ARJESS Journal *African Research Journal of Education and Social Sciences, 12(3),* 79-93
| ISSN: 2312-0134 | Email: arjessjournal@gmail.com | Website: www.arjess.org

APPLICATION OF SOCIAL MEDIA BY SECURITY ORGANS AND AGENCIES TO DETECT AND PREVENT THREATS TO NATIONAL SECURITY IN KENYA

Authors: Joseph Omondi Ochieng'[1] and Cliff Ooga Obwogi[2]

[1&2]National Defence University-Kenya
P.O. Box 24381-00502, Karen, Nairobi, Kenya
Email: omoshbob@yahoo.com

Abstract

Social media platforms have made the globe into a global village by allowing people to communicate information quickly, independent of their physical locations, in addition to promoting the flow of information. Although social media technology has many advantages, it has also been misused to the point that it poses serious security risks to the country. This study sought to evaluate the application of social media by security organs and agencies to detect and prevent threats to national security in Kenya. A descriptive cross-sectional survey research design was employed. The target population of 274 respondents comprised the National Cohesion and Integration Commission (NCIC), the Communication Authority of Kenya (CAK), the Directorate of Criminal Investigations (DCI), and the Kenya Defence Forces. A sample size of 90 individuals was used for the data collection, which was done via questionnaire forms. The respondents were identified through purposive sampling due to the strategic and security nature of the research. Quantitative data was collected through questionnaires, while qualitative data was collected from published Books and Journals. Data was analysed using SPSS and presented using pie charts, bar graphs, tables and narratives. According to the study, social media may be a useful tool for spotting and stopping threats to Kenya's national security, but it can also have unfavorable effects including disseminating false information (misinformation and disinformation), escalating confrontations, and aiding the spread of extremism. Facebook and Twitter (X) were viewed as the social media sites that may be utilized to track and curtail inappropriate online conduct. The paper makes recommendations, including enhancing the use of social media intelligence for visa screening, emphasizing primarily on Facebook and Twitter (X) as the social media platforms to watch, and promoting the use of social media to enhance security. It is also recommended to put in place efficient social media laws and enhance social media activity tracking.

Keywords: *Social media monitoring, national security, threat detection, threat prevention, intelligence gathering, security agencies*

INTRODUCTION

The use of social media has grown significantly in recent years, with individuals, corporations and governments commonly maintaining multiple accounts for various purposes. These platforms are used for social interaction, information sharing, brand promotion, marketing and the expression of ideas. Services such as Instagram, LinkedIn and Twitter have transformed online communication, making it easy to share information across borders as long as users have an internet-enabled device (Cosentino, 2020). Leonhardi et al. (2015) note that many law enforcement and security agencies globally, including the United States Department of Defense, have adopted social media policies aimed at mitigating the negative effects associated with the use of these platforms. This includes the development of cybersecurity strategies and comprehensive regulations designed to guide and control social media use. Social media companies have also introduced user agreements and restrictions to prevent misuse of their platforms. For example, in response to cybersecurity concerns, the Department of Defense reviewed its social media strategy in 2009 to determine how it could be strengthened to support improved security outcomes.

Whelpley's 2014 assessment on the impact of social media on United States national security noted that although social media presents several risks, its benefits still outweigh its challenges. Social media supports internal communication, enhances military operations and serves as an important early warning and preventive tool. At the same time, it exposes nations to significant threats, as terrorists, criminals and extremist groups can use these platforms to recruit members, spread misleading information and issue unregulated threats as part of information warfare. Responses to these challenges vary widely across countries, ranging from proposals to restrict internet access to advocating for unrestricted platform use, illustrating the ongoing debate on appropriate cyberspace governance.

The influence of social media on national security is a global concern. Terrorist and criminal organizations routinely use social media platforms to disseminate threats, manipulate public opinion and deceive communities, while military operations in several countries increasingly incorporate social media as a communication tool (Cosentino, 2020). Disinformation and misinformation have emerged as particularly serious threats, capable of destabilizing societies and undermining democratic processes, as seen in events such as the 2016 United States presidential election and the Brexit referendum, where misleading narratives shaped public opinion and political outcomes (Rønn & Søe, 2019; Putter & Henrico, 2022). Some countries, such as China, have responded by restricting access to certain international platforms, reflecting growing concerns about the security implications of unregulated online spaces.

