UNIVERSITY OF NAIROBI
INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

IMPACT OF SOCIAL MEDIA ON NATIONAL SECURITY IN AFRICA: CASE STUDY KENYA

BY
IMMACULATE MUENDI WAMBUA
R47/35875/2019

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF POSTGRADUATE DIPLOMA IN STRATEGIC STUDIES.

NOVEMBER, 2020

DEDICATION

This research project is dedicated to my family and especially to my husband, who has supported in whatever I do to ensure that I always give out the best.

ACKNOWLEDGEMENT

For the knowledge and wisdom, strength and good health, I owe them to the Almighty God; to Him I give Him the Glory.

My sincere appreciation goes to my supervisor, Prof Amb Maria Nzomo, Phd for offering to supervise me at the eleventh hour and for the selfless and professional guidance she accorded me throughout the project despite her tight work schedule.

Special dedication to Victor Muithya as one of my directing staff who sacrificially guided me throughout this project paper.

I hereby acknowledge my husband Stephen, daughter Hope and sons Mark and Victor, my nephew George for their support in one way or another towards the triumphant conclusion of this research project.

DECLARATION

I declare that this is my original work and has not been submitted for any award at any other university

Signature……………………………………..Date………………………………………

IMMACULATE MUENDI WAMBUA

Supervisor:

The research project is submitted for examination with my approval as the university supervisor

Signature……………………………………..Date………………………………………

PROFESSOR AMBASSADOR MARIA NZOMO, PHD.

ABSTRACT

This study focuses on the social media sphere in Africa with specific focus on Kenya and the various implications on national security. As internet technology continues to proliferate through the continent, there is a need to assess the role of social media in national security and develop appropriate policies to regulate online content. Issues such as cyberterrorism are still new to the continent, and Kenya as the technology hub of East Africa needs to pioneer change in online forums to better develop security policy. The aim of this study is to analyze the impact of social media on national security in Africa: case study of Kenya. The three specific objectives guided the study; to assess the nature of social media in Africa; to determine the impact of social media use on national security in Kenya; to examine the use of social media in Kenya and how it has impacted on national security. The study adopted a descriptive survey research design. The researcher used primary and secondary data as the main source of information. Primary data was obtained from questionnaires filled by social media influencers and users with different exposure to different platforms, different genders and careers. Secondary data was obtained through in-depth study of the findings of various material in this topic of social media. The target population comprised of 30 respondents in Kenya. The data collected and findings from the various sources made inferences through discussions based on the three objectives of this study. The data collected for the study established that social media has a significant impact on national security in Kenya. The government applies social media in various aspects of governance with varying results. The study further proved that social media is growing in popularity in the country and security agencies lag behind in the application of internet technologies to address crucial security issues in the country. The study concluded that cybercrime and cyberterrorism remain a significant threat to national security and security agencies are not doing enough to curb online crime. In Africa, social media usage is on the rise and governments are increasingly engaging citizens through online platforms. Similarly, terrorists and other non-state actors are using the platforms to spread propaganda and compromise national security. The readiness of security organs to deal with the online threat is critical in today's world. The study identifies the various weaknesses of cybersecurity in Kenya, especially in relation to social media, such as phishing attacks, trojans and malware. It recommends that Kenya needs to reevaluate the internet technology framework and provide lasting solutions to cybercrime. The government needs increased focus on education and research in the field of cybertechnology to ensure that security agencies are proactive against online threats. The study also recommends that the government needs stricter laws on social media platforms to protect against hate speech, misinformation and propagation of crime.

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AMISOM - African Union Mission in Somalia.

CAK - Communications Authority of Kenya.

CDC - Centre for Disease Control and Prevention.

CEO - Chief Executive Officer.

CIA - Central Intelligence Agency.

COVID 19 - Corona Virus Disease.

DCI - Directorate of Criminal Investigation.

DHS - Department of Homeland Security.

DR - Democratic Republic.

EU - European Union.

ICT - Information and Communication Technology.

ISIL - Islamic State of Iraq and the Levant.

ISIS - Islamic State of Iraq and Syria.

KDF - Kenya Defence Forces.

KE-CIRT/CC - Kenya Computer Incident Response Team-Coordination Centre.

