.

Keywords: *Digital protests, misinformation, networked publics, securitisation, social media, youth activism.*

Received: 18 May 2025
Revised: 25 August 2025
Accepted: 20 October 2025
Published: 15 December 2025

Citation: Ouma, O. J., (2025). Youth, Digital Communication and National Security in Kenya: The Gen-Z Protests (2024–2025). *National Security: A Journal of National Defence University-Kenya*, *3*(2), 132–148.

DOI: https://doi.org/10.64403/89txsx23

Introduction

Communication has been central in organising political power and negotiating legitimacy. From pre-colonial oral traditions to the nationalist press of the independence period, history has shown that communicative practices were historically organised regarding how authority was exercised and fought in Kenya. However, when digital technologies spread rapidly in the twenty-first century, communication became a source of empowerment and vulnerability. Social media platforms are accessible platforms where citizens talk, organise and express grievances and also offer novel surveillance, securitisation and disinformation infrastructures (Morozov, 2011; Castells, 2012). The duality of communication as both emancipatory and destabilising has come into special focus in situations where young populations interact with growing economic frustrations and unstable state-society relations (Mohamed & Tohami, 2013).

This is the dynamic with Kenya. With a median age below 20 years and mobile penetration exceeding 100% due to the widespread adoption of multi-SIM technology, the nation is one of Africa's most digitally affluent societies (Nyabola, 2018). Innovations such as M-Pesa have made Kenya a hub for mobile money and social networking applications like TikTok, X (formerly Twitter), Instagram and WhatsApp are among the leading providers of news, political commentary and civic expression among Generation Z members (Battochio et al., 2023). The weight of demographic change has reorganised political communication: instead of conventional party politics or civil-society organisations, young Kenyans are engaging in more decentralised, networked forms of activism mediated by short videos, memes and viral hashtags (Papacharissi, 2015).

The youth protests of 2024 were a turning point in this direction. The protests began in response to the Finance Bill 2024's unpopular taxes on basic commodities and digital services and quickly evolved into an online movement. Then, the movement spread to the streets across the country. The movement's communicative architecture was apparently enormous, horizontal, leaderless and digitally powered. Hashtags like #RejectFinanceBill2024 and #GenZRevolution went viral worldwide, helping to create a shared identity that no longer depended on deeply rooted ethnic and regional divisions within Kenyan politics (Ingutia, 2025). The demonstrations peaked by the end of June when the protesters stormed Parliament in Nairobi. This was met with riot control, live ammunition and legal actions that were linked to counter-terrorism, indicating the securitisation of youth dissent (Muchiri et al., 2025).

This event highlights the fact that communication has become one of the contentious national security arenas. Informational flows were both weaponised and served as a shield. Protesters leveraged them to mobilise, document atrocities and gain international support, and the state tried to rebrand dissent as a security concern and resorted to digital censorship and narrative control (Arzani Ardebili, 2025). To make it even more complicated, disseminating misinformation, disinformation and rumours, including inflated casualty numbers and fake videos, caused credibility loss and increased volatility (Petla, 2025). Accordingly, the demonstrations demonstrated an unstable nexus of communication security, where mobilisation, securitisation and information disorder interrelate in real time.

The Kenyan case, offers a distinct empirical point of entry for theorising the role of communication in the politics of security in modern times. First, it highlights the agency of the networked public, which influences political outcomes beyond institutional processes (Nyabola, 2018; Wamuyu 2020). Second, it demonstrates how securitisation theory can be applied to digital activism, in which states often perceive online dissent as a threat to their existence. Third, it telegraphs the contribution of information disorder as a tactical tool and a source of structural weakness of contentious politics. Lastly, it makes one consider the possibilities and vulnerabilities of democratic digital publics in societies characterised by economic precarity and unequal connectivity (Habermas, 1989; Papacharissi, 2015).

Therefore, this paper aims to answer three related questions: How did digital communication support the mobilisation and framing of the Gen-Z protests? Why did the Kenyan state securitise communication, and on what grounds did it react with extraordinary measures? What contributed to misinformation and disinformation in protest dynamics and security reactions? To answer these questions, the study will employ a convergent mixed-methods design, combining computational social science, discourse analysis and

interviews with protest actors and policymakers. This inquiry is important in that it contributes to three levels of understanding. It conceptualises securitisation, in theory, as a digitally mediated and controversial process. Regarding methodology, it provides evidence of the usefulness of a network analysis, content analysis and qualitative interpretation in investigating contentious politics in the Global South. Empirically, it presents the earliest systematic scholarly explanation of the Gen-Z protests in Kenya, situating them within the context of African and broader global discussions about youth activism, network politics and national security.

Finally, the Gen-Z protests demonstrate a paradox: digital communication empowers youth to organise nonviolent protests and voice democratic demands. However, on the other hand, it puts pressure on the state's ability to control the situation and provokes securitisation processes. This paradox is particularly significant for Kenya and other states that struggle to navigate the complex intersection between digital politics and national security in an era of networked publics.

Theoretical and Conceptual Framework

The Gen-Z protests in Kenya offer a critical moment to question how governments and the people negotiate security, legitimacy and communication in the digital era. To make this interplay sense, this paper employs securitisation theory as its primary conceptual framework. Securitisation theory, developed by the Copenhagen School, is a valuable tool for understanding how state actors create threats through language and how such discursive actions justify extreme actions that transcend standard politics (Buzan et al., 1998). With an emphasis on the speech acts in which actors make an issue a question of survival, securitisation theory sheds light on how governments package dissent not as a form of opposition, but as a life-threatening challenge to state sovereignty and stability.

Securitisation Theory

The crux of securitisation theory is that security is not a state of being but a constructed position granted by discourse. A securitised issue is represented by a securitising actor (typically a political leader or institution) as an existential threat to a referent object (the state, society, or economy) in such a way that it justifies extraordinary action ((Stritzel, 2014). In Kenya, the Gen-Z protests were depicted by the top government officials, such as the President and Cabinet Secretaries, as anarchic, foreign-led and a menace to national peace. It was through this type of framing that the state was able to legitimise actions that involved police deployments of military grade weaponry, live ammunition, internet blackouts and invoking counter-terrorism patterns. This act is typical of what the securitisation theory calls the extraordinary leap: the power to go beyond usual democratic politics in the name of the urgency of survival. Securitising youth dissent allowed the Kenyan government to bypass the standard processes of dialogue and compromise and to put protesters in the same category as terrorists or insurgents. Securitisation thus provides a strong explanatory framework for the state's mobilisation of communication to transform acceptable dissent into an issue of security exceptionalism.

