

Effect of Digital Electoral Mobilization on National Security in Nairobi City County, Kenya

Jairus Mutinda Kilatya, Prof. Ngari Lazarus Kinyua (PhD), Dr. Odhiambo Evans Onyango

Department of Security, Diplomacy and Peace Studies, Kenyatta University, September, 2025

DOI: <https://dx.doi.org/10.47772/IJRISS.2025.909000299>

Received: 18 September 2025; Accepted: 24 September 2025; Published: 09 October 2025

ABSTRACT

This study specifically analyzed assessed the effect of political party online electoral mobilization on national security. Human Security and Securitization Theories explained how online electoral mobilization can threaten individual safety and national stability, and how such threats are framed to justify state security responses in Nairobi's informal settlements. The study used a **mixed-method design** with 400 purposively sampled respondents from Nairobi's informal settlements. Data were collected through interviews, questionnaires, and focus groups, and **thematic analysis** was applied to organize qualitative insights into themes, providing a comprehensive understanding of electoral security and social dynamics. This study observed that digital platforms can enhance electoral security by enabling real-time alerts, rumour control, and peace campaigns, helping communities and authorities prevent violence. However, they also pose risks, as misinformation, hate speech, and online echo chambers can quickly escalate tensions and undermine social cohesion, creating a national security challenge. Digital platforms aid political engagement and peace-building during elections but can also spread misinformation and incite violence, posing national security risks. Addressing this requires balanced monitoring, digital literacy, and responsible platform use.

BACKGROUND TO THE STUDY

The electoral environment in informal settlements is closely tied to national security due to the socio-political and economic fragilities that define these areas. Overcrowding, poverty, joblessness, inadequate state presence, and weak security structures create fertile ground for political manipulation, ethnic or patronage-based politics, and criminal activity during elections. Such vulnerabilities allow gangs and militant groups to flourish, fueling instability that threatens both community safety and national cohesion (Haysom, 2013; Wilkinson, 2004).

This is not unique to Kenya; similar patterns emerge globally. In India, slums are shaped by clientelist politics (Sharma, 2013), while in Brazil, favelas remain under the influence of gangs and militias despite a formal electoral framework (Wacquant, 2008). Karachi's informal settlements in Pakistan have long been arenas of violent competition between political militias (Gazdar, 2007). In Mexico, cartels distort elections through intimidation and collusion (Camp, 2017), while in the Philippines, political dynasties and warlords maintain dominance through coercion (Mendoza, 2012). Across Africa and the Middle East including Ghana, Nigeria, Sudan, Egypt, Morocco, South Africa, and Uganda weak institutions, authoritarian tendencies, violence, and exclusion undermine the credibility of elections and erode security (Gyimah-Boadi, 2009; Lindberg, 2006; Mwagiru, 2012).

Kenya reflects these global dynamics, with informal settlements becoming flashpoints for electoral violence driven by ethnic mobilization, competition for political power, and the influence of organized criminal groups (Kanyinga & Long, 2009). Despite interventions by bodies like the National Cohesion and Integration

Commission (NCIC) and civil society organizations promoting voter education, challenges such as mistrust in electoral institutions, rapid urban growth, and fragile governance structures perpetuate insecurity (Mutahi, 2018; Omolo, 2010). Taken together, the global and local picture demonstrates that in marginalized urban spaces, electoral politics and insecurity are deeply intertwined, making credible, inclusive, and peaceful elections indispensable for sustaining national stability.

Statement of the Problem

In Kenya, digital and online platforms have become central to electoral mobilization, but in informal settlements such as Mathare, Kibera, Korogocho, and Mukuru, they also fuel insecurity. Political elites and their agents exploit these platforms to spread disinformation, incite ethnic tensions, and intimidate opponents, heightening the risk of violence in already fragile communities marked by poverty, weak state presence, and mistrust of institutions. State responses to harmful digital mobilization are fragmented and reactive, while civil society lacks the authority to curb its negative impacts. Community leaders, though influential offline, have limited effectiveness in countering online incitement, leaving a gap between digital manipulation and on-the-ground security risks. This convergence of online electoral mobilization with entrenched vulnerabilities in informal settlements poses a significant threat to national security and undermines confidence in democratic processes.

Specific Objective

Assessing the effect of political party online electoral mobilization on national security

Justification

Elections in Nairobi's informal settlements are frequently marked by insecurity and violence, with community leaders playing a critical yet often overlooked role in promoting peace. Investigating their impact is essential for ensuring national stability and strengthening democratic processes, as it generates evidence to guide policy, enrich scholarly discourse, and support local peace-building efforts. This research will assist the Government, particularly the Ministry of Interior, by providing policy recommendations to counter divisive political practices that undermine security. Additionally, it will raise public awareness about the risks of political manipulation during campaigns. From an academic perspective, the study advances knowledge by exploring under-researched areas such as electoral campaign tactics, the influence of community leaders, government interventions, and patterns of displacement within informal settlements.