KOT - Kenyans on Twitter.

Mpesa - Mobile money transfer service in Kenya.

NIS - National Intelligence Service.

OAU - Organization of African Unity.

PDP - People's Democratic Party.

PC - Personal Computer.

TJRC - Truth Justice and Reconciliation Commission.

UGT - Uses and Gratification Theory.

UN - United Nations.

UNDP - United Nations Development Programme.

WHO - World Health Organization.

Table of Contents

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

Social media is viewed as the most widely adopted technological invention in the 21st century. Social media has evolved to revolutionize social communication in the world. The development of small screens has made it possible for people to own and communicate through handheld devices and Personal Computers (PCs) from anywhere in the globe[1]. Forms of media such as television have changed with the emergence of the small screens as mass media has become increasingly mobile. Wireless laptops, cell phones, tablets and the iPad have become the basic devices for online conversations, collaboration and linkage.

In the recent past, social media networks such as Facebook, Twitter, YouTube, Instagram and Reddit have become a staple in the daily lives of people around the world. These networks form the primary form of interaction between individuals, governments and businesses[2]. Modern social media emerged from the Web 2.0 revolution, which incorporated a variety of applications and features which promoted interoperability, sharing and multiple way communication. The launch of Facebook in 2004 paved the way for the development of other social media platforms. These networks grew in prominence with users, becoming stitched on the fabric of modern society.

The significance of these websites grew from the fact that users spent a significant amount of time interacting with other users and creating and updating online profiles[3]. The accessibility of social media has attracted a plethora of opinions, ideologies and 'facts' from people of different backgrounds. Consequently, social media networks have become hotbeds of misinformation, propaganda and promotion of both positive and negative agendas. Politicians,

[1] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

[2] Ibid

[3] Ibid

celebrities, religious groups, terrorist organizations and individuals have taken advantage of the scope of social media to spread their information and ideas. Globalization has enabled social media to reach beyond continental borders, creating strong online movements that have been responsible for shaping social, economic and political status in the world[4].

Developed nations have worked to ensure that everyone has access to the internet. Developing countries are also collaborating with the private sector to enhance the connectivity of their population. Governments have adopted social media as the platform of official communication regarding various public service issues[5]. Education, healthcare and national economy are some of the issues whose discourse is primarily hosted on social media. In the recent past, national security issues have emerged as a vital discussion on these online forums. Non state actors such as protestors, terrorists and criminals have gained the ability to influence policies which shape national and international security. States are gradually losing their power as groups and individuals are able to galvanize support, organize protests and start movements that will force policy makers to pass certain laws on national security[6]. Activists have used social media to amplify their voices and coordinate actions against government and law enforcement. The Arab Spring of 2011 is a significant example of how social media is a powerful tool that impacts national security matters.

In the 21st century, terrorist organizations such as al-Qaeda, ISIS and right-wing political organizations have used the internet to spread propaganda on their ideologies, coordinate attacks and as a recruitment tool[7]. Twitter has been especially notorious in the past as the host forum for various terrorist organizations such as Al-Shabaab and Taliban. The advancement of

[4] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.
[5] Jost, John T., Pablo Barberá, Richard Bonneau, Melanie Langer, Megan Metzger, Jonathan Nagler, Joanna Sterling, and Joshua A. Tucker. 2018. "How Social Media Facilitates Political Protest: Information, Motivation, And Social Networks". *Political Psychology* 39: doi:10.1111/pops.12478.
[6] Lerner, Jennifer S. 2019. "Decision Science Meets National Security: A Personal Perspective". *Perspectives On Psychological Science* 14 (1): doi:10.1177/1745691618815822.
[7] Demidov, Oleg. 2012. "Social Networks In International And National Security". *Security Index: A Russian Journal On International Security* 18 (1): doi:10.1080/19934270.2012.634122.

social media technology has allowed these groups to misuse the speed of algorithms to market their ideas and beliefs. The global battlefield of war has changed as a result. Nefarious actors within and outside the government have implemented information warfare to support certain narratives in favor of and against national security[8]. Social media is an essential tool for actors to weaken trust in national institutions, challenge national values and culture and influence the international community on certain aspects of global security. This has transformed modern warfare from periodic conflict to continual competition that carries on within the depths of the internet. Individuals with uninformed ideas, unverifiable facts and extreme ideologies have a global reach, which promotes offensive use of social media to threaten national security in different countries. Therefore, there is a need to constantly monitor the working of social medial platforms, their algorithms and their potential influence on key social and political issues.

