05 Dynamics Hindering Efficiency of Social Media Intelligence in Countering Criminality in Kenya

Mutai Kiplagat, Juliet Kamau, and Irene Mukiri Mwingirwa

Abstract

Social media sites provide a haven for criminals. This threatens national security, hence the need for effective counter strategies. Despite the criminals' shifting to social media platforms, government security agencies remain slow in adopting emerging technologies and rely more on traditional intelligence collection methods, which fall short of capturing what occurs in the virtual world. The foregoing informed this research study on the dynamics hindering the efficiency of social media intelligence in countering criminality in Kenya. The objective was to determine the challenges that affect the efficiency of social media intelligence in countering online crimes in Kenya. The research applied technology acceptance theory to expound on the utilisation of social media platforms by criminals and subsequent challenges of counter-measures by government security agencies. The study applied a descriptive research design targeting government security agencies dealing with online countering of organised crimes and terrorism. The study established that existing challenges include criminal use of fake identities, secure applications, inadequate technical support and skills, weak legal frameworks, existing social media corporation bureaucracies, identification problems in virtual realms and technological adoption challenges. In conclusion, social media threats are cross-cutting and the emergence of many social media applications requires government security agencies to utilise all sources of information to mitigate strategic surprises. As a result, the research recommends enhancing the capabilities and capacity building of online investigation officers; investing more in research and innovation; enhancing information sharing and collaboration among key stakeholders; and formulating stringent measures.

Keywords: Social media intelligence, traditional collection methods, criminality, organised crimes, terrorism, government security agencies, social media platforms, bureaucracies, and virtual realms.

Introduction

Advancements in technological systems have accelerated globalisation through the use of the Internet, which has become more accessible and affordable in communication and information (Dahlman, 2007). However, the emergence of technology leaves organisations without the option of investing more in adopting new information and communication systems to harness opportunities and mitigate threats (Montasari, 2022). The efficiency and effectiveness brought about by adopting new technologies are unmatched in enhancing faster service delivery and organisational productivity. The evolving nature of technologies has also led to the development of social media applications that utilise the Internet for interconnectivity, which offers a platform for criminals to advance their activities.

The emergence of social media platforms (SMPs) has led to changing dynamics of terrorist organisations like Al-Shabaab and the Islamic State. Terrorists primarily utilise social media as a tool for spreading propaganda to discredit the government and gain publicity (Hossain, 2018). For instance, Al-Shabaab uses social media propaganda to target vulnerable individuals for recruitment, coordinate their activities, and reach out to sympathisers for funds (Cox et al., 2018). In addition, Al-Shabaab terror group has optimised SMPs to showcase its fighters during training and graduation to demonstrate its capabilities to attract foreign recruits.

Terrorists have used SMPs while executing attacks. For example, in January 2020, during the Manda attack in Lamu, Al-Shabaab operatives forwarded the images and videos of the destroyed United States (U.S.) aircraft via social media for an Al-Kataib press release (Pantucci, 2020). Social media therefore remains a powerful instrument with seemingly limited restrictions for terrorists to actualise their agenda within the virtual community. Similarly, the evolving nature of social media requires security agencies to monitor criminals' activities closely, examine their modus operandi, and assess potential threats. Social media threat assessment and close monitoring aim to prevent the states from being caught off guard in the event of possible hostile use (Kimutai, 2014).

Criminal optimisation of diverse SMPs poses a significant danger and challenge to national security. The threat landscape within the virtual realms makes the existing counter strategies fall short of obtaining the real threats proactively, thereby leaving security teams in a firefighting posture. SMPs such as Facebook, Telegram, WhatsApp, X, Dark-web, YouTube, Conversation, Instagram, WeChat, Signal, TikTok, and Snapchat are increasingly being utilised by individuals engaged in illicit activities (Almadhoor et al., 2021). The multiplicity of SMPs offers more alternatives and choices for criminals to evade security

trailing. This shows that criminals do not have a specific chosen platform, but their utilisation largely depends on the kind of activity they are engaged in. Similarly, security agencies rely more on traditional collection methods such as Human Intelligence (HUMINT), Open Source Intelligence (OSINT), Technical Intelligence (TECHINT), Signal Intelligence (SIGINT), Imagery and Photographic Intelligence (IMINT), Geospatial Intelligence (GEOINT), and Measurement and Signature Intelligence (MASINT) to counter criminal activities (Johnson, 2010; Maltego, 2022).

On their part, criminals have shifted most of their activities to both open and private SMPs to reach out to wide support networks, optimise secure communications, enjoy a higher degree of anonymity, and evade security trailing. Some of the illicit online activities include cybercrimes, sourcing weapons, optimising secure communication with support networks, carrying out online radicalisation and recruitment, sharing security training manuals, and acquiring tactics to evade security agencies (Bartlett & Reynolds, 2015; Claudia, 2021). In addition, SMPs offer criminals convenience and global diversity to achieve their intentions while limiting security tracking.

Moreover, the COVID-19 pandemic measures, including encouraging people to work from their homes, saw a shift to more online activities leading to an increase in virtual crimes (Montasari, 2022). During this period, criminals optimised the unpreparedness of people to handle online threats due to the rush to adopt remote working and online transactions. Further, criminals disguised as health experts exploited people's desperation through phishing and other social engineering techniques for selfish gain (Saleous et al., 2023). Furthermore, the increased online transactions allowed criminals to obtain personal information on social media and use it to lure unsuspecting citizens through scam mail, text, and links to hack their financial accounts or credit cards. The online platform, therefore, is becoming a haven for criminals and thus requires close monitoring of their activities in order to mitigate threats (Thukral & Kainya, 2022).