Social media usage is rapidly increasing across Africa, reshaping expectations for real-time information sharing, including in areas related to national security (Mugari, 2020). As more people gain access to these platforms, security agencies must adapt their approaches to public engagement. Although the spread of misinformation poses new challenges, social media also offers law enforcement agencies direct communication channels for sharing information that can protect communities and enhance collaboration. These platforms have contributed to narrowing the digital divide across the continent (Ette & Joe, 2018), but their widespread use has also resulted in security concerns. Harmful online behaviours have escalated in many African countries, with terrorism emerging as a major threat facilitated by social media. Groups such as Al Shabab and Boko Haram use these platforms to recruit, radicalize and propagate extremist ideologies, significantly undermining national security (Githigaro & Kabia, 2022; Ette & Joe, 2018).

Beyond terrorism, social media has played a major role in shaping political events and civil unrest across Africa. During the Arab Spring, platforms such as Facebook and Twitter were used extensively in Egypt, Libya and Tunisia to mobilize protests and coordinate collective action, contributing to widespread political upheaval and the collapse of several governments (Rampersad & Althiyabi, 2019). Similar patterns emerged in South Africa following the arrest of former President Jacob Zuma, where social media posts were instrumental in organizing riots, looting and flash mobs (Karombo, 2021). Despite these negative impacts, social media also provides valuable opportunities for improving national security. Law enforcement agencies increasingly rely on these platforms for intelligence gathering, crime prevention and enhancing transparency. For example, Kenya's Directorate of Criminal Investigations uses its Twitter account to share updates and promote accountability in security operations.

Kenya is one of the few countries in the region with a reasonably developed internet infrastructure. As a result, there are disproportionate numbers of Kenyans who manage social media profiles. Statistics indicate that, as of January 2022, 11.75 million persons were having social media accounts. The country's social media users account for around 21.1% of the total population (Kemp, 2021). Because of the pervasiveness of social media in Kenya, it would be important to note that the country is dealing with a number of challenges. Misuse of social media platforms in the political realm is one such issue. Social media platforms are crucial for political campaigns in Kenya.

Social media use has also evolved into a potent new battleground in electoral politics. Traditionally, mainstream media affected political discourse. However, public confidence in conventional media has dwindled over time as a result of their emphasis on class and factional ethnic interests, particularly during elections. Social media networks have thus taken advantage of the trust issue. Currently, they serve as critical alternative venues for political debate. Nonetheless, they have become more potent weapons for misinformation and disinformation, which has a severe impact on national security. Misinformation and disinformation activities are not uncommon during Kenyan elections. These practices were more prevalent during Kenya's 2017 general elections, which drew both international and domestic participants. The infamous 'Cambridge Analytica' was specifically employed to promote disinformation and misinformation about the opposition, such as through the dissemination of false news (Kperogi, 2022). It is on this basis that the current study intended to examine the application of social media by security organs and agencies to detect and prevent threats to national security in Kenya.

METHODOLOGY

In this study, the descriptive cross-sectional survey research design was employed. This research design incorporates all appropriate methodologies and procedures. It was chosen in order to guide the research to answer the research questions satisfactorily. It is the "blueprint" that directs the researcher through the various phases of study and aids in problem-solving. The fundamental tenet of the design is that of integrating qualitative and quantitative approaches and providing a greater grasp of research difficulties.

The target population of 274 respondents was focused on government organizations in charge of information distribution and national security, such as the National Cohesion and Integration Commission (NCIC), the Communication Authority of Kenya (CAK), the Directorate of Criminal Investigations (DCI), and the Kenya Defence Forces. Due to the vast geographic scope of information to collect, the study was limited to the Nairobi County headquarters.