Nevertheless, securitisation can never be a one-way process. Although the Copenhagen School originally brought central attention to the dynamics of states, later research has increased emphasis on audiences and counter-securitisation (Balzacq, 2011; Stritzel, 2014). Audiences must be comfortable securitising claims to make them successful, and counter-actors can fight back by reshaping the problem. In the Kenyan case, the protesters positioned themselves as patriotic champions of democracy and fiscal justice against state efforts to criminalise them. An example of such counter-securitising actions is the use of such videos to demonstrate police brutality and international solidarity hashtags. This scenario is an extension of securitisation theory, focusing on contestation and audience agency, which is key to extending the theory into the digital age.

Although securitisation theory is the paper's backbone, other theoretical traditions enhance the paper by shedding light on specific mechanisms in the securitisation process. The framing theory posits that actors strategically emphasise certain aspects of reality that shape people's perception and understanding (Entman, 1993). In the Gen-Z protests, the protesters framed the protests as the Finance Bill was unjust and

undemocratic, whereas the state framed the protests as chaos and disorder. Such rival frames are part and parcel of securitisation: they form the discursive space onto which securitising speech acts are challenged. The reason why the protests might be organised in a leaderless but coordinated manner can be described by the theory of networked publics Hodzi, & Zihnioğlu, 2024; Papacharissi, 2015). On platforms like TikTok and X, digitally mediated publics were formed around which youth identities, grievances and solidarities could assemble outside institutional frameworks. Such networked publics were not just communication tools, but the audience whose approval or disapproval made the difference between the success or failure of securitisation efforts.

Habermas's concept of the public sphere (1989) can also serve as a normative marker for evaluating the democratic potential of digital communication. Twitter Spaces and TikTok live served the purpose of deliberation by young people, as they discussed taxation, corruption and governance. However, they were spheres with limitations, such as platform algorithms, data costs and state censorship. Securitisation-wise, these online worlds were also an area of contention, and the audience for securitising moves was also a subject of negotiation. Lastly, information disorder (Petla, 2025) is a concept that emphasises the role of misinformation, disinformation and malinformation in unstable communication during the protests. Fabricated casualty figures, doctored videos and conspiracy theories circulated widely, complicating the ability of both the state and citizens to establish credible narratives. Information disorder thus shaped the context in which securitisation unfolded, affecting the credibility of both securitising and counter-securitising claims.

The Digital Securitisation Cascade

This paper develops the digital securitisation cascade, based on the securitisation theory and complemented by these other supportive views. The model builds on classical securitisation theory by incorporating it into networked publics and information disorder dynamics. It theorises securitisation as a recursive cascade rather than a process occurring in a linear and elite way, shaped by digital visibility, framing contestation and misinformation flows.

Table 1

Stages of the Digital Securitisation Cascade

Stage	Description
Trigger	A policy shock, such as the Finance Bill 2024, sparks grievances.
Mobilisation	Networked publics emerge via hashtags, influencers and viral content.
Visibility	Frames gain traction through algorithmic amplification and agenda-setting.
Securitising Move	State actors frame protests as existential threats.
Extraordinary Measures	Exceptional policing, censorship and legal repression follow.
Counter-Securitisation	Protesters deploy counter-frames, global solidarity and visual evidence of abuses.
Information Disorder	Mis/disinformation complicates credibility, amplifying volatility.
Feedback Loop	Each stage reshapes mobilisation, securitisation and audience acceptance.

Source: Researcher, (2025)

This model has three contributions to the theory of securitisation. First, it highlights the agency of networked publics as both audiences and counter-securitising actors. Second, it predicts the effect of visibility and algorithmic mediation in securitising at a faster pace. Third, it incorporates the information disorder as a structural element that compromises the transparency of securitising claims. These extensions, in combination, transform securitisation theory to suit the digital communication context of the Global South. Placing securitisation theory into its proper context by centring it and broadening it through other literatures on framing, networked publics, public spheres and information disorder, this paper establishes a solid conceptual basis for analysing the Gen-Z protests. The theory of securitisation provides the best perspective on how dissent can be discoursed into a security threat. The supportive theories enhance the picture by shedding light on how frames are challenged, how publics are formed and how misinformation makes it difficult to ascertain credibility. The suggested Digital Securitisation Cascade summarises these observations into a theoretically sound and empirically based framework in the Kenyan context.

Literature Review

It is essential to understand the Gen-Z protests in Kenya and situate them within the broader scholarship on digital activism, securitisation, networked publics, information disorder and African politics of communication. The review is structured thematically to draw out the conceptual building blocks of the study. Although securitisation theory is the key construct of this article, the literature review draws on other traditions to shed light on specific mechanisms that enhance our understanding of the analysis.

National security has remained a key paradigm that states articulate and react to threats to their sovereignty, stability and the well-being of their citizens. Historically, it placed the focus on the territorial defence and military preparedness (Buzan, 2008). However, it is the twenty-first century and national security has expanded to encompass not only political, economic and environmental aspects, but also digital ones. The hybrid security issues of terrorism, governance instability and cyber vulnerabilities have been catalysts for this change in the African context. According to Owuondo (2025), the hybrid war challenges in Kenya demonstrate the convergence of cyberattacks, disinformation and physical sabotage, with digital vulnerability becoming an integral part of national security infrastructure.

The latest evaluations of sponsored cyberattacks by states also indicate that communication systems and web infrastructures have been incorporated into current warfare tactics and intelligence measures. Mumma-Martinon et al. (2024) emphasise that cyber conflict can no longer be viewed in isolation from traditional security issues. Kabata and Garaba (2020) in Kenya demonstrate that digital surveillance and data-control provisions have been institutionalised by the Security Laws (Amendment) Act 2014 and the Computer Misuse and Cybercrimes Act 2018 as an integral part of national-security governance. These models illustrate how security logics are integrated into everyday communication practices.