The challenges for using social media for national security matters include, disclosing information that can be used by the enemy, sharing unacceptable political views, posting discriminatory comments and copyright infringement[9]. On the other hand, social media provides an opportunity for a nation to reach strategic national security objectives, predict how threats will work in the future and how to counter their effects[10]. Law enforcement agencies can use social media to cultivate transparency and accountability to the public, maintain social connections with family, friends and support groups and seek networking opportunities with professionals in different fields. The exponential increase of social media tools and users gives platform-based service providers the ability to provide personalized services, recommending content to friends and upgrading the user experiences[11]. Users therefore become more addicted

[8] Ibid

[9] Ramona, Diana L, and Liana M Marcu. 2016. "Social Media Platforms As A Tool For Sharing Emotions. A Perspective Upon The National Security Agencies". *Management Dynamics In The Knowledge Economy* 4 (1): 141-152.

[10] Ibid

[11] Lerner, Jennifer S. 2019. "Decision Science Meets National Security: A Personal Perspective". *Perspectives On Psychological Science* 14 (1): doi:10.1177/1745691618815822.

to their personal beliefs and sentiments, reinforced by shared experiences with friends. This results in the creation of user-centered contents ecosystems, which can be both beneficial and dangerous to national security.

Social media ecosystems are designed to foster the interests of people, who would otherwise not interact in the real world. Unfortunately, these forums suffer from data interception, information fraudulence, copyright infringement, privacy spying, and non-friendly participation bodies[12]. Attackers threatening national security may hijack communications between users and insert their own information meant to destabilize a nation. In the past decade, the increase in social media cybersecurity incidents has resulted in explosive results for individuals and nations as well. The potential of interception of messages in social media calls for increased responsibilities of organizations and platform monitoring services[13]. There is a need for these social media ecosystems to establish security and trustworthiness. These features are essential for service efficiency, content creation and recommendations and information management. The biggest challenge for security agencies and social media organizations, in the development of sophisticated cybersecurity technology, that will enable identification of roles and behaviors of users, while respecting their privacy needs[14].

The enthusiasm for Information and Communication Technology (ICT) requires an objective understanding of the implications of privacy. Social media platforms leverage images, videos and location data for users as part of their user experience package[15]. The user data contains information such as age, gender, political beliefs, religious beliefs, hobbies and geographic data which is important for communications, social interactions and business transactions.

[12] Jost, John T., Pablo Barberá, Richard Bonneau, Melanie Langer, Megan Metzger, Jonathan Nagler, Joanna Sterling, and Joshua A. Tucker. 2018. "How Social Media Facilitates Political Protest: Information, Motivation, And Social Networks". *Political Psychology* 39: doi:10.1111/pops.12478.
[13] Ibid
[14] Ibid
[15] Demidov, Oleg. 2012. "Social Networks In International And National Security". *Security Index: A Russian Journal On International Security* 18 (1): doi:10.1080/19934270.2012.634122.

Institutions such as banking, healthcare, defense entertainment and industry rely on this information to better understand their users and shape their online experience. This influx of unregulated private information might be used by totalitarian governments and non-state actors to influence national security policies[16]. Unmonitored surveillance of civilian activity on social media sites changes the discourse on national security across the legal, constitutional, socio-economic and political landscapes. The threat of data mining and hacking raises challenges to national security agencies on sharing national security affairs through social media platforms.

The advancements in computer science have enabled the growth of social media to the point where exchange of information has a global influence[17]. Social media is largely outside state control and does not discriminate. This study examines how the freedom of social media can be used to foresee emerging threats and how to leverage critical information for national security purposes. There is a clear disconnect between national security policy and social media use. Further, the generational gap in the use and understanding of social media makes it an unreliable tool for essential communications[18]. This paper elaborates the aim for regulation and enforcement of innovative policies to develop a culture where personnel understand the limitations of social media. It is important to comprehend the various interactions that shape online trends, the spread of information and the key areas of the internet that have the biggest public influence. This paper provides recommendations on how to fix the issues within social media technologies that are detrimental to national and international security.