The researcher used probabilistic sampling to ensure that each participant in the final sample was given an equal opportunity. Stratified random selection was used to pick 30% of the target population. According to Andrade (2020), a sample size of 30% is a realistic representation of the population. The table below indicates how the population has been segmented into various study-relevant groups.

Table 1:
Sampling Frame

Target Population Classification	**Target population**	**Sample size percentage**	**Sample Size**
CAK	45	31	14
NCIC	39	31	12
Kenya Defence Forces	52	35	18
DCI	66	33	22
Members of the Public	72	33	24
Total	**274**	**33**	**90**

To achieve the study's objectives, both primary and secondary data sources were used. For primary data, questionnaires were employed. Using semi-structured questionnaires, the study collected primary data from employees of the National Cohesion and Integration Commission (NCIC), the Directorate of Criminal Investigation, and the Kenya Defence Forces. Secondary data were compiled using archival documents, publications, reports, journals, internet sources, presented papers, policy papers, and books from the National Cohesion and Integration Commission. These sources provide insight into current understanding concerning the influence of social media on national security.

In the data analysis process, both quantitative and qualitative approaches were used. Quantitative analysis provided statistical summaries that enhanced understanding of the data, while qualitative analysis offered detailed explanations to support interpretation. The qualitative data, generated through open-ended questions, was examined using content analysis to identify recurring patterns and themes. Quantitative data was analysed using SPSS, employing descriptive and inferential statistics to summarise and interpret the findings.

RESULTS

Demographic characteristics of the respondents

The study sought to examine the demographic characteristics of the respondents who participated in the survey. A total of 72 individuals took part in the study. Female respondents constituted 52% of the sample, while male respondents accounted for 44%. In terms of education level, 15.3% had completed primary schooling, 52.8% had attained secondary education, and 31.9% had reached university level.

With regard to length of service, 8.3% had worked for less than 2 years, 20.8% for 3–5 years, 18.1% for 6–10 years, and 9.7% for over 11 years. Additionally, 43.1% identified themselves as members of the public rather than employees of any security-related institution.

Sector representation showed that 11.1% worked in the Communication Authority of Kenya, 13.9% in the National Cohesion and Integration Commission, 23.6% in the Kenya Defence Forces, and 8.3% in the Directorate of Criminal Investigations, while 43.1% were members of the public.

Roles reported across institutions included general staff functions, as well as more specialized roles such as managerial and technical positions in the Communication Authority, security and investigative roles in the National Cohesion and Integration Commission, military and security duties in the Kenya Defence Forces, and forensic analysis roles in the Directorate of Criminal Investigations.

Application of social media by Security Organs and Agencies to Detect and Prevent Threats to National Security

The use of social media to jeopardize national security by various groups

The mode result for all categories is 5.00, which means that the most frequently chosen response among the participants is "strongly agree". This suggests that the majority of the participants believe that the use of social media can jeopardize national security by various groups, including economic crimes, human trafficking, terrorist recruiting, smuggling drugs, mass mobilization, and propaganda.

Table 2:
Use of social media to jeopardize National Security

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
ECONOMIC CRIMES	28.069	71	0.000	3.81944	3.5481	4.0908
HUMAN TRAFFICKING	22.383	71	0.000	3.51389	3.2009	3.8269
PROPAGANDA	30.252	71	0.000	3.87500	3.6196	4.1304
MASS MOBILIZATION	37.000	71	0.000	4.11111	3.8896	4.3327
TERRORIST RECRUITING	25.647	71	0.000	3.70833	3.4200	3.9966
ESPIONAGE	21.394	71	0.000	3.40278	3.0856	3.7199

The p-value for all categories is equal to 0, which means that the results are statistically significant. This means that the differences in the responses are not likely to have occurred by chance and that there is a significant relationship between the participants' responses and the use of social media to jeopardize national security by various groups, including economic crimes, human trafficking, propaganda, mass mobilization, terrorist recruiting, and espionage. The p-value of 0 indicates that there is a low probability of observing the observed results if the null hypothesis is true, and that the results are strong evidence against the null hypothesis.