Simultaneously, digitalisation has introduced new weaknesses in the institutions of the population. Studies warn that ransomware, data breaches and denial-of-service attacks pose a threat to the sustainability of governance, as well as national development goals (Tsanis et al., 2022). In addition to Kenya, Ignatov and Kerimi (2025) note that states are increasingly utilising AI systems and online infrastructure as part of securitised conceptions of AI sovereignty and that even the autonomy of technology per se has turned into a national defence concern. As a result, digital communication is no longer a fringe concern for national security; it is now a core area of dispute. Online protests, hashtags and mobilisations formed over the network can be securitised as a potential threat to state stability and seen by activists as democratic instruments to hold them accountable (Nyabola, 2018). Conceptualising national security as a developing and socialised process that has introduced information control and cyber governance to the current process, therefore, offers the required conceptual framework upon which digital activism, securitisation and counter-securitisation in the Kenya Gen-Z protests can be analysed.

The past 20 years have witnessed a significant shift in how contentious politics is structured and communicated. Scholars have emphasised the ability of digital platforms to reduce barriers to entry into

collective action and decentralised coordination, and they can amplify the voices of marginalised individuals (Arzani Ardebili, 2025; Bennett & Segerberg, 2012; Ortiz et al., 2019). The campaigns of the Arab Spring revolts, the *Black Lives Matter* movement in the United States and the *EndSARS* movements in Nigeria demonstrate that social media campaigns, along with digital infrastructures, enable new kinds of connective action, where informal networks often take the place of formal organisations. Digital activism is particularly relevant in Africa, where young demographics and lopsided democratic integration define the situation (Nyabola, 2018). In Nigeria, the hashtag #EndSARS highlighted the need for coordinated leadership, which Twitter and Instagram facilitated.

In contrast, in Uganda, digital blockages during elections highlighted the state's fear of online mobilisation. Kenya is not an exception: SMS proved to serve as a crucial instrument of mobilisation and incitement during the 2007/2008 post-election violence (Goldstein & Rotich, 2008) and later, Twitter emerged as a space for citizen journalism and real-time accountability (Omanga & Mainye, 2019). The Gen-Z protests follow a similar line but depart from the previous movements. The protests mobilised a generation of economically precarious and digitally fluent people, unlike previous times when mobilisation was dominated by ethnic identity. Networked activism literature can be used to understand why the mobilisation was rapid, large-scale and emotionally impactful and why networked publics are valuable sources of collective identity (Hodzi, & Zihnioğlu, 2024; Papacharissi, 2015).

The securitisation literature provides a conceptual entry point for understanding how states address dissent. According to Buzan, Waever and de Wilde (1998), the problems are not security concerns due to their inherent danger, but rather have been brought to the forefront by elites who manage to pose them as existential threats. After securitisation, extraordinary legitimisation is justified. Securitisation theory has been applied in areas beyond military security, including migration (Huysmans, 2006), health (McCoy et al., 2023) and climate change. Recent scholarship has started to address the digital realm. Vromen (2016) demonstrate the process of securitising communication infrastructures through surveillance and censorship, while others focus on the securitisation of online activism in the context of authoritarian protests.

However, little is known about securitisation in African democracies. Immediate exceptions are studies on counter-terror in Kenya, where the Al-Shabaab has been characterised as an existential threat, which justified surveillance and emergency legislation (Anderson & McKnight, 2015). The Gen-Z protests are a significant continuation: no more outside terrorist groups, but a national youth protest was the target of securitisation. This also depicts the malleability of securitisation and the controversial audience. Protesters, journalists and international actors opposed securitising claims by generating the protests as a free democratic exercise. This aspect of counter-securitisation, the capacity of actors to counter or reframe securitising speech acts, is also emphasised in the existing literature (Balzacq, 2011; Stritzel, 2014). The Kenyan example provides a viable context for implementing and generalising the securitisation theory in the digital age.

Closely associated with the literature on securitisation is the literature on framing. Frames are decoding packets that draw attention to some aspects of reality and leave out others, influencing how viewers perceive matters (Entman, 1993). Frames are mobilising, whereas counter-frames are used to delegitimise dissent by a state. Research on digital activism focuses on how hashtags serve as framing devices. In Nigeria, the kidnapping of schoolgirls was characterised as an internal matter and a global human rights matter using the hashtag of the movement that was called BringBackOurGirls (Oriola, 2024). Hashtags such as # RejectFinanceBill2024 in Kenya condensed complaints into stories that were easy to share, crossing boundaries and platforms. Frames work also via pictorials. Studies indicate that images of police brutality, martyrdom, or governmental corruption can mobilise emotional reactions and are capable of producing mobilisation effects (DeLuco, Lawson and Sun, 2012). When the protests of Gen-Z arose, the virality of the TikTok videos of police shootings turned into a rallying point despite the state's trying to make the protests seem criminal. Literature on framing thus fills in the gaps left by securitisation theory because it elucidates the processes by which rival accounts attain popularity among audiences.

The Networked Publics scholarship suggests that digital media reconfigure the concept of publics by altering the affordances of communication, including persistence, visibility and searchability (Hodzi, & Zihnioğlu,

2024). Conceptualised by Papacharissi (2015) as affective publics, these are movements in which people feel outraged, hopeful, or grieved, which spread to keep the movement alive. African scholarship demonstrates how digital publics can be leveraged in opposition to established power. Bosch (2017) demonstrates the power of X to create solidarity among the South African student protests and Nyabola (2018) captures the Kenyan activists who used digital platforms to mount a feminist and political movement. The Gen-Z protests carry these lessons: young people formed publics that transcended ethnic boundaries, asserting their status as digital natives, challenging the misrule of the elites. This literature also points out the weaknesses. Networked publics can be easily monitored, influenced and disintegrated. Divisive or sensational information can be boosted by algorithms that precede engagement (Ortiz et al., 2019). Such mechanisms make counter-securitisation initiatives difficult to achieve because state actors use platform weaknesses to silence or twist the protests.

The standard for assessing digital protests remains the concept of the public sphere, as understood by Habermas, an area where people discuss issues of shared interest (Habermas, 1989). According to optimists, social media broadens deliberation by creating various entry points for participation (Castells, 2012). Pessimists argue that digital communication fosters a public that is isolated within echo chambers and undermines rational discourse (Sunstein, 2018). This ambivalence is manifested in Kenyan scholarship. Omanga and Mainye (2019) demonstrate that X serves as a mechanism of citizen-based accountability, while others caution that the threat to deliberative quality is a phenomenon associated with elite capture and misinformation. X Spaces and TikTok Lives served as transient mass spaces where the Gen-Z generation discussed taxes and government during the protests. However, the access was restricted by state censorship, data expenses and digital divides, casting doubts on inclusiveness. This way, the public sphere literature gives us a normative ideal, whereas the Kenyan scenario characterises its uneven and contentious realisation. These spheres are important in securitisation since they form the audiences whose approval or disapproval of securitising moves defines securitising success.