LITERATURE REVIEW

Digital electoral mobilization has transformed political campaigning, voter engagement, and election processes worldwide. Social media and encrypted messaging apps allow political actors to reach large audiences instantly and mobilize voters efficiently. However, these tools also pose national security threats by spreading disinformation, polarizing societies, and undermining trust in democratic institutions. The 2017 French presidential election, as analyzed by Ferrara (2017), illustrates this risk: coordinated bot campaigns on Twitter spread fake documents and conspiracy theories targeting Emmanuel Macron, influencing voter perceptions and eroding confidence in the electoral process. While Ferrara's study details bot behaviors, it does not address the policies or institutional measures needed to prevent such digital influence operations, particularly in countries with weak cyber defenses.

Studies on digital electoral mobilization highlight both its democratic potential and national security risks. Stella, Ferrara, and De Domenico (2018) show that bots during the Catalan independence referendum amplified polarizing content, exacerbating societal cleavages and potential violence, though they do not explore concrete countermeasures for security agencies. Shao (2017) found that bots disproportionately spread low-credibility material in Western elections, skewing discourse and threatening electoral integrity, but their

work overlooks governance strategies to mitigate such influence while respecting individual rights. In Nigeria's 2023 elections, Aideloje, Sylvester, and Jacintha (2024) observed that social media mobilized youth participation but also intensified pre-election tensions and real-life conflicts, with limited discussion on institutional protections.

Historical analysis by Ngange and Elonge (2019) of Cameroon shows that even with low internet penetration, parties experimented with digital mobilization, increasing political reach, though security strategies were underdeveloped. Across these cases, digital mobilization emerges as a dual tool enhancing engagement but also posing risks to stability while research gaps remain in effective institutional and policy responses.

Recent studies on digital electoral mobilization in Kenya highlight both its democratic potential and national security risks. Daka, Oando, and Majiwa (2024) argue that reliance on proprietary electoral technologies introduces vulnerabilities, including cyber-interference and loss of transparency, while leaving unclear the role of state agencies in overseeing private sector involvement. Wefwafwa, Wekesa, and Gagliardone (2025) show that WhatsApp facilitates voter mobilization but also spreads unverified information, presenting a privacy-versus-security dilemma.

Harris, Kamindo, and van der Windt (2022) demonstrate that SMS campaigns can increase voter registration but raise concerns about surveillance and misuse of personal data. Mare, Mainye, and Manga (2024) highlight the influence of digital actors such as influencers, consultants, and bots in shaping electoral debates, with limited regulation contributing to disinformation and societal polarization. Across both African and global contexts, digital electoral mobilization emerges as a double-edged sword: it can enhance democratic participation while simultaneously threatening national security through disinformation, polarization, and potential violence (Ferrara, 2017; Stella, 2018; Shao, 2017; Aideloje, 2024; Wefwafwa, 2025).

Several research gaps emerge from the synthesis of existing literature on digital electoral mobilization. There is limited empirical analysis of how security agencies can intervene in digital mobilization without infringing on rights to free expression and privacy. Most studies focus on short-term electoral events, leaving the long-term impact of digital mobilization on national security largely unexplored. Third, the role of private technology companies in electoral processes and the associated security risks remains underexamined. Fourth, citizens' perceptions of security interventions in the digital sphere a key factor in electoral legitimacy have received little attention.

Theoretical Framework

This study adopted the theories of Human Security Theory by the United Nations Development Programme (1994) and Securitization Theory by Barry Buzan (1998). Human Security theory emphasizes protecting individuals from multiple threats and empowering them to safeguard their welfare. In Nairobi's informal settlements, elections often cause violence, displacement, and livelihood disruptions, making elections agents of insecurity. Applied to online electoral mobilization by political parties, the theory highlights how digital campaigns can expose citizens to risks like misinformation, cyber harassment, and political manipulation, which threaten personal and community security and, in turn, national stability. The theory underscores the need to safeguard citizens while allowing safe engagement in electoral processes.

Securitization Theory, developed by Barry Buzan, views security as socially constructed through speech acts that frame issues as existential threats. In Nairobi's informal settlements, electoral struggles are often securitized, justifying increased state presence or coercive actions. Securitization Theory helps analyze how online electoral mobilization by political parties can be framed as a threat to national security, justifying state interventions. It highlights how digital campaigns influence government responses, public perceptions, and democratic processes, showing the interplay between political actors, digital platforms, and security institutions in shaping national stability.

RESEARCH METHODOLOGY

Research Design

The study used a mixed-method design combining a descriptive survey and historical research to examine electoral security in Nairobi's informal settlements, focusing on Kibera, Kawangware, and Mathare. The research involved about 2 million residents and key political and security actors, capturing patterns of election-related insecurity and tracing historical trends in violence and local peace mechanisms.

Sample Size and Sampling Procedure

Purposive sampling was employed to select participants with in-depth knowledge of electoral politics and security challenges, including local leaders, security officers, election monitors, and residents with first-hand experiences of electoral violence. A total of 370 respondents participated, 100 from four settlements (Kibera, Mathare, Korogocho, and Eastleigh) and 300 political actors and community representatives with 274 completed questionnaires, ensuring contextually rich data on the complex relationship between electoral processes and security in marginalized urban areas.