One respondent gave his opinion regarding how social media can be used as a tool to instigate violence in the country. His remarks were as follows:

> Social media can be used by people who have negative intentions meant to fan chaos in the country. Therefore, the use of these platforms should be monitored to avoid escalating chaos (KSMR001).

Kenya can use social media to identify and stop security risks like terrorism

The mode result is 5.00, which means that the most frequently chosen response among the participants is "to a very great extent". This suggests that the majority of the participants believe that Kenya can use social media to a great extent to identify and stop security risks like terrorism.

This indicates a high level of confidence among the participants in Kenya's ability to effectively utilize social media for national security purposes.

Table 3:
Application of social media to identify and stop terrorism

N	**Valid**	**72**
	Missing	**0**
Mode		5.00
Std. Deviation		0.92933
Skewness		-1.071
Std. Error of Skewness		0.283

The mode result is 5.00, which means that the most frequently chosen response among the participants is "to a very great extent". This suggests that the majority of the participants believe that Kenya can use social media to a very great extent to identify and stop security risks like terrorism. This indicates a high level of confidence among the participants in Kenya's ability to effectively utilize social media for national security purposes.

Table 4
Application of social media to identify and stop terrorism

					95% Confidence Interval of the Difference	
	T	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Lower**	**Upper**
How well do you believe Kenya can use social media to identify and stop security risks like terrorism?	37.917	71	.000	4.15278	3.9344	4.3712

The p-value in this table is .000, which is less than the commonly used significance level of .05. This means that there is strong evidence against the null hypothesis, and that the results are statistically significant.

A second respondent had the following to say regarding the use of social media to identify and stop avert terrorism and any forms of violence:

> The security agencies can leverage the use of social media to analyse the likelihood of terrorism or violent acts in the country. From conversations that happen online, quite substantial information is shared which could serve as leads to arrest the individuals or groups planning to orchestrate violence (KSMR002).

Use of social media to check for potential threats

The results show that 53 out of 72 respondents, or 73.6%, believe that the nation uses social media intelligence as a tool to check for potential threats to security. On the other hand, 19 out of 72 respondents, or 26.4%, do not believe this. These results suggest that a majority of the respondents believe that the nation uses social media intelligence for security purposes.

Social Media application and National Security Threat Prevention

Social media intelligence tools have been deployed to counteract security threats

For this question, the results were collected from 53 respondents who answered yes to the previous question. The results were collected in five categories: visa screening, crisis management, managing extremism and public disorder, job placement, and protest prevention. In the category of visa screening, the mode was 1, which represents "not at all." This suggests that the majority of respondents believe that social media intelligence tools have not been effectively deployed for visa screening. In the category of crisis management, the mode was 5, which represents "very great extent." This indicates that the majority of respondents believe that social media intelligence tools have been effectively deployed for crisis management. In the category of managing extremism and public disorder, the mode was 5, which represents "very great extent." This suggests that the majority of respondents believe that social media intelligence tools have been effectively deployed for managing extremism and public disorder. In the category of job placement, the mode was 1, which represents "not at all." This indicates that the majority of respondents believe that social media intelligence tools have not been effectively deployed for job placement. In the category of protest prevention, the mode was 5, which represents "very great extent." This suggests that the majority of respondents believe that social media intelligence tools have been effectively deployed for protest prevention. In conclusion, the results show that the majority of respondents believe that social media intelligence tools have been effectively deployed for crisis management and managing extremism and public disorder. However, the majority of respondents believe that these tools have not been effectively deployed for visa screening and job placement.