Lastly, information disorder literature highlights the role of misinformation, disinformation and malinformation as destabilising in digital politics (Petla, 2025). Scholars demonstrate how disinformation campaigns are used by both the state and non-state actors to delegitimise their adversaries, disorient audiences and undermine trust (Marwick & Lewis, 2017). In Africa, misinformation spreads quickly due to a high dependence on mobile messaging applications and inadequate verification systems (Coulibaly, 2023). In Ethiopia, Nigeria and South Africa, some protests saw inflated casualty numbers and fake videos fuelling the conflict intensely. Similar processes were apparent in the Gen-Z protests in Kenya: there were disseminated fake photos of allegedly foreign mercenaries as well as unsubstantiated reports about government collapses. This literature also throws up a significant challenge to securitisation theory. When audiences are overloaded with incongruent information, their ability to believe or disbelieve securitising claims has been compromised. Information disorder, therefore, is a structural variable that preconditions the success of securitisation and counter-securitisation.

The literature reviewed has led to the convergence of three insights. To begin with, online platforms have restructured the mobilisation process, allowing young people to challenge state discourse and influence political agendas. Second, the securitisation theory offers a strong framework for states' reactions, but needs to be adjusted to consider networked publics, problematic frames and the influence of misinformation. Third, African empirical experiences also provide distinct perspectives on advancing these debates, as they have young populations, disproportionate connectivity and mixed regimes. Within these scholarly debates, by locating the Kenyan Gen-Z protests in these debates, this paper contributes to the current literature by making three contributions: it also applies securitisation theory to online youth protests in a democratic African setting; it emphasises the role of networked publics in the roles of audiences and counter-securitising agents; and it incorporates the notion of information disorder as a driving force to protest-security relations. This literary review thus forms the basis of the Digital Securitisation Cascade proposed in the study, which theorises securitisation in the age of networked publics and shifting information environments.

Methodology

The paper presents a convergent mixed-methods research study that explores the securitisation of the 2024 Gen-Z protests in Kenya. The use of mixed methods is necessary because the dynamics to be studied, digital communication, securitisation and youth mobilisation, are presented in both quantitative and qualitative forms. The pattern of diffusion and visibility represents the quantitative aspects, while the qualitative aspects are vested in discourse and experience. The study combines computational social science and qualitative inquiry to present an empirically strong, theoretically sensitive account (Creswell & Plano Clark, 2018). It is designed around three dependent and interrelated questions: How did digital communication support the mobilisation and framing of the protests? How did the Kenyan state securitise dissent through discourse and extraordinary action? How did misinformation and disinformation affect the process of mobilisation and repression?

The study uses a broad spectrum of data sources to triangulate views. The primary corpus consists of social media data. Four large platforms, X (formerly Twitter), TikTok, Instagram Reels and WhatsApp, served as content sources. Hashtags such as #RejectFinanceBill2024, #GenZRevolution and #OccupyParliament were monitored on X and TikTok to identify diffusion and virality trends. Based on posts that have received more than 10,000 interactions, which is the definition of a viral post, it was further analysed to trace the spread of frames and securitising narratives. TikTok videos were also analysed for multimodal aspects, such as images, audio and text layers. Instagram was used as a source of additional information through protest memes and short videos. In contrast, as an encrypted and private service, WhatsApp was accessed indirectly through interview accounts.

Traditional and official sources were incorporated into social media data. Daily Nation, The Standard, Citizen TV and KTN archival content were organised to follow the mainstream outlets' state and protester framing patterns. Government publications, such as press releases, police statements and parliamentary debates, were studied to include securitising speech acts and justification of extraordinary measures. Lastly, semi-structured interviews were conducted with twenty-five actors, including protest organisers and influencers, journalists, civil society leaders and policymakers, to gather primary data. These interviews provided valuable insights into the strategies of mobilisation and the understanding of securitisation. The records of protest events in geolocation formulas were gathered through human rights NGOs and open-source conflict data collection systems, such as ACLED, to coordinate the data on discursive and communicative expression with the physical protest processes.

The study's time frame is between June and August 2024, a period during which the introduction of the Finance Bill will be held, the height of the demonstrations, including the storming of Parliament and the direct state reaction is expected to take place. This window ensures that the analysis includes both the escalation and aftermath. The sampling of social media was based on the fifteen most commonly used protest hashtags, determined by frequency. An optimal approach was a purposive strategy in which viral content was considered, but still retained a broad post base for computational modelling. Purposive and snowball sampling were employed to identify interview participants, taking into account gender, regional diversity and actor category to minimise sampling bias.

Quantitative approaches were used to identify macro trends in digital mobilisation. Retweet and share networks were analysed by network to identify central actors and the communities according to which the information flowed. Measurements of degree centrality and modularity shed light on the role of the influencers and bridges within communities. Topic modelling (LDA) was an automated content analysis tool used to identify dominant themes, whereas sentiment analysis was used to measure the affective valence of protest discourse. A supervised classifier trained using a manually coded subset identified online communication as securitising frames. The analysis of time-series (Granger causality modelling) tested whether an increase in online activity was predictive of securitising the speech acts by state officials. Moreover, 200 viral TikTok videos were multimodally analysed alongside metadata, such as views and shares and visual and auditory coding was manually performed to investigate the mobilisation of images of violence and solidarity.

Qualitative methods were used to supplement these computational methods to get meaning and interpretation. Government statements, pressure conferences and parliamentary debates were subjected to critical discourse analysis (CDA) to detect securitising moves and the referent objects. The following analysis was based on the discursive production of youth dissent as something threatening and the extraordinary actions that discursively justified the legitimisation of such actions. NVivo software analysis of interview transcripts revealed common themes potentially related to mobilisation, state repression and misinformation. The coverage and analysis of editorials and media broadcasts on the protests followed the mediation and re-packaging of the securitisation of the protests by mainstream media outlets.

To bolster its validity and reliability, several strategies were employed. The intercoder agreement for the manual coding of protest videos and tweets was calculated and found to be 0.82, providing confidence in the consistency of the coding. Human-coded samples were used to evaluate the performance of automated classifiers. We employed inter-method triangulation, such as comparing network analysis findings with interview narratives, to ensure the convergence of results. Alternative thresholds of defining virality were tested to ensure robustness and a placebo time-series analysis of unrelated hashtags was performed to ensure that spurious correlations were avoided.