The existing studies in Kenya have focused on using social media as an open-source intelligence tool (Kimutai, 2014; Olasya, 2018). The studies covered use of open or public SMPs by government security agencies such as the military, Directorate of Criminal Investigations, and police to obtain criminal information from the public. The studies show the inherent reactive nature of security agencies in dealing with social media crimes. The current study was thus aimed at filling the existing gaps in challenges hindering the efficiency of social media intelligence in countering criminality in Kenya.

Statement of the problem

Criminals have shifted their activities to SMPs, however, security agencies have been unable to adequately equip government security officers with the requisite skills and tools to effectively counter online threats (Montasari, 2022). The existing traditional collection methods remain inadequate for conducting a comprehensive online investigation of criminal activities. The prevailing challenges due to overreliance on traditional collection methods, therefore, hinder effective analysis of the connection between the virtual and real world. This often leads to incidences of intelligence failures. There is still a research gap on how well security agencies can mitigate strategic surprises by utilising social media intelligence to complement the existing traditional collection methods. The intervention is important in providing better situational awareness to decision-making.

Limitation of the study

The research dealt with classified information, which might have affected collection of detailed data. However, the researcher explained to the respondents the importance of the study for public good and that all ethical considerations had been approved by the relevant authorities.

Significance of the study

The study addresses existing challenges hindering the efficient utilisation of social media intelligence as a data collection instrument that can complement traditional methods. The advancement of technology and unlimited access to the Internet makes social media a critical source of information due to the changing threat environment and shifting criminal modus operandi. This dynamic requires government security agencies to be in the lead to harness the opportunities and possible measures to mitigate online threats. The study therefore sought to establish the existing challenges and possible mitigation measures that may counter social media criminality in Kenya.

Literature review

Threats emanating from criminal usage of social media sites

Criminals exploit personal data in social media to extort money or target personal accounts from unsuspecting citizens through phishing. Phishing is a form of cybercrime where an individual is lured through email, text messages, or calls by a criminal pretending to be from a legitimate financial institution or a telecommunication company requesting the targeted individual to provide personally identifiable information (Mary et al., 2015). The criminals will use the information to access personal accounts and steal money from the bank or mobile wallets.

Thukral and Kainya (2022) stated that phishing is one of the most straightforward techniques employed is used by hackers to illicitly acquire login credentials, infiltrate personal accounts, and distribute harmful links. Similarly, criminals can generate fake email links that resemble a particular corporate institution that has promotional rewards for the clients to lure vulnerable individuals into providing personal information (Montasari, 2022). The criminals can also forward a link in the form of ransomware to unsuspecting individuals or companies in order to extort money.

Identity theft is another cybercrime activity that involves the intentional exploitation of another person's private information for illegal activity without that person's consent (Tariq & Irshad, 2018). The information obtained could be used for fraud or to generate illegal documents to support in committing crimes. For instance, criminals create fake accounts on social media sites by impersonating senior politicians or government officials for monetary gain. Security agencies require up-to-date technologies to authenticate true identities and deconflict the fake accounts created by criminals.

The malware threat continues to persist and expand due to the massive utilisation of SMPs. This has offered an opportunity for cybercriminals to employ the tactic of embedding malware within posts, friend requests, and updates from friends, and leveraging photo tagging notifications to entice users into opening infected documents. Nadeem and Mohamed (2017) emphasised that the expansion of attack surfaces is accelerated by the multiplicity of social media networking sites and emerging applications. For instance, most of the daily basis routine work or transactions, especially after COVID-19, are done online. This makes it susceptible to criminal attacks.

In addition, criminals use ransomware, a type of software that spreads like a worm and prevents users from accessing their system unless a ransom is paid. Cybercriminals optimise ransomware to extort money from individuals, companies, and institutions with payments mostly in cryptocurrencies to evade security trailing. The incidence of cyberattacks in Kenya had a significant surge of 76%, with exploits emerging as the prevailing method of attack within the country. For instance, the group known as Anonymous Sudan claimed responsibility for a substantial cyber assault in Kenya in July 2023. This resulted in the disruption of many government systems and prompting apprehensions regarding digital security (Amber, 2023).

In efforts to evade security agencies' tracking, criminals now operate on dark websites, which are inaccessible using ordinary search engines but are highly encrypted with peer-to-peer security features that challenge security infiltration (Montasari, 2022). A dark website can be accessed using a unique search

engine called 'The Onion Router' (TOR), which separates individual information and creates anonymity (Finklea, 2017). Moreover, dark web websites are becoming market hubs for criminals' illicit activities, with terrorists advancing to optimise cryptocurrency to evade tracking. Davies (2020) added that the dark web has strong anonymity and encryption features that complicate security monitoring and locating the server's Internet Protocol (IP) or identifying the criminal. Further, Davies highlighted the impersonation of criminals by security agencies or undercover operations and hacking into the dark web websites to be crucial in identifying the individuals involved.

Terrorist online prevalence was evident in 2020 after the European Union Agency for Law Enforcement Cooperation (EUROPOL), collaborating with 17 member states, pulled down more than 1900 Uniform Resource Locators (URLs). The URLs removed from 180 SMPs, were linked to terrorism in a single day (UNICRI & UNCCT, 2021). In 2019, Facebook removed at least 26 million pieces of terrorist content linked to the Islamic State of Iraq and Levant (ISIL) and Al Qaeda. The disruption of terrorist accounts on social media, however, remains a challenge globally as many platforms with different security features emerge. For instance, to counteract these safeguards and keep up their internet activities, the Islamic State of Iraq and Syria (ISIS) shifted its focus to private sites such as Telegram, Signal, and WhatsApp (Weimann & Vellante, 2021). Private social media sites offer criminals anonymity status and control of their associates to minimise security infiltration into their networks.