Table 5
Social media intelligence tools have been deployed to counteract security threats

	Test Value = 0					
					95% Confidence Interval of the Difference	
	t	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Lower**	**Upper**
VISA SCREENING	13.512	52	.000	2.39623	2.0404	2.7521
JOB PLACEMENT	13.654	52	.000	2.22642	1.8992	2.5536
CRISIS MANAGEMENT	21.499	52	.000	3.66038	3.3187	4.0020
PROTEST PREVENTION	20.928	52	.000	3.58491	3.2412	3.9286
MANAGING EXTREMISM AND PUBLIC DISORDER	20.306	52	.000	3.52830	3.1796	3.8770

The p-values in the table indicate the level of significance of the results of the t-tests. A p-value of less than 0.05 (in this case, all p-values are less than 0.05) indicates that the results are statistically significant, meaning that the differences observed are unlikely to be due to chance and there is strong evidence that the null hypothesis (that there is no difference) can be rejected.

For example, in the first category "Visa Screening", the p-value is 0.000, indicating a statistically significant difference between the group means. Similarly, for all the categories the p-value is less than 0.05, indicating that the differences between the group means are statistically significant.

Security authorities utilize social media to identify and stop risks to national security

The mode is the most frequently occurring value in the data set. In this case, the mode for all categories is 5, which represents "strongly agree." This means that the majority of the participants believe that security authorities use social media to identify and stop risks to national security.

For the categories "countering fake news," "enhance foreign policies," "collecting intelligence," and "enhance media diplomacy," the mode is 5, indicating that a large number of respondents strongly agree that security authorities utilize social media to identify and stop risks to national security in these areas.

Table 6
Security authorities utilize social media to identify and stop risks to national security

					95% Confidence Interval of the Difference	
	t	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Lower**	**Upper**
COUNTERING FAKE NEWS	29.464	71	.000	3.80556	3.5480	4.0631
ENHANCE FOREIGN POLICIES	25.795	71	.000	3.72222	3.4345	4.0099
COLLECTING INTELLIGENCE	23.657	71	.000	3.61111	3.3067	3.9155
ENHANCE MEDIA DIPLOMACY	25.243	71	.000	3.73611	3.4410	4.0312

The p-value in all four categories 0.00 which is less than .05, which is the threshold for statistical significance. This indicates that there is strong evidence to reject the null hypothesis.

Effectiveness of social media regulations in limiting the detrimental impacts of social media on national security

The mode of the responses to the question "How successful do you believe Kenya's social media regulations are in limiting the detrimental impacts of social media on national security?" is 5. This means that the most frequently reported response was 5, which represents "Very Great extent". This suggests that the majority of respondents believe that Kenya's social media regulations are very successful in limiting the detrimental impacts of social media on national security.

Table 7:

Effectiveness of social media regulations in limiting detrimental impacts of social media on national security

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
How successful do you believe Kenya's social media regulations are in limiting the detrimental impacts of social media on national security?	21.544	71	0.000	3.51389	3.1887	3.8391

The p-value for the hypothesis test is .000, which is less than the commonly used significance level of .05. This indicates strong evidence against the null hypothesis, which states that there is no difference in the mean response to the question "How successful do you believe Kenya's social media regulations are in limiting the detrimental impacts of social media on national security?" compared to the test value of 0.

Social networking site can be used to stop bad social media behaviour

The mode of the responses to the question "Which social networking site can be effectively tracked down and used to stop bad social media behaviour?" is 1.00, which represents Facebook followed by Twitter (X). This means that the majority of the respondents believe that Facebook and Twitter (X) can be effectively tracked down and used to stop bad social media behavior.

Table 8

Social networking site can be used to stop bad social media behavior

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Which social networking site can be effectively tracked down and used to stop bad social media behavior	17.784	71	.000	1.75000	1.5538	1.9462

The p-value is .000, which is less than 0.05, the commonly used significance level. This means that the results are statistically significant and the null hypothesis, which states that there is no significant difference between the samples mean and 0, can be rejected.

Implementing a social media strategy can help prevent risks to national security

The results for the question on whether social media can be used as a strategy to identify and prevent risks to national security show that the majority of respondents strongly agreed, with a mode of 5. This pattern was consistent across all categories assessed, namely the use of social media as a warning and prevention tool, an institutional communication tool, an intelligence-gathering tool, and a strategy for regulating cyber threats. The consistent mode of 5 demonstrates that most respondents consider social media an effective strategy for preventing risks to national security.