Table 1.1: Sample Size

Category	Population	Proportion	Sample Size= (Proportion*Total Sample size(400))
Citizens	2,000,000	Purposively selected	200
Political players	69	17.5%	34
IEBC	11	2.5%	6
Election observers	30	7.5%	15
Religious leaders	50	12.5%	25
NPS	200	50%	100
Representative of Residents	40	10%	20
Total		100%	400

Source: Researcher (2025)

Methods of Data collection and Analysis

The study sampled **400 respondents** to capture diverse perspectives across Nairobi's heterogeneous informal settlements, allowing comparisons between population subsets and enhancing statistical power to examine links between electoral processes and national security. **Data collection** combined interviews, semi-structured questionnaires, and focus group discussions (FGDs), providing in-depth insights from key informants, standardized quantitative data, and community perspectives on electoral security. **Thematic analysis** was used to code and group qualitative data into themes, capturing participants' experiences and views, with findings presented in **tables, diagrams, and narrative form** to provide a rich interpretation of complex social dynamics.

Response Rate

The study targeted 400 participants across the different informal settlements in the Nairobi City County, including Kibera, Mathare, Korogocho, and Eastleigh. Of these, 370 respondents completed the questionnaires and returned them, thus resulting in a response rate of 92.5%. Mugenda & Mugenda (2003) assert that a 70% or above response rate is acceptable in the context of social science research, thus justifying the reliability and generalizability of the findings of the current study.

The 30 non-participants were individuals within the target population of people who did not participate in the study, possibly because of attrition, lack of cooperation, or inaccessibility. Although their refusal will inject potential demographical or attitudinal differences, their high base level of 92.5 per cent response rate eliminates significant risks of observed statistical bias or impaired generalizability, improving the accuracy of the findings in their non-response.

Table 4.1: Response Rate

Target Respondents	Actual Responses	Response Rate (%)
400	370	92.5

Source: Researcher (2025)

Effect of Digital Electoral Mobilization on National Security in Nairobi City County

Introduction

This section examines how political parties and online electoral mobilization influence national security in Nairobi's informal settlements. It highlights the growing role of digital platforms in shaping political participation, as well as their potential to trigger election-related tensions and violence. Given that residents are politically aware but socially and economically marginalized, they are particularly vulnerable to both the benefits and risks of online engagement. The analysis focuses on how local actors used digital spaces during general elections and the resulting security implications, with findings organized into thematic patterns derived from the data.

Patterns of Digital Space Mobilization

Study findings indicate that digital platforms played a significant role in the electoral process in Nairobi's informal settlements, particularly in facilitating information sharing and community discussion. WhatsApp emerged as the most widely used platform, followed by Facebook and Twitter, with usage patterns reflecting differences in age, digital literacy, and political engagement. While these tools were valued for their immediacy and perceived trustworthiness compared to traditional media, the way they were used varied across settlements, influenced by local socio-political dynamics and youth density. Other platforms like TikTok and YouTube were mentioned mainly as sources of entertainment or commentary rather than active political engagement.

Digital Platform Usage During Elections in Informal Settlements

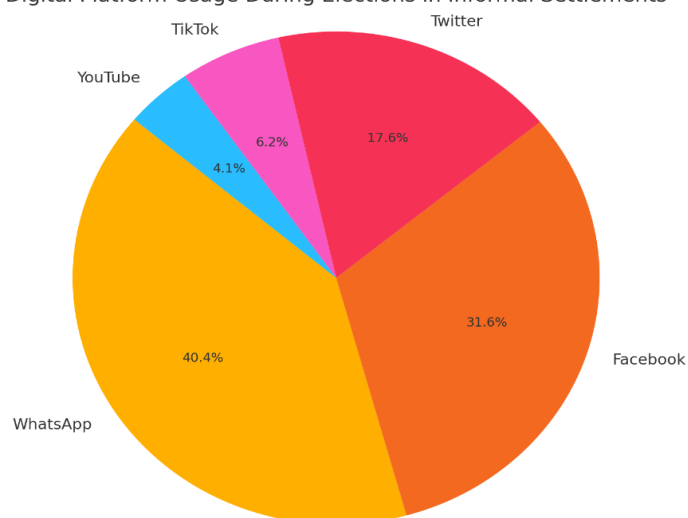


Figure 1.1 Platform Usage Frequencies Among Respondents.

Source Field Data

The high use of WhatsApp (40.4%) and Facebook (31.6%) for political engagement in Nairobi's informal settlements has significant national security implications. WhatsApp, favored for its affordability and accessibility, serves as a primary source of political information, campaigns, and security messages. Its private and group-based communication, however, makes it difficult to monitor, facilitating the rapid spread of misinformation, disinformation, and potentially violent content, which can threaten social cohesion and electoral stability. Facebook, on the other hand, is widely used for broader political mobilization, campaign announcements, live streaming rallies, and influencing public opinion, including discrediting opponents. This dual role of digital platforms as tools for civic engagement and channels for misinformation highlights the need for measures to promote responsible information sharing, especially during elections, to safeguard national security and democratic governance. Studies, such as by IDS (2021), show that in settlements like Mathare, Kibera, and Korogocho, WhatsApp often surpasses traditional media in local political communication, while Facebook facilitates large-scale mobilization and political influence.