The usage of social media by terrorist groups poses a multitude of new challenges for social media companies, policymakers, and security agencies (Kumar, 2022). The exponential expansion of SMPs presents a highly advantageous prospect for terrorist organisations to propagate their ideology. For instance, Al-Shabaab has capitalised on the secretive nature of the Kenyan government and the lack of coordinated strategic communication to spread propaganda, mainly following attacks (Mbithi, 2022). The terror group capitalises on propaganda to instil fear in the citizens, expose inadequacies of the government to provide security, and criticise them for fighting a losing war that targets Muslims. In addition, Al-Shabaab propaganda has been established to convince the audience through suggestions that their actions or opinions are moral and correct. This offers them an alternative sense of belonging (Odhiambo et al., 2013). Further, Weimann (2018) revealed that SMPs facilitate the utilisation of a targeting technique referred to as narrowcasting by terrorist organisations. Narrowcasting is a communication strategy that targets specific groups of the public based on their values, tastes, demographic attributes, or subscriptions. Terrorist groups therefore spread targeted propaganda to obtain support from sympathisers who harbour similar ideologies, thereby leaving the security agencies with a huge task of countering.

Challenges of social media intelligence

The mandate of the intelligence community to protect the nation's security means that they must utilise all sources of information both overtly and covertly, including on social media sites. However, proponents of democracy are against this, citing violations of human rights, such as freedom of expression. This debate allows for criminal optimisation as government security agencies battle with policy implementation on monitoring online activities. In addition, government security agencies will use many resources to obtain superior technologies and employ multilingual expertise to counter threats (Omand et al., 2012). Moreover, numerous social media sites exist and many more are emerging, thus technology compatibility ceases with time. SOCMINT therefore proves expensive for government security agencies and calls for a more collaborative way between the government and private social media companies to counter threat dynamics.

SOCMINT can sometimes be misleading if not critically examined, especially in the era of fake news and propaganda. An investigating officer must keenly focus on the context of the data before drawing an assessment (Omand et al., 2012). Despite employing AI to support analysis, the origin of the data or the content will be determined by the investigating officer to ensure an informed judgement to guide policymakers. Therefore, if the information is not well counter-checked, it can lead to poor decision-making and a waste of resources. Additionally, the conservative nature of government security agencies in adopting emerging technologies is among the hindrances to SOCMINT. Barnea (2019) explains that security agencies hesitate to venture into technology compared to the business world. Despite the threat environment, security agencies worry more about losing sensitive data or exposing their operations, thus remaining reactive.

Theoretical framework

Technology acceptance theory

Davis (1986) proposes the Technology Acceptance Theory in his research model on the effects of system characteristics to explain the adoption and usage of information systems. He notes that technology acceptance theory tenets include perceived usefulness and ease of operation as well as external conditions influencing technology. These include language, skills, experience, perceived risks, and social influence. The usefulness of adopting new technology is paramount in improving an individual's performance, thus the efficiency of the technology may be hindered if users do not consider it useful in addressing the specific challenges faced in Kenya's criminal landscape. For example, if social media platforms lack relevant information or if the intelligence generated is not actionable, it may be perceived as less useful, leading to decreased efficiency.

SMPs are user-friendly and have numerous advantages, such as enhancing communication, interaction, social networking, and sharing. Criminals thus capitalise on the usefulness of SMPs to conduct their activities, which challenges security counter strategies.

The ease of operating technology tenet elaborates that the efficiency of social media intelligence in countering criminality may be hindered if the technology is complex or difficult to navigate. If government security agencies or other stakeholders find it challenging to extract relevant insights or interpret social media data, the perceived ease of operation may be low. This leads to reduced efficiency in countering criminal activities. In addition, the efficiency of social media intelligence may be hindered if it is not compatible with the existing strategies, resources, or regulatory frameworks. If there is a mismatch between the technology and the operational requirements of government security agencies or other stakeholders, the adoption and efficiency may be compromised.

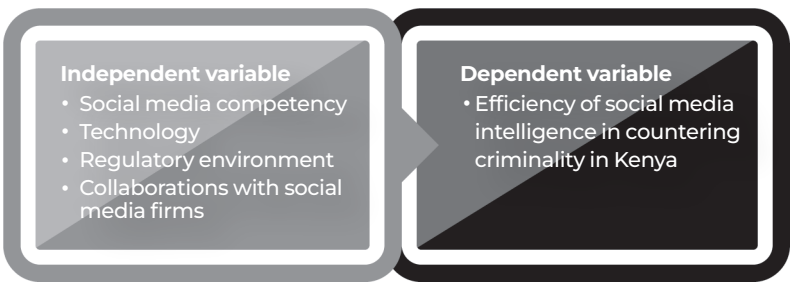
The perceived risk in technology acceptance theory on usage of social media intelligence expounds the concerns about privacy, data security, or the accuracy of information that may hinder efficiency in countering criminality. If stakeholders perceive significant risks in utilising social media intelligence, they may be reluctant to fully embrace the technology, leading to limitations in its effectiveness. Taherdoost (2018) contends that the objective of the Technology Acceptance Theory is based on people's willingness to use new technology. Technology acceptance in the organisation is influenced by the policymaker's understanding of new technology, which informs the decision of whether or not to adopt it.