1.2 Statement of the Problem

Social media is among the 21st century inventions that have defined and changed social and political interactions across the world. Technology has seen the creation of better and improved

[16] Ibid

[17] Eltanawy, Nahed, and Julie B Weist. 2011. "Social Media In The Egyptian Revolution: Reconsidering Resource Mobilization Theory". *International Journal Of Communication* 5.

[18] Chukwuere, Joshua Ebere, and Francis Onyebukwa Chijioke. 2018. "The Impacts Of Social Media On National Security: A View From The Northern And South- Eastern Part Of Nigeria". *International Review Of Management And Marketing* 8 (5). doi:10.32479/irmm.6852.

means of communication with social media use shaping the Society in all aspects be it political, economic, social, security, health and entertainment issues. Social media has become embedded into the fabric of everyday life, with a significant feature of many platforms supporting anonymity of users away from the governments' eyes. Various countries across the world have witnessed the full impact of misuse of social media.

The Kenyan government has established several measures to combat the spread of hate speech and online abuse on social media. The spread of hate speech, especially during election period has been a significant problem to national security in Kenya. The government has made several arrests of prominent individuals and social media users inciting violence and rebellion through social media. However, there is still the issue of fake news. There are no legislations or initiatives to curb the creation and spread of fake news in Kenya. The media in Kenya has fallen victim to misinformation campaigns which have been detrimental to political and economic stability. Further, cyberterrorism has established itself as a new threat to national security. Hackers and malicious actors have used social media platforms to threaten national security and advertise their acts of violence. There is a deficiency of research on how social media contributes to national security, especially in third world nations. While developed nations have solid investments and national agencies focusing on online crimes, African nations have yet to utilize the full capabilities of internet technologies at their disposal. Therefore, there is a need to research on the extent of the threat of social media to national security in Kenya and the necessary legal and technological policies needed to address the threats.

1.4 Research Questions

The following three questions have been designed to guide the study:

1. What is the nature of social media platforms that are in use in Africa?

2. Has social media impacted positively or negatively in the achievement of national security goals in Africa?

3. How has the use of social media shaped opinions and influenced national security in Kenya?

1.4 Objectives of the study

1.4.1 General Objective

The main objective of the study is to establish how social media impacts on national security in Africa, case study of Kenya.

1.4.2 Specific Objectives

1. To assess the nature of social media and national security in Africa.
2. To determine the impact of social media use on national security in Africa.
3. To examine the use of social media in Kenya and how it has impacted on national security.

1.5 Justification of the Study

1.5.1 Academic Justification

The purpose of this research paper is to examine the various social media platforms used in Kenya and address the implications of the increasing use of social media on national security, the responsibilities of security organizations and the necessary changes of social media use for the benefit of national security. The key concerns of this study are the arguments for and against social media use on national security threats across the world and more specifically in Kenya.

The rapid and dynamic social platforms are evolving rapidly and it informs the need for education sector to sensitize the students, to create awareness as well as inform research with the ever-changing technology and increasing cyber threats. This study acknowledges the extent of social media use among young people and the lack of technical knowledge needed to understand the threats in digital spaces. The findings on this study will establish a framework for building a national curriculum to address the digital knowledge deficiencies of the population and inform on how to eliminate the hurdles to communication through social media, effective security regulations and define the way forward in sharing of crucial national security information online.

1.5.2 Policy Justification

This study was undertaken to highlight the increasing use of social media platforms, both positive and negative uses through the years, the influence on national security and the challenges faced in regulating information transfer through the platforms. This research is timely as it examines the growing pains of developing nations in handling the consequences of social media on security institutions. It is an area of security studies that requires more discussion and research in information technologies, data analysis and social media privacy, regulation and policy development. It incorporates the legislature and judiciary, the two arms of government with the biggest impact on the development and enforcement of digital policy. The research analyses the specific roles of the legislature in creating laws, the various hurdles posed by the judiciary and the way forward in creating efficient digital laws. This paper addresses the implications of social media on national security, the responsibilities of security organizations and the necessary changes to social media policy for the advancement of national security goals.