Current research on digital rights by ARTICLE 19 Eastern Africa (2022) shows that young people and grassroots activists in the informal settlements (such as Mathare and Kibera) in Nairobi are turning to Twitter to create greater political accountability and visibility. The use of hashtags such as #RespectOurVote, #SabaSabaMarchForOurLives, and #RejectElectoralFraud were established as informal campaigns organised by residents with little access to conventional media. Thus, this platform was then used to advocate and take responsibility.

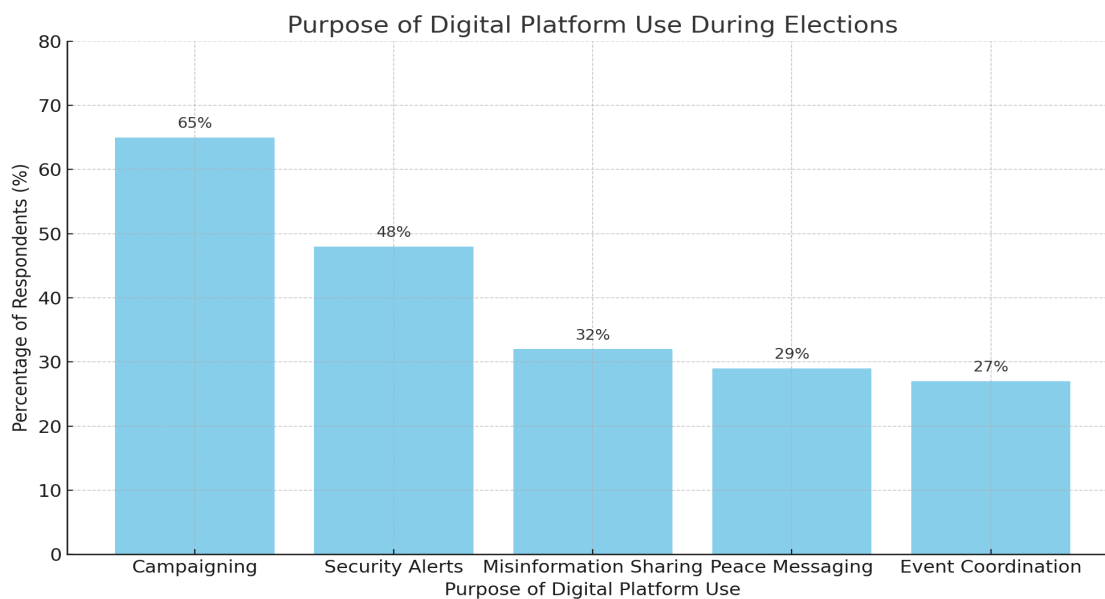


Figure 1.2 : Purpose of Digital Platform Use During Elections

Source Field Date 2025

The study highlights how digital platforms play a critical role in elections within Nairobi's informal settlements, with significant implications for national security. Campaigning (65%) is the most common use, though seemingly benign, it can spread politically charged content that may incite unrest. Security alerts (48%) show citizens' reliance on online platforms for real-time safety information, yet they risk manipulation and panic. Misinformation sharing (32%) directly threatens national stability by undermining trust and potentially inciting violence, while peace messaging (29%) and event coordination (27%) are positive but less prevalent.

Settlement-specific patterns reveal differences: Kibera showed high digital campaign activity, with youth mobilization and partisan WhatsApp groups intensifying political polarization and online conflict. Mathare focused more on security-related communications, creating effective community-led early warning systems, but also risking vigilantism and misinformation. Korogocho exhibited lower digital activity due to limited smartphone access and digital literacy, although NGOs facilitated peace-focused groups. Eastleigh favored

Twitter and Telegram for rapid coordination, reflecting a literate, diasporic population able to respond quickly to local events.

Overall, digital platforms provide unique opportunities for political engagement, community safety, and rapid local coordination. However, unregulated or partisan use, misinformation, and over-reliance on individual digital literacy pose serious national security risks, underlining the need for supportive mechanisms to counter disinformation and ensure information integrity.

Digital platforms in Nairobi's informal settlements play a dual role in electoral processes, shaping both national security risks and community resilience. Their speed, informality, and localization make them effective for real-time reporting, economic coordination, and citizen mobilization, but these same features render them vulnerable to misinformation, disinformation, and propaganda. Malign actors can exploit these networks to spread fear, incite violence, or polarize communities, while reliance on informal channels can bypass official security mechanisms, weakening state control.

WhatsApp, Telegram, and Facebook dominate local digital engagement, with residents rapidly sharing security alerts, election updates, or community warnings. However, unverified claims, particularly during vote counting, have triggered panic and threatened social cohesion, illustrating the fragile balance between rapid communication and national security.