This theory explains why organisations take time to adopt new technologies despite threat dynamics. The slow pace of acceptance of the technologies might be due to high cost, secrecy doctrine, fear of losing data, and lack of research within the organisation. While government security agencies are grappling to learn about new technologies, criminals leverage utilising the existing technologies to advance their intentions. Government security agencies therefore remain playing catch-up as criminals optimise multiple SMPs to actualise diverse activities. This further complicates countermeasures. With a good understanding of these dynamics, government security agencies can identify effective strategies to address the hindrances and enhance the efficiency of social media intelligence in countering criminal activities in Kenya.

Conceptual framework

Several dynamics hinder the efficiency of utilising social media intelligence in countering criminality. This conceptual framework aims to identify and analyse the key independent and dependent variables that influence the effectiveness of social media intelligence in addressing criminal activities in Kenya. The conceptual framework defines the relationships between the independent variables and the dependent variable (Ravitch & Carl, 2021). These correlations show how the dynamics of each independent variable influence the effectiveness of social media intelligence in combating criminality in Kenya. The independent variables include social media competency, technology infrastructure, legal and regulatory environment, and collaborations with social media companies, whereas the dependent variable is the efficiency of social media intelligence in countering criminality in Kenya. These independent variables collectively shape the effectiveness of utilising social media platforms as a tool of enhancing law enforcement efforts against criminal activities in Kenya. Figure 5.1 shows the conceptual framework.

FIGURE 5.1 ◢ Conceptual framework



Methodology

The study used a mixed-methods research approach and a descriptive research design to gain a comprehensive understanding of the criminal utilisation of SMPs and the challenges faced by government security agencies in countering criminality. The researcher purposively selected four key departments in government security agencies tasked with online counter-organised crime and counter-terrorism within Nairobi to obtain relevant data. The target population was 240 officers from government security agencies mainly responsible for analysing online criminal activities in Kenya.

The researcher applied Yamane's (1967) formula to establish the representative sample size. The sample size was 150 respondents, which allowed the researcher to randomly distribute questionnaires for data collection. In addition, the researcher conducted eight in-depth interviews targeting four (4) heads of

departments and four (4) social media mining experts within the government security agencies. The researcher conducted a pilot test with eight (8) security officers working in the selected departments dealing with online counter-terrorism and eight (8) from online counter-organised crimes. Those who participated during piloting were excluded during administration of questionnaires. Furthermore, a reliability test using Cronbach's alpha established a coefficient of 0.8 (above the desirable threshold of 0.7), indicating that the instruments were highly reliable. (Creswell, 2014).

From the distributed 150 questionnaires, a total of 118 responses were received, indicating a response rate of 78.67%. This is above the threshold of at least 70% which is recommended for a thorough analysis of the research findings. (Kothari, 2011; Mugenda and Mugenda, 2019).

Findings and discussion

The challenges of countering social media criminals

The research sought to establish the challenges that the security agencies faced in countering social media criminals within their departments. The outcome revealed that 102 (86.4%) of the respondents confirmed that they had challenges while 16 (13.6%) did not. The respondents who indicated having challenges had reasons such as criminal use of fake identities to create anonymity, security features of applications, inadequate technical support and skills, bureaucracies of social media corporations, existing weak laws in prosecuting social media crimes and identity of criminals and security role players in the virtual arena.

Criminals' use of fake identities

The research established that criminals used fake identities or pseudonyms to conceal their identities on SMPs. Notably, criminals created anonymous accounts that made it difficult for government security agencies to identify the real users. For instance, when security agencies closed fake accounts, criminals could easily open new accounts using different identities or migrate to other platforms. Therefore, SMPs provided a greater level of anonymity to criminals, whichchallenges government security agencies in tracing the exact location and identity of perpetrators. Moreover, the global interconnectedness increases anonymity as criminals might be from other jurisdictions or using bot accounts to advance their activities. For example, Participant 4 during an interview revealed that:

> *Anonymity of criminals within SMP makes it challenging for government security agencies to put a face on the real user of the account. Additionally, the use of fake details and the changing of a Virtual Private Network (VPN) to a different country to evade security traceability has complicated analysis hence the usage*

of more resources and time during investigation. (P 04)

Futhermore, criminals create fake accounts on social media sites to impersonate senior politicians or government officials for monetary gain while others circulate fake corporate recruitment advertisements to target vulnerable citizens (Mbithi, 2022; Ombati, 2022). The technology acceptance theory explains that the perceived usefulness and ease of operating information systems influence decision-making. This theory demonstrates why criminals prefer SMPs with unlimited restrictions to conceal their activities and remain anonymous. Montasari (2022) states that the freedom of transition from one social media platform to another offers criminals the opportunity to further their sphere of influence leaving security agencies with daunting task in resolving the issues.