1.6 Limitation of the Study

The scope is limited to national security only and the time required to plan, compile responses and compare to secondary research will limit the depth of the research. Further, given the sensitivity of discussing sensitive security information, the respondents and secondary sources may not have adequate data to compile a robust response to the research questions. The primary data collected will inform the key aspects of the study.

1.7 Literature Review

International politics are characterized by issues bordering on maintaining and tackling national security challenges across the globe. Policy makers, decision-makers and leaders across the globe have recognized the difficulties in creating robust national security policies in the age of information[19]. Today, smartphones and PCs are being mass produced as their demand increases. Many social and personal services today can be conducted from the convenience of an internet device. People with access to the internet can pay for social services, register to vote, communicate directly with leaders, debate with peers through social media and voice their opinions on crucial international affairs in a public forum. This widespread accessibility to the internet creates unprecedented consequences for a state strategic interest. Mass media is no longer the only government watchdog; anyone can criticize and complement the government on matters of national security. The use of social media presents a chance for a nation to achieve strategic goals through public participation.

Facebook was founded in 2004, YouTube in 2005 and Twitter in 2006. These platforms have in the recent years been used as the primary discussion and communication forums for political issues. Social media has been linked to the spread of political protest in several cities around the world including Tripoli, Moscow, Madrid, Athens, Kiev, Hong Kong and Istanbul. On Twitter the #OWS (Occupy Wall Street), #Jan 25 (Egypt protests) and #direngeziparki (Turkish protests) movements have defined political movements in the past decade. These hashtags are easily connected to message content, user metadata and social networks. Researchers can access critical information on user metadata, which presents an unparalleled opportunity for scientific research.

[19] Chukwuere, Joshua Ebere, and Francis Onyebukwa Chijioke. 2018. "The Impacts Of Social Media On National Security: A View From The Northern And South- Eastern Part Of Nigeria". *International Review Of Management And Marketing* 8 (5). doi:10.32479/irmm.6852.

The Arab Spring in 2011 is a model of the significance of social media in instituting an uprising against oppressive regimes[20]. The role of social media in the Arab Spring has been a hotly contested topic among researchers for the past few years. Some researchers have deduced that collective intelligence and crowd dynamics in social media have enormous power to support a collective action[21]. In Egypt and Tunisia Facebook and Twitter had a key role in organization of protests and spreading awareness among the citizens. The social media movements were started by frustrated citizens who set out to organize nationwide protests and labor protests. Movements such as the April 6 Movement of 2008 and Progressive Youth of Tunisia were an example of the influencing power of Facebook and Twitter in national issues[22]. After the Arab Spring protests began, the number of Facebook users in the Arab world increased to over 27 million people[23]. Researchers suggested that this facilitated the concept of a digital democracy in North Africa which formed the basis of future uprisings. Users created Facebook pages to raise awareness on issues such as police brutality and other crimes against humanity in the Egyptian Revolution[24]. The collaborative efforts of western social media and Arabs resulted in one of the biggest social media revolutions in recent history.

“Social media in general, and Facebook in particular, provided new sources of information the regime could not easily control and were crucial in shaping how citizens made individual decisions about participating in protests, the logistics of protest and the likelihood of success”[25].

[20] Mellen, Roger P. 2012. "Modern Arab Uprisings And Social Media: An Historical Perspective On Media And Revolution". *Explorations In Media Ecology* 11 (2): doi:10.1386/eme.11.2.115_1.

[21] Eltanawy, Nahed, and Julie B Weist. 2011. "Social Media In The Egyptian Revolution: Reconsidering Resource Mobilization Theory". *International Journal Of Communication* 5.

[22] Hirschkind, Charles. 2011. "From The Blogosphere To The Street: Social Media And Egyptian Re Mellen, Roger P. 2012. "Modern Arab Uprisings And Social Media: An Historical Perspective On Media And Revolution". *Explorations In Media Ecology* 11 (2): doi:10.1386/eme.11.2.115_1.volution". *Oriente Moderno* 91 (1): doi:10.1163/22138617-09101007.