Positive interventions emerged through peace messaging campaigns, youth-led initiatives, and NGO programs, which used local networks to promote verified information, unity, and social resilience. These bottom-up approaches proved more effective than top-down government interventions, building trust and countering polarization. Kibera and Mathare experienced high digital political activity and security coordination, while Korogocho faced lower engagement but relied on community-based initiatives. Eastleigh leveraged more literate, diaspora-linked platforms like Telegram and Twitter for rapid coordination.

Implication of Digital Mobilization to National Security

The mobilization of digital space had a dual role in defining the landscape of national security during the electoral process within informal settlements in Nairobi. On the one hand, digital platforms such as WhatsApp, Facebook, and Twitter have become important instruments for early warning, the dissemination of news, and the policing of communities. Conversely, the same media were used to propagate hate and fearmongering, fake news, and increase tension and violence in some cases. The answers provided by the major respondents demonstrated the positive and negative aspects of the digital platforms in the context of electoral campaigns and their impact on security. Table 1.2 contains the findings.

Table 1.2 : Implications of Digital Mobilization on Security

Statement	N	SD	D	N	A	SA	Mean	Std. Deviation
Digital mobilization has facilitated the ability to share verified information	274	6%	16%	4%	40%	34%	3.72	0.54
Digital platforms have helped in enhancing community policing hence influencing security	274	3%	15%	3%	47%	32%	3.98	0.49
Digital platforms are reshaping information dissemination and perception of reality, directly impacting national security	274	8%	14%	2%	49%	31%	4.02	0.38
Digital space platforms in Kenya have been used to fuel tribal and ethnic tensions which leads to violence during elections	274	7%	10%	2%	44%	37%	4.07	0.24
Digital media despite its positives has also become catalysts of divisions during elections to the detriment of national security	274	8%	7%	1%	45%	39%	4.21	0.12

Digital space platforms in Kenya have been used to fuel tribal and ethnic tensions which leads to violence during elections	274	9%	9%	3%	43%	36%	4.05	0.22
Most digital media spaces in Kenya have become platforms of political propaganda against certain political opponents	274	11%	13%	3%	40%	33%	3.67	0.85
Average Scores	274						3.96	0.41

Source: Research Data (2025)

The study findings from Table 1.2 indicate that digital mobilization has both positive and negative impacts on elections and national security in Kenya. On the positive side, respondents agreed that digital platforms enable faster sharing of verified information (Mean=3.72, SD=0.54), improve community policing (Mean=3.98, SD=0.49), and transform information delivery and perception, influencing national security (Mean=4.02, SD=0.38). A significant proportion of respondents acknowledged these benefits, demonstrating that online networks can enhance community organization and security during elections.

Conversely, digital spaces were also seen as sources of electoral insecurity. Respondents agreed that social media incites tribal and ethnic tensions (Mean=4.07–4.05), fosters political division (Mean=4.21), and is used to propagate political propaganda (Mean=3.67). These findings align with previous studies, including Verdeja and Hook (2022), Oluleye (2023), and Wambua (2020), which highlight the potential of digital platforms to spread misinformation, political lies, and polarization, threatening national security.

Key informant interviews and focus group discussions across Kibera, Mathare, Korogocho, and Eastleigh revealed nuanced perceptions of digital platforms, emphasizing their dual role in both mitigating and aggravating electoral insecurity. Overall, the findings reflect mixed outcomes regarding the usefulness of digital media in enhancing election security.

Early Warning Systems

The digital sphere, particularly through informal WhatsApp groups, has enabled community-based early warning systems in vulnerable urban areas. Over 54% of survey respondents reported receiving real-time alerts on security threats, such as demonstrations, armed youths, or suspicious vehicles. These networks allow communities to respond quickly, often instructing people where to hide or avoid, compensating for perceived gaps in formal security provision. While these systems can save lives and property, they also pose national security risks, including the spread of misinformation, panic, or mob violence, and reflect strained relationships with formal security agencies. A 2022 Kenya Red Cross study noted that during elections, such local networks helped residents take precautionary measures, sometimes even informing official police actions. In places like Eastleigh, WhatsApp groups among business or religious circles helped guide safe movement and prevent conflict escalation.

Information Dissemination

Digital mobilization played a crucial role in rapidly sharing verified information during elections, with 62% of respondents noting that platforms like WhatsApp helped them stay informed about electoral outcomes, changes in voting schedules, and official security directives. For residents without access to traditional media, WhatsApp acted as a primary source of official communication, with peer-to-peer sharing of screenshots and videos shaping perceptions of reality. While this democratized access to information and empowered marginalized groups, it also increased vulnerability to misinformation through manipulated media. The importance of digital literacy initiatives is highlighted to combat misinformation and maintain national stability. Additionally, Facebook and Twitter served as amplifiers for security and peacebuilding campaigns, allowing NGOs and civil society organizations to reach youth in areas typically inaccessible to traditional outreach.