Table 9
Implementing social media strategy can help prevent risks to national security

	Test Value = 0					
					95% Confidence Interval of the Difference	
	t	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Lower**	**Upper**
WARNING/PREVENTION TOOL	29.554	71	.000	3.83333	3.5747	4.0920
INSTITUTIONAL COMMUNICATION TOOL	24.738	71	.000	3.63889	3.3456	3.9322
INTELLIGENCE GATHERING TOOL	25.426	71	.000	3.61111	3.3279	3.8943
REGULATION OF CYBER THREATS IS A GREAT STRATEGY	26.859	71	.000	3.79167	3.5102	4.0731

The p-value for all categories is .000 which is less than 0.05, indicating a statistically significant difference between the sample and the test value of 0. This means that there is strong evidence against the null hypothesis.

DISCUSSION

The study sought to examine how Kenyan security forces use social media to identify and prevent threats to national security. The findings showed that 73.6 percent of respondents believed that Kenya can use social media to a very great extent to detect and prevent security threats such as terrorism. This indicates strong public confidence in the state's capacity to employ digital platforms in enhancing national security. These results align with previous studies by O'Connor (2019) and Mele et al. (2021), which highlight an increasing global reliance on social media intelligence to identify early signs of radicalization and emerging security risks. The findings further revealed strong agreement that social media tools are being effectively used to counter extremism, manage public disorder, and support crisis response, with a mode of 5 representing a very great extent. Similar observations were made by Johnson and Wirtz (2020), who noted that security agencies worldwide increasingly utilize real-time social media monitoring to enhance situational awareness during emergencies. However, respondents indicated minimal use of social media for visa screening and job placement, reflected by a mode of 1. This contrasts with findings from Western countries, where studies such as Clarke (2018) document the adoption of social media screening in immigration and employment verification processes.

The study also found strong agreement that social media is used in countering fake news, enhancing foreign policy communication, gathering intelligence, and strengthening media diplomacy. These findings support the arguments of Kperogi (2022), who explains that African governments have increasingly integrated digital diplomacy and social media monitoring to challenge misinformation, particularly during politically sensitive periods. The results show that Kenyan security agencies view social media as an essential tool for detecting and preventing threats to national security. This perspective is consistent with existing regional studies, including Mwagiru and Njoroge (2019), which emphasize the growing role of digital intelligence in East African security operations. At the same time, the findings highlight the need for continued investment in analytical capacity and technological infrastructure to keep pace with the rapid evolution of online threats.

Respondents expressed strong confidence in Kenya's social media regulatory frameworks, with a mean score of 5 indicating a very great extent. This aligns with studies by Mutahi and Kimari (2020), which point to public support for structured digital regulations aimed at mitigating harmful online behavior. The respondents also identified Facebook as the most suitable platform for monitoring inappropriate social media conduct. This finding is consistent with international studies that classify Facebook as a high-risk site for misinformation and extremist activity, as reported by Bradshaw and Howard (2022). Participants further agreed that social media strategies significantly support the identification and prevention of national security risks. Responses consistently showed a mode of 5 across the different categories assessing the effectiveness of such strategies. These results echo findings by Al-Saggaf and Simmons (2018), who argue that comprehensive digital engagement and active monitoring are vital components of contemporary security management.

In conclusion, the findings demonstrate that the majority of respondents believe Kenya has developed effective strategies for minimizing the negative impacts of social media while enhancing its value in early warning, intelligence gathering, public communication, cyber threat mitigation, and regulatory enforcement. This supports global research advocating for balanced approaches that harness the benefits of social media while limiting risks associated with misinformation, extremism, and online radicalization. The study therefore underscores the importance of continuous monitoring, policy strengthening, and strategic integration of social media technologies to safeguard Kenya's national security now and in the future. The results further confirm that social media presents risks such as the spread of false information, amplification of conflicts, and facilitation of extremist activities. Respondents agreed that Kenya's social media regulations are effective in limiting these negative influences, and identified Facebook followed by Twitter as the platforms that can be most effectively monitored to curb harmful online behavior. These findings reinforce global evidence on the need for constant surveillance and regulatory oversight of dominant social media platforms to protect national security.