Ethical aspects dominated this, as protest research is sensitive. All interview participants provided informed consent and anonymity was ensured through the use of pseudonyms. Data on social media were anonymised and all publicly available data were analysed. Sensitive data that could make activists the target of persecution was omitted and all information was stored in encrypted repositories. The research was conducted in accordance with institutional ethical standards and the review board approved it. However, despite these protections, there are constraints. Bans on platform APIs limited the availability of TikTok and WhatsApp data, preventing the digital archive from being full. Falsehood, in particular, was not easy to trace, as it was in a transient state of circulation across closed networks. The data collected in the interviews are also prone to recall bias, as the participants looked back and may have distorted their recollections of the protest events. However, these shortcomings were mitigated using triangulation, transparency in the coding process and acceptance of uncertainties.

Overall, the approach combines the scope of computational analysis with the depth of discourse analysis and interview techniques. This design will allow the study to follow the macro-level trends of digital diffusion and the micro-level meaning of securitising speech acts. It can also be used to analyse the influence of misinformation and networked publics in the success or failure of securitisation. These methodological strands are combined to ensure that the research is not only empirically grounded in the analysis of the Gen-Z protest in Kenya, but also contributes to the further refinement of securitisation theory in digital areas of the Global South.

Findings

The empirical results of the research are covered in four thematic sections, including (1) the tendencies in digital mobilisation, (2) the securitisation chronicle, (3) the applicability of visual proof and counter-securitisation and (4) the impact of information disorder. The findings are pegged on the mathematical analysis of social media information, qualitative analysis of discourses and semi-structured interviews. Tables and figures are also included to show the significant patterns.

Digital Mobilisation Patterns

The scale and pace of mobilisation of the Gen-Z protests were unprecedented. The X and TikTok data analysis revealed that over 5 million posts, shares and interactions were generated between June and August 2024 on the top fifteen protest hashtags. Network analysis revealed a decentralised, interrelated mechanism of mobilisation. Although high-profile influencers (including musicians, comedians and online activists) dominated the centre of the network, it also featured several micro-influencers whose content experienced viral dissemination in localised clusters.

Table 2

Descriptive Statistics of Digital Mobilisation Data

Platform	**Posts Collected**	**Viral Posts (>10k interactions)**	**Distinct Hashtags**	**Median Engagement**
X (Twitter)	2,300,000	4,200	15	2,100
TikTok	1,800,000	1,700	12	8,900
Instagram	700,000	450	8	3,200
WhatsApp*	N/A (interview data only)	N/A	N/A	N/A

Note: The content on WhatsApp was not scraped directly, as it was encrypted; the insights were created through interviews.

Source: Researcher (2025)

Network analysis (Figure 2) shows that the mobilisation depended on no single leader. Instead, it was born out of networked publics, fitting the affective public notion developed by Papacharissi (2015). Activists stated that anyone could participate in the revolution with just a phone (Interview 7, activist). This devolution rendered the leadership of protests difficult for the authorities to co-opt or neutralise.

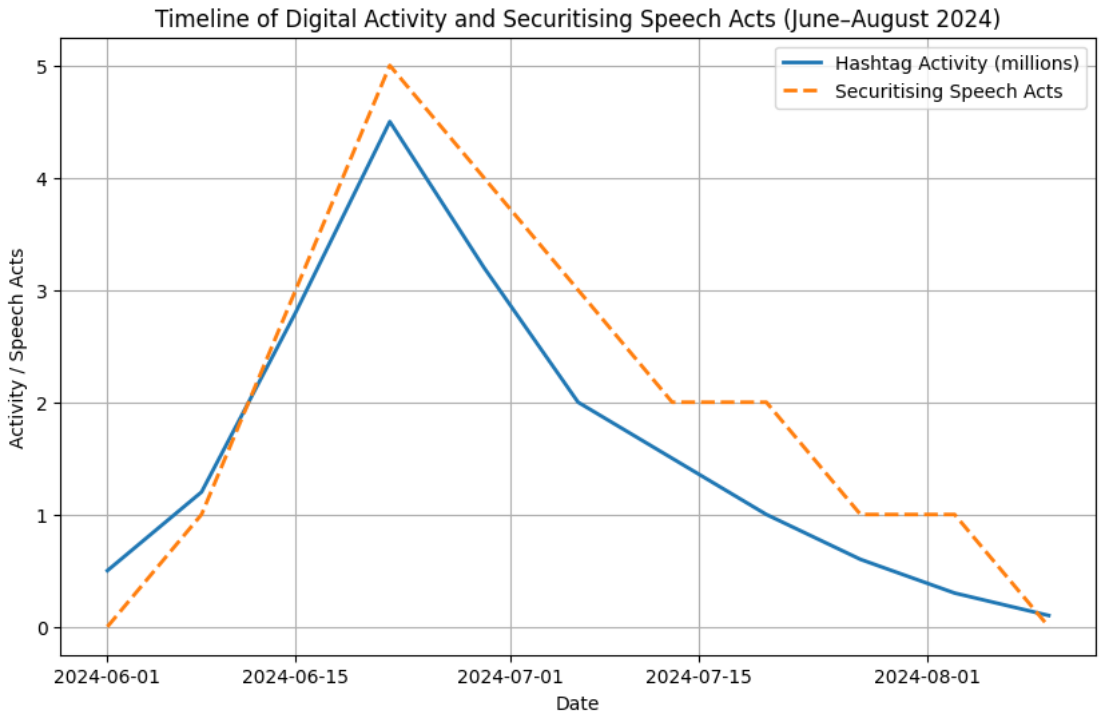
Securitisation Timeline

The second conclusion is that mobilisation and securitisation occur in time. A time-series analysis found that a surge in online activity was a regular predictor of securitising speech acts by government officials. In particular, the results of the Granger causality tests showed that large growths in protest-related hashtag activity predicted securitising statements in 72 hours at a 0.05 confidence level.

The relationship is presented in Figure 2, which demonstrates that the trajectory of online activity and securitising speech acts can be compared from June to August 2024.

Figure 1

Securitisation Timeline



Source: Researcher, (2025)

The sequencing confirms the assertion that the state's securitisation was reactive in that the visibility of digital mobilisation induced it. This dynamic was substantiated in interviews with policymakers; one senior official admitted that in a situation where TikTok portrayed Kenya as unmanageable, they had to discuss it in terms of national security (Interview 21, policymaker).