Community Policing and Reporting

Residents increasingly leveraged digital platforms, especially WhatsApp, to support community policing, with over 46% of respondents sharing or receiving crime-related alerts. In areas like Mathare and Korogocho, youth groups trained by peacebuilding organizations logged incidents, photographed hotspots, and coordinated with local administrators, enhancing situational awareness and potentially speeding response times. While these informal networks improve intelligence gathering and community safety, they also carry risks such as misinformation, vigilantism, and the emergence of parallel authorities that may challenge official law enforcement. Communities even used improvised incident mapping to identify flashpoints, enabling preemptive action by peace monitors or elders. Social media's immediacy allows youth to act as both witnesses and informants, sometimes outpacing traditional media in speed and reach.

Spread of Hate Speech

Hate speech on digital platforms was identified as a major security risk during elections, with 63% of respondents observing tribal, ethnic, or political slurs online. Partisan WhatsApp groups and Facebook pages often circulated unverified claims, such as accusations of vote rigging, which fueled suspicion and mistrust among neighbours in communities with historical ethnic and political tensions, like Kibera. The viral and anonymous nature of social media exacerbates these divisions, undermining social cohesion a fundamental pillar of national security. Combating such threats requires monitoring and moderating harmful content, promoting digital literacy, and fostering community dialogues and peacebuilding activities to restore trust and resilience. Research indicates that social media can be used deliberately to polarize communities, dehumanize opponents, and inflame social conflict, with informal platforms like WhatsApp presenting particular challenges for regulation.

Fake News and Disinformation

Fake news emerged as a major digital security threat, with over 52% of respondents having seen or shared election-related misinformation, such as manipulated videos, false results, or fabricated statements by candidates. In Eastleigh, a viral video of burning ballots, later proven to be filmed abroad, caused widespread panic, illustrating how rapidly unverified content can undermine trust in electoral processes and government institutions. Such misinformation highlights vulnerabilities in national security, especially in densely populated and socially dynamic areas prone to tension. Addressing this requires authoritative fact-checking, improved digital literacy, platform accountability, and rapid content moderation to reduce the window in which false information can spread and destabilize communities. Youth, in particular, are highly susceptible to sharing misinformation due to limited verification skills.

Fear, Panic, and Heightened Tensions

Digital mobilization had significant psychological effects, as unverified warnings of violence on platforms like WhatsApp generated widespread fear, sometimes causing entire neighborhoods or markets to shut down. Such rapid responses illustrate the vulnerability of informal settlements to misinformation, with direct economic consequences and disruptions to social stability. The reliance on informal networks, due to perceived inadequacies in formal security, heightens susceptibility to panic, rumors, and potential exploitation by criminal or political actors. This underscores the importance of strengthening community policing, digital literacy, and trust between residents and formal security forces to mitigate fear, economic disruption, and inter-community tensions. Research shows that rumours, especially in politically tense environments, can trigger immediate behavioral responses, further destabilizing local communities and social cohesion.

Table 1.3: Frequency of Security Incidents Linked to Online Mobilization by Settlement

Settlement	High Frequency	Moderate Frequency	Low Frequency
Kibera	43%	38%	19%
Mathare	39%	41%	20%

Eastleigh	28%	46%	26%
Korogocho	22%	34%	44%

Source Field data

Analysis of Table 1.3 reveals a hierarchy of national security risks across urban settlements. Kibera and Mathare are the most vulnerable, with the highest percentages of high-frequency online mobilization-related incidents (43% and 39%), indicating a greater likelihood of frequent and severe security threats. Eastleigh and Mathare also show high percentages of moderate-frequency incidents, highlighting persistent local security challenges. Korogocho has a comparatively lower high-frequency risk (22%) but still reflects overall vulnerability. These findings underscore the need for a tailored, risk-based national security approach, including targeted monitoring of hotspots, enhanced digital literacy, and measures to counter online misinformation, ensuring communities are resilient to digital incitement and potential unrest.

Relationship between Digital Space Mobilization and National Security

The overall objective aimed at establishing the nexus between digital space mobilization and national security in Nairobi's informal settlements. This subsection presents the model summary, ANOVA and regression output where other factors are kept constant.

Table 1.4 : Model Summary (Digital space mobilization)

Model	R	R ²	Adjusted R ²	S.E of the Estimate	F Change	df1	df2	Sig. F Change
1	.629 ^a	.396	.394	.39082	151.039	1	273	.000

a. Predictors: (Constant), Digital Space mobilization

Source: Research Findings (2025)

The results in Table 1.4 indicate a correlation coefficient $R=0.629$ and $R^2=0.394$, meaning that 39.4% of the variation in national security can be explained by changes in digital space mobilization strategies. The p-value (<0.05) shows that this impact is statistically significant. This aligns with Hunter (2022), whose cross-national study of 158 states found that social media disinformation, online political polarization, and coordination of offline violence through digital platforms undermine democratic stability.

Table 1.5 : ANOVA (Digital space mobilization)

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	23.428	1	23.428	151.039	.000 ^b
1 Residual	40.450	273	.161		
Total	63.878	274			

a. Dependent Variable: National Security

b. Predictors: (Constant), Digital space mobilization

Source: Research Findings (2025)

Table 1.5 shows that the F-statistic was significant ($p < 0.05$), indicating that the model effectively explains the relationship between digital space mobilization and national security. ANOVA results suggest statistically significant differences in the impact of various digital mobilization activities such as propaganda, social coverage, tribal/ethnic mobilization, and media coverage on national security. This aligns with Ogenga (2024), who notes that social media during elections in Africa simultaneously facilitates democratic participation and poses critical threats to stability. The findings confirm that different aspects of digital space mobilization have

varied and significant effects on national security.’