Criminals' use of secured applications for communication

The research established that security features of SMPs like Telegram's end-to-end encryption make traceability of the criminal more difficult. For instance, criminals use closed or private social media channels that make retrieval of valuable information complex. In addition, criminals utilise secure applications with auto-delete settings which makes it difficult for government security agencies to get evidence for prosecution. Moreover, criminals compartmentalise online communication using different accounts and coded texts in SMPs to deter security monitoring and locate the exact position of the criminal. The finding was reinforced by Participant 02 during an interview that:

Criminals can change a Virtual Private Network (VPN) to reflect a different country which automatically changes the Internet Protocol (IP) address location to evade security detection. (P 02)

Also, Participant 08 added that:

Encryption remains a challenge for government security agencies to unravel criminal activities within the virtual community. Social media applications with end-to-end users are difficult to intercept as the communication is direct and no third party or linkage is involved. (P 08)

The findings were further emphasised by Participant 1 who said that:

The use of private channels by criminals makes it difficult for government security agencies to monitor their activities. Additionally, security features like end-to-end encryption and peer-to-peer communication allow criminals to communicate freely. For instance, terrorists use open social media sites for general information and targeting of potential recruits, but clandestine terror activities are solely conducted in private channels. (P 01)

Claudia (2021) reveals that the ISIS has widely adopted end-to-end encrypted communication platforms and applications to recruit, communicate with, and distribute terrorist training materials and propaganda among its members and support networks. Furthermore, in an effort to evade security agencies' tracking, criminals now operate on dark websites, which are inaccessible using ordinary search engines but are highly encrypted with peer-to-peer security features that challenge security infiltration (Montasari, 2022). The decision to choose an application for communication by criminals can be better explained by the technology acceptance theory that ease of operation, usefulness, and potential risk of a specific technology influence the adoption and usage (Davis, 1986). For instance, social media provides a platform that may be utilised by criminals to generate the interest and inquisitiveness of a prospective recruit, subsequently transitioning interactions from public platforms such as Facebook to more confidential channels such as WhatsApp or chat room communication (Cox et al., 2018).

Inadequate technical support and skills

Inadequate technical support and skills coupled with insufficient resources hinder effective analysis of social media crimes. The study established that 88 (74.6%) of the government security agencies in the targeted departments had not been trained in social media mining. In addition, 102 (86.4%) of the government security agencies revealed lack of smart analytic tools within the departments, thus hindering the efficiency of social media intelligence in countering criminality in Kenya. For instance, lack of properly trained government security agencies with the necessary skills in social media mining and lack of smart analytic tools contribute to the inadequate utilisation of social media intelligence in countering criminality in Kenya. Moreover, social media applications are ever-evolving and very dynamic, thus requiring continuous training and effective adoption of emerging technologies and tools which require more financial resources. For instance, Participant 04 stated during the interview that:

> *There exists a gap in the development of effective tools to counter social media criminals as the software developers normally work in isolation and do not know the exact challenges faced by the analysts, hence, not providing a comprehensive solution.* (P 04)

Participant 08 further observed that:

> *Some government security agencies are not aware of what is happening within their jurisdictions but are quick to task the online teams, yet crucial information is easily available on SMPs that can help in strengthening investigations.* (P 08)

Consequently, staying up to date with the latest technologies and tools necessitates ongoing training and effective implementation. This was elaborated by the technology acceptance theory that organisations make decisions based on usefulness and ease of operation in choosing a technology to adopt (Davis, 1986). This, in turn, demands a greater allocation of financial resources. Correspondingly, Smith et al. (2015) mentioned that the use of smart analytic tools provides security agencies with a proactive edge in understanding trends, associations, and plans to provide more insights into their modus operandi. This includes ways of evading security agencies or concealing identity within SMPs. Stegen (2019) stated that the current threat environment requires sophisticated collection and analysis of data for government security agencies to be on top of securing the state. The threat environment comprises both the physical and virtual world, thus all source information is critical in mitigating uncertainties.

Existing weak legal framework

The study established that the existing laws for prosecuting online criminals were weak and required a high threshold to pursue a case. For instance, justifying that the material was used for radicalisation and attached to a particular individual is a challenge for security agencies in prosecuting the perpetrator. Similarly, the conversion of information obtained from SMPs to evidence for prosecution remains a hurdle for security agencies. The lack of enforcement from the Communication Authority of Kenya on criminals using highly encrypted applications or private social media sites further complicates countermeasures. For example, during an interview, Participant 06 opined that:

> *A weak legal framework for countering online crimes coupled with high evidential threshold requirements to prosecute social media crimes portends challenges to government security agencies. The current Prevention of Terrorism Act (POTA) framework is inadequate to prosecute online terrorism and the loopholes have been optimised by the suspects' lawyers to ease acquittal or prosecutors' only option is to press penal code charges on the suspect ...* (P 06)

Despite existing laws with clear regulatory measures, enforcement them remains a challenge as most SMPs were from various jurisdictions. For instance, the Kenya Information and Communication [Amendment] Bill (2019) regulates SMPs and demands the owner to provide information upon request by the commission. The existing laws therefore depend more on the goodwill of the social media corporations for them to be effective rather than the government authority to regulate or demand the information as stated in the bill. Omand et al. (2012) established that the intelligence community's mandate to protect national security requires utilising all sources of information, including social media, but proponents argue that it violates human rights and allows criminal optimisation.

Identification problem in virtual realms

The study established that despite the existence of mutual legal agreements to bridge the extraterritorial collection of information on SMPs, it still took a long time to process the requested information for action due to the existing bureaucracies. For instance, when government security agencies requested social media corporations to pull down extremist content on the platforms, it normally takes time to be actioned and even sometimes it is never acted upon. In addition, research found that Kenya had a mutual legal agreement with Meta Platforms Inc. (Meta) only, which further challenges countering social media criminals who utilise other private channels.

During interviews, Participant 08 revealed that:

> *Some social media companies like Telegram and TikTok have no mutual legal agreement with Kenya, thus countering criminal activities on these platforms is difficult, or even obtaining information that can support the prosecution of the offender as the law limits infringement of personal privacy.* (P 08)

In agreement, a study conducted by the United Nations Office of Drugs and Crimes (2021) on mutual legal agreement response rate found 57.7% for no response, 30.8% for quick response, and 11.5% for slow response. This outcome affirms that mutual legal agreement response to requests or support in countering social media criminals is still low. National Association of Attorneys General (2019) observed that obtaining responses from social media corporations situated beyond the legal authority of a particular country posed a significant challenge. Regrettably, the extent to which prosecutors can acquire material varies based on their geographical location. Therefore, social media bureaucracies undermine the effectiveness of social media intelligence in countering criminality.