Visual Evidence and Counter-Securitisation

One of the most important aspects of the protests was the spread of visual evidence in the form of videos of police violence. A sample of 200 viral TikTok videos was coded, revealing that 42% of the videos recorded use of force by the state and 31% recorded protest solidarity (chants, marches, or creative performance). Framing protesters as being violent was only 10%. These images played a counter-securitising role. Through the recording of malpractices, demonstrators undermined the state's securitisation efforts. As an illustration, a popular video of a young protester being shot and killed by the police attracted international disapproval and the United Nations demanded that it calm down.

Table 3

Content Coding of 200 Viral TikTok Videos

Content Category	Frequency	Percentage
Police violence	84	42%
Protest solidarity	62	31%
Protest creativity (art, memes, satire)	34	17%
Protester violence	20	10%

Source: Researcher (2025)

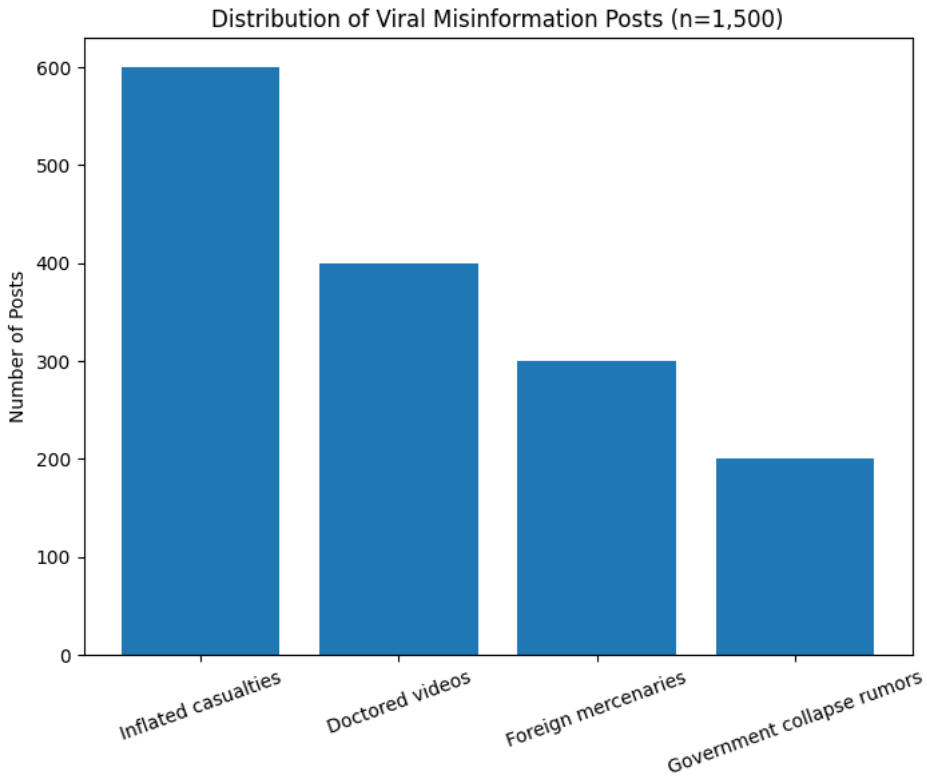
Interviewees repeatedly emphasised the significance of these visuals. According to one of the activists, we used TikTok to demonstrate the truth that the government could not. The videos showed the world our side (Interview 12, activist).

Disorder of Information and Dynamics of Protest.

Lastly, the findings reveal the presence of misinformation and disinformation. Both X and TikTok provided 1,500 posts that were determined to have untrue information. These were inflated casualty figures and fake pictures of foreign mercenaries.

Figure 2:

The Distribution of Misinformation Posts by Category



Source: Researcher, (2025)

False information made securitisation and counter-securitisation more difficult. To state officials, false claims undermined credibility and fostered a sense of distrust in the official casualty figures. In the case of protesters, false information contradicted valid complaints by confusing fact with fiction. Discontentment with this dynamic was found in interviews. One of the reporters said it was daily that we were forced to fact-check death tolls. Protesters claimed we were on the government side, yet we could not check it (Interview 18, journalist). On the same note, one of the protesters even said that we sometimes shared things too quickly and then realised they were false. However, by then, everybody thought they were right (Interview 10, activist).

A combination of the results sheds light on a Digital Securitisation Cascade. Networked publics created mobilisation quickly; protest frames made visible led to securitising speech acts; extraordinary measures were taken; counter-securitisation was a series of images of abuse; and misinformation increased instability throughout the process. Notably, securitisation was not one-sided: demonstrators did not passively accept the state's discourse but used digital technologies to oppose the delegitimisation process. The cascade was recursive. One phase formed the other, creating feedback mechanisms that extended mobilisation and securitised it even more. As of August 2024, the strength of protests had abated, although the communication security nexus they highlighted remains a pressing concern for Kenya regarding the resilience of democracy.

Discussion

To begin with, digital visibility, due to networked publics on X, TikTok and Instagram, had a strong relationship with state securitising efforts: time-series and Granger-causality tests reveal that online action spikes were always strictly followed by securitising speech acts within a narrow timeframe (approximately 72 hours). This sequencing suggests that securitisation was responsive to digital amplification, rather than anticipatory or preemptive. Second, visual evidence created by the protesters (videos of police brutality, solidarity video) limited the coercive latitude of the state materially by creating both domestic and international examination. Third, misinformation, which was measured by the number of verifiably false viral posts, not only weakened the official credibility but also complicated the counter-narratives of protesters, creating a destabilising effect that geometrically increased contestation in the digital environment. These empirical trends can be directly overlaid onto the Digital Securitisation Cascade suggested above, thereby confirming the cascade as a heuristic for analysing digitally mediated securitisation.

The result suggests that securitisation theory needs to be recalibrated for the digital age. Classic Copenhagen-School formulations highlight the speech acts of the elite and their acceptance by the audience as the critical process that transforms political issues into existential challenges. The central role played by speech acts is verified in the Kenyan case, but the case also illustrates that the audience is no longer a mass and is no longer situated in concrete spaces of physical publicness alone; networked publics are audiences and agents actively engaged in counter-securitising action. The protesters did not simply await a verdict from the political elites; they created alternative evidence, frames and globalised solidarities that squarely challenged securitising claims. The proposed alteration of the status quo, then, would be contested securitisation: securitising moves are still needed but still not sufficient to achieve extraordinary politics in circumstances where digitally networked publics can (1) anticipate alternative framings in advance; (2) provide multimodal counter-evidence; and (3) exercise transnational normative pressure that increases the reputational costs of disproportionate state action. This recursion is captured in the cascade, which involves visibility leading to securitisation; securitisation is an invitation to counter-securitisation through visuals and frames and information disorder facilitates this process.