Table 1.6 : Regression Output (Digital space mobilization)

Model		Unstandardized Coefficients		Standardized Coefficients		t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta				Lower Bound	Upper Bound
1	(Constant)	1.651		.156		10.664	.000	1.348	1.958
	Digital space mobilization	-.506		.041	.609	-12.301	.000	.426	.589
a. Dependent Variable: National Security									

Source: Research Findings (2024)

Table 1.6 shows the model $Y = 1.651 - 0.506X_4 + e$, indicating that digital space mobilization has a negative and significant effect on national security ($r = -0.506$, $p < 0.05$). This means that increased digital mobilization during elections is associated with a notable decline in national security. These findings align with Feldstein (2021), who observed that both authoritarian regimes and their opponents use digital tools to monitor citizens and manipulate political narratives, thereby threatening national security.

Table 1.7: Model Summary (Digital space mobilization)

Model	R	R ²	Adjusted R ²	S.E of the Estimate	F Change	df1	df2	Sig. F Change
1	.629 ^a	.396	.394	.39082	151.039	1	273	.000
a. Predictors: (Constant), Digital Space mobilization								

Source: Research Findings (2025)

The results in Table 1.7 show $R = 0.629$ and $R^2 = 0.394$, indicating that 39.4% of the variation in national security can be explained by digital space mobilization strategies. The p-value (< 0.05) confirms that this impact is statistically significant. This aligns with Hunter (2022), whose cross-national study of 158 states found that social media disinformation, political polarization, and coordination of offline violence through digital platforms undermine democratic stability.

Table 1.8 ANOVA (Digital space mobilization)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	23.428	1	23.428	151.039	.000 ^b
	Residual	40.450	273	.161		
	Total	63.878	274			
a. Dependent Variable: National Security						
b. Predictors: (Constant), Digital space mobilization						

Source: Research Findings (2024)

Table 1.8 shows a significant F-statistic ($p < 0.05$), indicating that the model effectively explains the relationship between digital space mobilization and national security. ANOVA results reveal statistically significant differences in the impact of various digital mobilization activities including propaganda, social coverage, tribal/ethnic mobilization, and media coverage on national security. This aligns with Ogenga (2024),

who notes that social media in African elections both facilitates democratic participation and poses critical threats to stability. The findings confirm that different forms of digital mobilization exert varying and significant effects on national security.

Table 1.9: Regression Output (Digital space mobilization)

Model	Unstandardized Coefficients		Standardized Coefficients		t	Sig.	95.0% Confidence Interval for B	
	B	Std. Error	Beta				Lower Bound	Upper Bound
1	(Constant)	1.651	.156		10.664	.000	1.348	1.958
	Digital space mobilization	-.506	.041	.609	-12.301	.000	.426	.589

a. Dependent Variable: National Security

Source: Research Findings (2025)

From the findings in Table 1.9, the model thus becomes

$$Y=1.651- 0.506X_4 + e$$

Table 1.9 shows that digital space mobilization has a negative and significant effect on national security ($r = -0.506$, $p < 0.05$), indicating that increased digital mobilization during elections corresponds to a notable decline in national security. This aligns with Feldstein (2021), who observed that modern regimes and their opponents use digital tools to monitor citizens and manipulate political narratives, thereby threatening national security.

CONCLUSION

This study noted that digital technologies have transformed electoral politics, especially in areas with limited traditional media. Platforms like WhatsApp, Facebook, and Twitter are central to political mobilization, information sharing, and community engagement. While they facilitate rapid communication, early warning systems, community policing, and peace campaigns, they also enable the spread of misinformation, hate speech, and politically charged rumours. This dual role means digital platforms can both support electoral stability and threaten national security by fueling polarization and real-world violence. Digital platforms are indispensable for political engagement and community safety, but their misuse poses serious national security risks. Effective strategies are needed to curb misinformation and tension without restricting freedom of expression, striking a balance between digital participation and societal stability.

RECOMMENDATION

Collaborative Digital Security Framework and Media Literacy

The digital domain has become a two-faced instrument: an effective vehicle of peace and prejudice at the same time. To mitigate that, it can be recommended to utilize a Collaborative Digital Security Framework that not only defines the power of digital platforms but also actively minimizes their risks. This framework would have a multi-stakeholder approach, which entails government, technology companies, and civil society.

A Digital Peace Corps ought to be set up. This would ideally be a youth-based, oppressed-led volunteer force, trained in digital forensics and media literacy. They would constantly check digital spaces in real time and remove hate speech, misinformation, and encourage violence. They would not become a censorship entity; rather, they would be working on counter-messaging and fact-checks. The corps would collaborate and coordinate with tech firms such as Meta (Facebook/WhatsApp) and X (formerly Twitter) to debunk false information with trusted facts and push the counteracting narratives of peace and unity as quickly as possible.