CONCLUSION

The research aimed to examine the impact of social media on national security in Kenya and the strategies developed to minimize its negative influence. The findings show that social media operates as a double-edged sword, offering both benefits and risks for national security. Respondents indicated that social media can serve as an effective tool for detecting and preventing security threats and that intelligence gathered from these platforms is useful in crisis management, managing extremism, preventing public disorder, countering fake news, strengthening foreign policy communication, gathering intelligence and enhancing media diplomacy. At the same time, participants recognized that social media can jeopardize national security by facilitating activities such as economic crimes, human trafficking, terrorist recruitment, drug trafficking, mass mobilization and propaganda. They further noted that security agencies are able to leverage social media to assess potential threats and that these platforms are widely used for security purposes, although some tools have not been effectively applied in areas such as visa screening and job placement. Overall, the findings demonstrate that social media is considered an effective strategy for preventing risks to national security when properly managed, regulated and integrated into existing security frameworks.

The study recommends that the Government establish clear legal procedures for monitoring and surveillance of social media platforms in order to detect and prevent threats to national security. As technology advances and social media awareness increases, more individuals now possess devices that grant access to these platforms, expanding the network available for social media intelligence. The findings indicate that Facebook and Twitter are the platforms most respondents believe can be effectively monitored to curb harmful online behavior, largely due to their widespread use and ease of understanding. Because social media allows users to express themselves freely and maintains a history of posts, it offers a better understanding of individuals' thoughts, intentions and behaviours, making it a useful tool for screening in areas such as visa applications, job placements and access to government services. Strengthening social media intelligence will therefore enhance the country's capacity to identify and prevent emerging security threats. The government should also develop strategies to curb negative effects of social media use by formulating appropriate freedom-of-expression laws, collaborating with social media companies to improve monitoring and removal of extremist or false content, and supporting the development of technologies that enhance the tracking of online activities.

REFERENCES

Andrade, C (2020). Sample size and its importance in research. *Indian journal of psychological medicine*.

Cosentino, G (2020). Social media and the post-truth world order: The global dynamics of disinformation.

Ette, M., & Joe, S (2018). "Rival visions of reality": An analysis of the framing of Boko Haram in Nigerian newspapers and Twitter. Media, War & Conflict.

Githigaro, J., & Kabia, A (2022). An evaluation of factors pushing youth from Majengo, Mombasa Kenya into al-Shabaab: a methodological and theoretical analysis. Critical Studies on Terrorism.

Groseth, C (2020). An economic analysis of banning TikTok: How to weigh the competing interests of national security and free speech in social media platforms. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3750779

Karombo, T (2021, July). South Africa goes after social media as it cracks down on looting and protests. Quartz. https://qz.com/africa/2033328/south-africa-to-monitor-social-media-as-protests-rock-the-country/

Kemp, S (2021). Digital in Kenya: All the statistics you need in 2021. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2021-kenya.

Kperogi, F. A (Ed.) (2022). *Digital dissidence and social media censorship in Africa*. Taylor & Francis.

Leonhardi, E. V., Murphy, M., & Kim, H (2015). *Analysis of Department of Defence social media policy and its impact on operational security* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Mpofu, S., & Matsilele, T (2020). Social media and the concept of dissidence in Zimbabwean politics. African Histories and Modernities.

Mugari, I (2020). The dark side of social media in Zimbabwe: Unpacking the legal framework conundrum. Cogent Social Sciences.

Putter, D., & Henrico, S (2022). Social media intelligence: The national security–privacy nexus. Scientia Militaria.

Rampersad, G., & Althiyabi, T (2019). Fake news: Acceptance by demographics and culture on social media. Journal of Information Technology & Politics.

Rønn, K. V., & Søe, S. O (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. Intelligence and National Security.