This reframing has three theoretical implications. First, it prioritises algorithmic mediation as an intervening variable: securitising and counter-securitising dynamics, meanwhile, are accelerated by platform affordances (visibility, virality, recommendation logics) and reduce the time available for deliberation and response. Second, it shows the normative ambivalence of networked publics. As they can provide quick democratic forms of expression and oversight, they can also spread misinformation capable of delegitimising legitimate claims and triggering increased policing. Third, challenged securitisation requires scholars to analyse audience

heterogeneity as analytically central, as different publics (domestic mainstream, diasporic and global human-rights constituencies) judge securitising claims based on different sets of repertoires of evidence, which in turn influence state strategies.

The policy trade-offs that the results shed some light on are harsh and avoidable. Making online harmful by controlling a site (removing content or de-ranking), or temporarily blocking (as an enforcement of online governance), can slow the spread of misinformation. However, it can also prevent the publicity of state crimes and the records of legitimate demonstrations. Conversely, a hands-off position preserves visible channels of evidence capable of opposing state power at the cost of revealing the information space to falsehoods that make it more volatile and securitised. Similarly, law-enforcement procedures that focus on quick containment minimise disorder in the streets in the short run but can also result in long-term delegitimisation when images of maltreatment circulate. Procedures that focus on restraint and transparency lead to reduced political expenses but can be viewed as ineffective in times of acute uncertainty. Such trade-offs require procedurally sound, rights-sensitive and temporally constrained governance solutions.

There are restrictions on generalisability claims. The available methodological limitations are that API access to TikTok and the inability to directly scrape encrypted WhatsApp data only mean that some private and high-impact flows are only partially observable; participant recall bias and the time-limited nature of the study (June 2024- October 2024) mean that even fewer constraints on making inferences about longer-term outcomes are possible. These reservations warn against generalising the Kenyan situation to all African democracies. There are, however, limited comparative lessons. In places where young populations and mobile penetration are high and a compromised state legitimacy co-exists with these traits (as in some regions of the West and Southern Africa), similar tendencies might occur: accelerated, informal mobilisation; amplified visibility through algorithms; securitised in response; and unstable narratives driven by both visualised data and fake news. The strength and consequences of these processes will depend on the institutional characteristics, including the independence of the judiciary, media plurality, the capacity of civil society and the professional ethics of the security services, which will mediate the differences between contested securitisation and democratic accountability or repression.

Overall, this paper reframes securitisation as a digitally disputed practice whereby networked publics have a material capacity to shape when extraordinary state actions are approved and when they are not. The Digital Securitisation Cascade elucidates the recursive, algorithmically mediated and information-saturated nature of contemporary securitisation. In practice, the evidence does not support binary decisions between censoring and permitting, but instead calibrated institutional responses involving procedural de-escalation, fast independent checking and transparent security operations to minimise the political incentives to securitisation and maintain social order.

Conclusion

This evidence indicates that the modern form of securitisation can no longer be considered a unidirectional elite action. However, it is a recursive process that runs through networked publics and platform dynamics. Digital visibility enhances security politics: viral content often leads to reactive securitising speech acts and protesters and civil society can generate multimodal counter-evidence that can constrain or delegitimise the use of force because it is publicly visible. Meanwhile, the high rate of circulation facilitates a state of information anarchy that, on the one hand, compromises plausible assertions and on the other, gives justifications to securitisation. This situation produces a shortened political attention span in which the institutional reactions previously based on considered action must now be acted upon within hours rather than weeks.

Policy must, instead, not create a false dichotomy between the uninhibited nature of the digital and the repressive nature of the controls, but must establish procedural safeguards that balance the demands of the populace with the defences of rights. The mentioned five recommendations transform the primary findings of the research into the practical governance proposals: they slow down the vicious circle of harm, promote

restraint by openness and supervision, improve the evidentiary ecology by platform and civil-society checking and conditionalise technical cooperation by accountability. All these actions reduce the political compensation of securitisation and hold the essential instruments of ensuring order.

Nonetheless, it is not without limitations: digital interventions may not be termed panaceas and institutional reform requires political will, resources and long-term involvement of civil societies. Nevertheless, when implemented, the recommendations will establish systemic incentives for de-escalation and enhance democratic resilience where youth demographics, mobile penetration and contentious legitimacy collide. To conclude, contest securitisation does not necessarily end in repression; networked publics through well-calibrated, transparent and rights-respecting policies can serve as a corrective power force strengthening accountability instead of exceptionalism.

Policy Recommendations

De-escalation Structure of Procedures to protect the company against the dangers of reflexive securitisation and reputational risk associated with harsh actions against demonstrations. It will be the responsibility of the National Police Service (NPS), the Ministry of Interior and the County Governments. Implement a legally required graduated response system with strict limits of each response level; non-coercive first response (negotiation teams, containment corridors) and stand-alone pre-authorisation of crowd-dispersal weapons use. At least once in three months, incident-level compliance reports can be made publicly available within 30 days.

Open Incident Reporting and External Control. Rationalisation: Intimate information gaps that contribute to disputational accounts and falsehoods.

Accountable: Ministry of interior, Parliamentary committee on security, office of the Ombudsperson. Measures: Publication of operation briefs (purpose, use of force), time-stamped by the direct security agency during the first 72 hours of major crowd events; an independent oversight organisation with the power to investigate abuse independently. Surveillance: Semi-annual public scorecards of timeliness and completeness of reporting.

Platform- State Rapid Verification Partnerships. Reason: Enhance evidentiary clarity and put damaging viral misinformation on the back burner. Accountable: Communications Authority of Kenya (CA), big platforms (X, TikTok, Meta), certified fact-checkers and media organisations. Measures: Pre-agreed Memoranda of Understanding to verify when there is unrest quickly; surfaces to expose provenance metadata and contextual labels ("Under verification") to viral protest content; throttling protocols that are bound by time in cases where the content plausibly poses a threat to others. Follow-Ups: Check and independent auditing are done every six months.