Existing social media firms' bureaucracies

The study established that there is an existing identification problem between real online criminals and government security agencies operating undercover within the virtual realms. For instance, government security agencies used undercover teams to penetrate criminal networks to obtain crucial information to enhance analysis and inform counter strategies. The virtual community therefore had a mix of undercover government security agencies and real criminals conducting diverse activities with different motives. In addition, the interconnectedness and lack of borders in the virtual world further complicate the identification of security agencies from real criminals due to similar modus operandi. Furthermore, the secretive nature and lack of information sharing among government security agencies widen the rift in identifying real criminals. During interviews, Participant 01 revealed that:

> *It is difficult to know who you are talking to especially since social media has created a borderless boundary. The online community is difficult as many government security agencies are using similar tactics to identify and recruit against online terror networks.* (P 01)

Participant 04 added that:

> *... identifying real criminals and government security agencies within the virtual community tends to affect online investigations since for every 20 people in the virtual investigation, 2 are likely to be criminals while 18 are government security agencies' role players ...* (P 04)

Further, the identification complexities within the virtual world are accelerated by a lack of authority in determining or controlling the users of SMPs (Ates, 2020). This complicates the efficiency of social media intelligence in countering criminality and enhances reactive countermeasures instead of proactive action.

Technological adoption challenges

The researcher provided five parameters related to technological adoption challenges that are likely to affect the efficiency of social media intelligence in countering criminality in Kenya. Thereafter the study sought a level of agreement with a scale rating of 1 to 5 where 1 = Strongly Disagree (SD); 2 = Disagree (D); 3 = Undecided (U); 4 = Agree (A); and 5 = Strongly Agree (SA). Table 5.1 shows the results.

TABLE 5.1 ◢ Technological adoption challenges

Parameters affecting the efficiency of social media intelligence in countering criminality in Kenya	SD (%)	D (%)	U (%)	A (%)	SA (%)
Expensive analytic tools	5.1	3.4	16.9	31.4	43.2
Lack of social media mining training	4.2	0.8	7.6	38.1	49.2
Inadequate social media mining tools	3.4	3.4	13.6	35.6	44.1
Lack of a software developer in the department	5.1	11	18.6	26.3	39
Lack of research and development	3.4	10.2	14.4	26.3	45.8

The outcome established that 74.6% of the respondents agreed that expensive analytic tools affect the efficiency of social media intelligence in countering crimes, while 16.9% were undecided, and 8.5% disagreed. The findings show that most of the respondents strongly agree that expensive analytical tools are a significant factor. Due to limited financial resources, government security agencies may be forced to rely on less expensive or less advanced analytic tools, which may

have limitations in their capabilities, and might hamper effective and efficient analysis in combating social media crimes.

On lack of social media mining training, 87.3% of the respondents agreed, while 7.6% were undecided, and 5% disagreed. The outcomes show that most of the respondents strongly agreed that a lack of social media mining training affects the efficiency of social media intelligence in countering criminality in Kenya. Law enforcement personnel receive training in social media mining to help them comprehend and recognise actionable intelligence from massive data. Lack of training may make investigators struggle to distinguish red flags, patterns, and trends of criminal activities on social media.

Regarding inadequate social media mining tools, 79.7% of the respondents agreed, 13.6% were undecided while 6.8% disagreed. The outcomes show that most respondents strongly agree that inadequate social media mining tools are a crucial factor. This is because security agencies with inadequate technologies may fail to obtain crucial insights in identifying complex criminal networks. Moreover, inadequate social media mining tools reduce the capabilities of proactive monitoring or timely notifications for suspicious criminal activities on SMPs.

On whether lack of software developers in the department affects the efficiency of social media intelligence in countering criminality, 65.3% of the respondents agreed, 18.6% were undecided, while 16.1% disagreed. The results show variations among the respondents but most of them agreed that lack of software developers in the departments affects the countering of social media crimes. Departments may rely largely on commercial off-the-shelf software solutions in the absence of in-house software developers. While it may serve the intended purpose, it may lack the required flexibility or customisation needed to handle the specific needs to counter increasing criminal activities. Using only commercial solutions may thus limit the intelligence agency's capacity to respond rapidly to counter the changing threat conditions to stay ahead of criminals.

Finally, on whether lack of research on new technologies affects social media intelligence in countering criminality in Kenya, 72.1% of the respondents agreed, 14.4% were undecided while 13.6% disagreed. The findings show that most of the respondents agree that lack of research on new technologies affects the countering of social media crimes. Criminals are quick to optimise emerging technologies and techniques to advance illicit activities on SMPs. Without sufficient research on emerging technologies, law enforcement agencies may struggle to understand and anticipate the tactics employed by criminals. As a result, government security agencies will tend to adopt a reactive posture in countering social media crimes instead of data-driven or evidence-based practices.

Despite the wide disparities in the level of agreement, the study established that expensive analytic tools, lack of social media mining training, inadequate social media mining tools, lack of software developers in the department, and lack of research on new technologies greatly affect the efficiency of social media intelligence in countering criminality in Kenya. The findings are similar to what Njoroge (2020) found that institutions still faced huge challenges in adopting new technologies specifically driven by insufficient resources. In addition, technology acceptance theory reinforces the findings and elaborates on the dynamics considered by an organisation in deciding on a particular adoption of technology (Davis, 1986).