The government and civil society should then initiate an expansive digital literacy program. This campaign, whose tagline is "Think Before You Share", would be run in the informal settlements in the form of community forums and digital workshops. It would aim to train citizens to think critically about the material on the internet, to learn how to recognize fake news and to learn about the implications of the distribution of information that has not been verified. This campaign would allow people to take charge of their digital security status, moving them away from being consumers of information and becoming critical thinkers and responsible digital citizens.

REFERENCES

1. Aideloje, S., Sylvester, A., & Jacintha, M. (2024). Social media and youth mobilization in Nigeria's 2023 elections: Implications for conflict and peacebuilding. *Journal of African Elections*, 23(2), 45–62.
2. ARTICLE 19 Eastern Africa. (2022). *Digital rights and grassroots activism in Kenya*. Nairobi: ARTICLE 19.
3. Camp, R. A. (2017). *Politics in Mexico: The democratic consolidation*. Oxford University Press.
4. Daka, J., Oando, P., & Majiwa, R. (2024). Electoral technologies and national security in Kenya: Risks and vulnerabilities. *African Journal of Democracy and Governance*, 12(1), 88–105.
5. Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.
6. Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*, 22(8). <https://doi.org/10.5210/fm.v22i8.8005>
7. Gazdar, H. (2007). Karachi's informal settlements and political militias. *Economic and Political Weekly*, 42(2), 94–101.
8. Gyimah-Boadi, E. (2009). African elections and democratization: Challenges for security and stability. *Journal of Democracy*, 20(3), 125–139.
9. Harris, K., Kamindo, P., & van der Windt, P. (2022). SMS campaigns and voter registration: Evidence from Kenya. *Electoral Studies*, 79, 102542. <https://doi.org/10.1016/j.electstud.2022.102542>
10. Haysom, S. (2013). Security and development in fragile states. *International Journal of Security and Development*, 2(3), 1–22.
11. Hunter, R. (2022). Social media, disinformation, and democratic stability: A cross-national analysis. *Journal of International Security Studies*, 45(4), 611–635.
12. IDS. (2021). *Digital media and political communication in Kenya's informal settlements*. Nairobi: Institute of Development Studies.
13. Kanyinga, K., & Long, J. D. (2009). The political economy of elections and violence in Kenya. *Journal of Eastern African Studies*, 3(2), 229–254.
14. Lindberg, S. I. (2006). *Democracy and elections in Africa*. Johns Hopkins University Press.
15. Mare, T., Mainye, J., & Manga, S. (2024). Digital actors and electoral debates in Kenya: Influencers, consultants, and bots. *African Media Studies*, 16(1), 55–72.
16. Mendoza, R. U. (2012). Political dynasties and poverty: Measurement and evidence of linkages in the Philippines. *Asian Journal of Political Science*, 20(3), 256–284.
17. Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. Acts Press.
18. Mutahi, P. (2018). *Political violence and insecurity in Nairobi's informal settlements*. Nairobi: Center for Human Rights and Policy Studies.
19. Mwagiru, M. (2012). *Conflict in Africa: Theory, processes and institutions of management*. Nairobi: CCR.
20. Ngange, A., & Elongé, C. (2019). Digital mobilization and electoral politics in Cameroon. *African Journal of Communication*, 5(1), 77–95.
21. Ogenga, F. (2024). Digital media and elections in Africa: Opportunities and threats. *Journal of African Media Studies*, 16(2), 201–218.
22. Omolo, A. (2010). Civil society and electoral violence in Kenya. *Democracy Review*, 18(1), 127–146.

23. Oluleye, A. (2023). Political lies and disinformation in African elections. *Journal of Democracy in Africa*, 4(2), 90–107.
24. Shao, C. (2017). The spread of low-credibility content by social bots. *Nature Communications*, 8, 1–9. <https://doi.org/10.1038/s41467-017-02093-5>
25. Sharma, A. (2013). Clientelist politics in Indian slums: Elections, services, and identity. *Asian Survey*, 53(6), 1114–1136.
26. Stella, M., Ferrara, E., & De Domenico, M. (2018). Bots increase exposure to negative and inflammatory content in online social systems. *Proceedings of the National Academy of Sciences*, 115(49), 12435–12440. <https://doi.org/10.1073/pnas.1803470115>
27. Verdeja, E., & Hook, S. (2022). Social media, polarization, and threats to national security. *Journal of Peace Research*, 59(4), 567–582.
28. Wacquant, L. (2008). *Urban outcasts: A comparative sociology of advanced marginality*. Polity Press.
29. Wambua, D. (2020). Digital propaganda and electoral insecurity in Kenya. *African Security Review*, 29(4), 349–364.
30. Wefwafwa, P., Wekesa, B., & Gagliardone, I. (2025). WhatsApp and electoral mobilization in Kenya: Privacy versus security dilemmas. *Information, Communication & Society*, 28(3), 455–472.
31. Wilkinson, S. I. (2004). *Votes and violence: Electoral competition and ethnic riots in India*. Cambridge University Press.