CVDL Houses. Justification: Establish resilience in society against misinformation and enhance channels of evidence by citizens. Accountable: Civil society partnerships, universities, donor partners. Measures: Invest in regional checking labs and grassroots digital-literacy campaigns; develop secure, anonymising submissions portals where the citizen evidence can be submitted with legal defence of the whistle-blowers. Monitoring: Measures how fast online responses to viral claims are, how many people are contacted by literacy programs and how many secure submissions are made.

Linked Accountability to Technical Assistance (Conditional). Reason: It has to stop the transfer of technologies that entrench securitisation without protection. Authority: International donors, development partners and the Ministry of Foreign Affairs. Measures: Link technical assistance on cybersecurity and policing to visible legal protection (judicial control, use-logs, human rights training); focus funding on institutional capacity (oversight, media freedom) rather than surveillance technology. Surveillance Tech. Surveillance: Assist subject to independent compliance auditing regularly (annually).

References

Anderson, D. M., & McKnight, J. (2015). *Kenya at war: Al-Shabaab and its enemies in Eastern Africa*. *African Affairs, 114*(454), 1–27.

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

Balzacq, T. (2011). *Securitisation theory: How security problems emerge and dissolve.* Routledge.

Barasa, M., & Agwuele, A. (2021). A Repertoire of Bukusu Nonverbal Communicative System: Some Gender Differences. In *The Palgrave Handbook of African Oral Traditions and Folklore* (pp. 377-401). Cham: Springer International Publishing.

Battocchio, A. F., Wells, C., Vraga, E., Thorson, K., Edgerly, S., & Bode, L. (2023). Gen Z's civic engagement: News use, politics and cultural engagement. In *Handbook of Digital Politics* (pp. 168–195). Edward Elgar Publishing.

Bennett, W. L., & Segerberg, A. (2012). *The logic of connective action: Digital media and the personalisation of contentious politics*. Cambridge University Press.

Bosch, T. (2017). Twitter activism and youth in South Africa: The case of# RhodesMustFall. *Information, communication & society*, *20*(2), 221–232.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Buzan, B. (2008). *People, states & fear: an agenda for international security studies in the post-Cold War era*. ECPR press.

Castells, M. (2012). *Networks of outrage and hope: Social movements in the Internet age*. Polity Press.

Coulibaly, S. (2023). Exploring health misinformation on WhatsApp within the African migrant and refugee community in Southeast Queensland (SEQ). *Media International Australia*, *189*(1), 8–23.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). Sage Publications.

DeLuca, K. M., Lawson, S., & Sun, Y. (2012). *Occupy Wall Street on the public screens of social media: The many framings of the birth of a protest movement*. *Communication, Culture & Critique, 5*(4), 483–509.

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51–58.

Goldstein, D. M., & Rotich, J. (2008). *Votes, shoes and the Internet: The 2007 Kenyan election and its aftermath*. *International Journal of Communication, 2*, 92–98.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. The MIT Press.

Hodzi, O., & Zihnioğlu, Ö. (2024). Beyond 'networked individuals': social-media and citizen-led accountability in political protests. *Third World Quarterly*, *45*(1), 43-60.

Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU.* Routledge.

Ignatov, A., & Kerimi, D. (2025). Russia's securitised approach to AI sovereignty. *The African Journal of Information and Communication*, *2025*(35), 1–11.

Ingutia, B. C. (2025). The Impact of Social Media in Shaping Kenya's Politics: Gen Z Uprising and the Rejection of the Finance Bill 2024. *African Multidisciplinary Journal of Research*, *1*(1), 47–68.

Kabata, V., & Garaba, F. (2020). The legal and regulatory framework supporting the implementation of the Access to Information Act in Kenya. *Information Development*, *36*(3), 354–368.

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

McCoy, D., Roberts, S., Daoudi, S., & Kennedy, J. (2023). Global health security and the health-security nexus: principles, politics and praxis. *BMJ Global Health*, *8*(9), e013067.

Muchiri, B., Odoyo, W., Kiptoo, J., & Cheboi, M. (2025). The Phone vs. The Bullet: Kenya's Gen Z Revolution and the Narrative War. *African Studies Review*.

Mohamed, A., & Tohami, A. (2013). *The Rupture in State-Society Relationships and the Prominence of Youth Activism in Egypt: Opportunities, Strategies and New Models of Mobilisation* (Doctoral dissertation, Durham University).

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. PublicAffairs.

Mumma-Martinon, C. M. M., Maina, L. W. M., & Kimuyu, J. J. K. (2024). The Rise of State-Sponsored Cyber-attacks: The Case for International Cooperation in Strengthening Defence Systems. *National Security: A Journal of the National Defence University-Kenya*, *2*(1), 114-133.

Nyabola, N. (2018). *Digital democracy, analogue politics: How the Internet era is transforming politics in Kenya*. Bloomsbury Publishing

Omanga, D., & Mainye, P. C. (2019). North-South collaborations as a way of 'not knowing Africa': Researching digital technologies in Kenya. *Journal of African Cultural Studies*, *31*(3), 273–275.

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

Ortiz, J., Young, A., Myers, M. D., Bedeley, R. T., Carbaugh, D., Chughtai, H., ... & Wigdor, A. (2019). Giving voice to the voiceless: The use of digital technologies by marginalized groups. *Communications of the Association for Information Systems*, *45*(1), 2.

Owuondo, J. O. (2025). Kenya's Hybrid Warfare Threats and National Security Infrastructure. *National Security: A Journal of the National Defence University-Kenya*, *3*(1), 84-96.

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

Petla, V. (2023). Information disorders and civil unrest: An analysis of the July 2021 unrest in South Africa. *Digital Policy Studies*, *2*(1), 23-31.

Stritzel, H. (2014). Securitization theory and the Copenhagen School. In *Security in translation: Securitization theory and the localization of threat* (pp. 11-37). London: Palgrave Macmillan UK.

Sunstein, C. R. (2018). *Republic: Divided democracy in the age of social media*. Princeton University Press.

Tsanis, K., Webb, H. C., & Warsama, I. (2025). Cybersecurity Matters in Fintechs in Africa. In *The Palgrave Handbook of fintech in Africa and the Middle East: Connecting the Dots of a Rapidly Emerging Ecosystem* (pp. 921–949). Singapore: Springer Nature Singapore.

Vromen, A. (2016). Digital citizenship and political engagement. In *Digital citizenship and political engagement: The challenge from online campaigning and advocacy organisations* (pp. 9-49). London: Palgrave Macmillan UK.

Wamuyu, P. K. (2020). The Kenyan social media landscape: Trends and emerging narratives, 2020.