Further, there are many SMPs and there are other emerging ones that require customised tools and understanding to enhance the effective countering of threats (Grizāne et al., 2022). Similarly, Taherdoost (2018), stated that the objective of technology acceptance theory is based on people's acceptance of new technology. The acceptance in an organisation can be influenced by the policymakers' understanding of new technology, which will inform the decision of whether or not to adopt it. The challenges of acceptance of technologies can be attributed to high cost, secrecy doctrine, fear of losing data, and lack of research within the intelligence organisation.

Several challenges greatly affect the efficiency of social media intelligence in countering criminality in Kenya. Social media companies develop user-friendly applications that do not require strict authentication in creating accounts or have security features that are only controlled by the administrator of a particular closed group. Similarly, advancement in technology offers an opportunity for criminals and challenges government security agencies to strategise on how to counter while observing the privacy laws of social media users. Comparably, emerging threats are cross-cutting among states and the borderless security system calls for the security security agencies to enhance information sharing, and collaboration among key stake-holders and incorporate all sources of information to effectively counter social media crimes and mitigate existing challenges.

Conclusion

The study established that there is need for the government to improve effectiveness in the utilisation of social media intelligence, mitigate challenges faced by government security agencies in countering social media criminals, and to discourage individuals from attempting or committing online crimes. This can be done by enhancing the capabilities of government security agencies; investing more in research and innovation of smart analytics and social media mining tools; enhancing information sharing and collaborations with social media corporations,

states agencies; and formulating and implementing stringent measures on social media criminals.

Recommendations

This study offers the following recommendations for consideration by the government security agencies:

i. offer training on social media mining and big data analytics, and empower departments with capabilities to monitor and counter social media crimes elevate their playing field;

ii. invest more in research and innovation to develop customised analytic tools, which are geared towards solving the immediate threat;

iii. improve technological infrastructure and invest more in human capital to strengthen online engagements such as social media monitoring and virtual personas to match the increasing challenges of online crimes;

iv. engage all stakeholders in periodic training with government security agency teams with a view to creating awareness to effectively counter of social media crimes; and

v. introduce heavy fines and long-term sentencing for offenders in order to reduce social media criminalities.

References

Almadhoor, L., Alserhani, F., & Humayun, M. (2021). Social Media and Cybercrimes. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 2972–2981. https://turcomat.org/index.php/turkbilmat/article/view/4947

Amber, J. (2023). *Cyberattack in Kenya impacts online government platforms*. Cyber Magazine. https://cybermagazine.com/application-security/cyber attack-in-kenya-impacts-online-government-platforms

Ates, A. (2020). Current Challenges and Trends in Intelligence. *Güvenlik Bilimleri Dergisi*, *9*(1), 177–204. https://doi.org/10.28956/gbd.736153

Barnea, A. (2019). Big data and counterintelligence in Western countries. *International Journal of Intelligence and Counterintelligence*, *32*(3), 433–447. https://doi.org/10.1080/08850607.2019.1605804

Bartlett, J., & Reynolds, L. (2015). Social media intelligence capabilities for counter-terrorism. *State of the Art 2015*, 1–97.

Claudia, J. (2021). Use of the Internet, other cyber and digital platforms as well as digital devices to support and commit acts of terrorism in Eastern Africa. *United Nations Office on Drugs and Crime*, 1–36.

Cox, K., Marcellino, W., Bellasio, J., Ward, A., Galai, K., Meranto, S., & Paoli, G. P. (2018). Social media in Africa: A double-edged sword for security and development. *United Nations Development Programme (UNDP)*.

Creswell, J. W. (2014). *Research Design-Qualitative, Quantitative and Mixed Methods Approaches* (V. Knight, J. Young, K. Koscielak, B. Bauhaus, & M. Markanich (eds.); 4th ed.). SAGE Publications Ltd.

Dahlman, C. (2007). Technology, globalization, and international competitiveness: Challenges for developing countries. *In O'Connor and M Kjöllerström (Ed.), Industrial Development for the 21st Century (Hyderabad: Orient Longman, Zed Books, and United Nations)*, 29–83. http://books.google.com/books?hl=en&lr=&id=DQGy1e9dv_YC&oi=fnd&pg=PA29&dq=Technology+,+globalization+,+and+international+competitiveness+:+Challenges+for+developing+countries&ots=RnSF1-vXf4&sig=Jref-sCx8cPkyqOUlfK3KAHzRu8g

Davies, G. (2020). Shining a light on policing of the Dark Web: An analysis of UK investigatory powers. *Journal of Criminal Law*, *84*(5), 407–426. https://doi.org/10.1177/0022018320952557

Davis, F. D. (1986). A technology acceptance model for empirically testing new end-user information systems: Theory and results. *Massachusetts Institute of Technology*. https://doi.org/10.1126/science.146.3652.1648

Dencik, L., Hintz, A., & Carey, Z. (2018). Prediction, pre-emption, and limits to dissent: Social media and big data use for policing protests in the United Kingdom. *New Media and Society*, *20*(4), 1433–1450. https://doi.org/10.1177/1461444817697722

Farzindar, A., & Inkpen, D. (2015). Natural language processing for social media. *Synthesis Lectures on Human Language Technologies*. https://doi.org/DOI 10.2200/S00659ED1V01Y201508HLT030

Finklea, K. (2017). Dark Web. *Congressional Research Service*. https://doi.org/10.4018/978-1-7998-5567-5.ch024

Grizāne, A., Isupova, M., & Vorteil, V. (2022). Social media monitoring tools: An in-depth look. *NATO Strategic Communications Centre of Excellence*. http://blog.namics.com/2010/05/social-media-monitoring-tools2.html

Gundechahuan, P., & Liu, H. (2014). Mining social media: A brief introduction. *Informs Tutorials in Operations Research 2012.*, *November 2018*, 1–17. https://pubsonline.informs.org/doi/10.1287/educ.1120.0105

Hossain, M. S. (2018). Social media and terrorism: Threats and challenges to the modern era. *South Asian Survey*, *22*(2), 136–155. https://doi.org/10.1177/0971523117753280

Johnson. (2010). *The Oxford Handbook of National Security Intelligence*. Oxford University Press, Inc198 Madison Avenue, New York, New York 10016 www.oup.com.

Kimutai, J. K. (2014). Social media and national security threats: A case study of Kenya. In *[Masters Thesis, University of Nairobi]*.

Kothari, C. R. (2011). *Research Methodology Methods and Techniques.* New Age International, New Delhi. https://doi.org/10.4236/ajibm.2014.412080

Kumar, R. (2022). *Social Media a Tool for Terror*. National Security Law & Policy. https://jnslp.com/2022/09/16/social-media-a-tool-for-terror/

Liaropoulos, A. N. (2013). The challenges of social media for the Intelligence Community. *Journal of Mediterranean and Balkan Intelligence*, *1*(1), 5–14. https://www.researchgate.net

Maltego. (2022). *Understanding the different types of Intelligence Collection Disciplines*. https://www.maltego.com

Mary, S., Usha, S., Bobby, Syiemlieh, P., & Mary Khongsit, G. (2015). Phishing is an analysis of the types, causes, preventive measures, and case studies. *Computer Engineering*. https://www.iosrjournals.org

Mbithi, J. V. (2022). Impact of Social Media on National Security in Kenya. In *Post Graduate Diploma Project from the University of Nairobi*.

Montasari, R. (2022). Artificial Intelligence and National Security. In *Artificial Intelligence and National Security*. https://doi.org/10.1007/978-3-031-06709-9

Mugenda, O. M., & Mugenda, A. G. (2019). *Research Methods: Quantitative, Qualitative & Mixed Methods Approaches* (Third). Centre for Innovative Leadership & Governance.

NAAG. (2019). *Overcoming Hurdles to Secure Evidence from Social Media Companies in Cybercrime Investigations and Prosecutions - National Association of Attorneys General*. National Association of Attorneys General. https://www.naag.org/attorney-general-journal/overcoming-hurdles-to-secure-evidence-from-social-media-companies-in-cyber crime-investigations-and-prosecutions/

Nadeem, S., & Mohamed, F. (2017). Ransomware-Threats, Vulnerabilities And Recommendations. *International Journal of Scientific & Technology Research*, *6*(06), 307–309.

Njoroge, A. W. (2020). *Intelligence aspects of big data analytics for Kenya's national security*.

Odhiambo, E., Maito, T., Kassilly, J., Chelumo, S., Onkware, K., & Oboka, W. (2013). Al-Shabaab terrorists propaganda and the Kenya government response. *International Journal of Humanities and Social Science*, *3*(7), 125–131. https://www.scirp.org

Olasya, D. P. (2018). *Assessing the impacts of social media on national security in Kenya*. The University of Nairobi.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

Ombati, C. (2022). *10 social media users were arrested for impersonating senior officials*. https://www.the-star.co.ke/news/2022-11-04-10-social-media-users-arrested-for-impersonating-senior-officials

Pantucci, R. (2020). A View from the CT Foxhole: Jonathan Evans, Former Director General, MI5. *CTC Sentinel*, *13*(3), 9–15. www.ctc.usma.edu/sentinel/

Ravitch, S., & Carl, N. (2021). Conceptual Frameworks in Research. *Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological*, 32–61.

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, *9*(1), 211–222. https://doi.org/10.1016/j.dcan.2022.06.005

Smith, M. A., Shneiderman, B., Milic-Frayling, N., Rodrigues, E. M., Barash, V., Dunne, C., Capone, T., Adam, P., & Gleave, E. (2015). Social media analysing networks with NodeXL. *Reputation Management: The Key to Successful Public Relations and Corporate Communication*, 126–152. https://doi.org/10.4324/9781315879987-12

Stegen, J. I. (2019). *Social Media Intelligence (SOCMINT) within the South African context: A theoretical and strategic framework for the national security environment Prof A Duvenhage Co-promoter: Prof MN Wiggill*. *May*.

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, *22*, 960–967. https://doi.org/10.1016/j.promfg.2018.03.137

Tariq, R. S., & Irshad, S. (2018). Identity Theft and Social Media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1), 43. https://www.researchgate.net/publication/323185128

Thukral, P., & Kainya, V. (2022). How social media influence crimes. *Indian Journal of Law and Legal Research*, *IV*(II).

UNICRI, & UNCCT. (2021). Countering Terrorism Online with Artificial Intelligence. *An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia*.

Weimann, G. (2018). Science & Technology Terrorist Migration to Social Media. *Georgetown University Press*, *16*(1), 180–187.

Weimann, G., & Vellante, A. (2021). The Dead Drops Of Online Terrorism: How Jihadists Use Anonymous Online Platforms. *Perspectives on Terrorism*, *15*(4), 39–53.

Yamane, T. (1967). *Statistics: An Introductory Analysis, 2nd Edition, New York: Harper and Row.*