[23] Mellen, Roger P. 2012. "Modern Arab Uprisings And Social Media: An Historical Perspective On Media And Revolution". *Explorations In Media Ecology* 11 (2): doi:10.1386/eme.11.2.115_1.

[24] Eltanawy, Nahed, and Julie B Weist. 2011. "Social Media In The Egyptian Revolution: Reconsidering Resource Mobilization Theory". *International Journal Of Communication* 5.

[25] Tufekci, Zeynep, and Christopher Wilson. 2012. "Social Media And The Decision To Participate In Political Protest: Observations From Tahrir Square". *Journal Of Communication* 62 (2): doi:10.1111/j.1460-2466.2012.01629.x.

Citizens in the Arab world were able to create a public sphere of communication through social media, where, through cohesive efforts they were successful in demanding changes from their governments. However, the use of social media also alerted terrorist organizations and sectarian groups who used the platforms to incite division among the people and promote more violence[26]. The government agencies could not control the spread of misinformation, the proliferation of images of violence across social media and the increasing interest of Western nations on the situation in the Arab world[27]. Governments and regimes were toppled, but at the expense of many lost lives, displacement of civilians and destabilization of an entire region. While social media had been used as a tool to unite the people against oppression, it also became a source of images that portrayed the violence and brutality of governments against their own people[28]. The uncontrolled flow of information meant that people could share images of dead people, seriously wounded individuals and the level of destruction caused by the government and terrorist forces. This shed light on an important issue of international and national security that forced the international community to intervene and attempt to solve their issues. On the other hand, terror groups such as Boko Haram in Nigeria uses social media to facilitate their activities. They use social media mainly to share propaganda and attract recruits. Their social media use is however not sophisticated as their counterparts in Al-Shabaab and ISIS. Their operations on social media have however increased after their allegiance to ISIL. The use of social media by terror groups poses a great challenge for national and international security agencies in the war against radicalization.

Social media is a structured medium that accommodates accelerated transmission of political and social events. Information technology has fostered the creation of a more participatory

[26] Mellen, Roger P. 2012. "Modern Arab Uprisings And Social Media: An Historical Perspective On Media And Revolution". *Explorations In Media Ecology* 11 (2): doi:10.1386/eme.11.2.115_1.
[27] Hirschkind, Charles. 2011. "From The Blogosphere To The Street: Social Media And Egyptian Revolution". *Oriente Moderno* 91 (1): doi:10.1163/22138617-09101007.
[28] Ramona, Diana L, and Liana M Marcu. 2016. "Social Media Platforms As A Tool For Sharing Emotions. A Perspective Upon The National Security Agencies". *Management Dynamics In The Knowledge Economy* 4 (1): 141-152.

network, with better information access and more opportunities of engagement on public events and participation in collective action[29]. Nevertheless, the use of social media by anti-government actors provides an opportunity for security authorities to detect and suppress protest activity. When the Hong Kong protests began in 2019, social media was again an effective tool for mobilizing the masses and organizing antigovernment protests. However, in this case, misinformation, disinformation, doxing and spreading of unverified rumor served to increase polarization among the public. The Chinese have a track record of using internet censorship to quash any attempts at public protest and demonstrations, while controlling the public opinion of the government on social media[30]. In Hong Kong, both the protestors and government used social media to incite violence and spread propaganda, which had worsened the situation in the country. Today, there exists a technological game of cat and mouse between dissidents and defenders of the existing regime, which is unlikely to dissipate in the near future.

Accurate content creation and circulation is one of the most powerful ways to target, attract and engage a target audience. Fake news has emerged as a new way to undermine national security in the world. Fake news is used as a weapon for organized disinformation campaigns, purposely aimed at sabotaging states by subverting societies and democratic processes[31]. During the 2016 American general election, the term fake news solidified itself in both mass media and social media. There were questions over the legitimacy of news that the Russian government had conspired to divide the American society through Facebook and Twitter[32]. President Donald Trump criticized the media of spreading fake news in an attempt to undermine his presidential victory. Fake news has been used as a tool by alt-right groups spreading disinformation on anti-globalism and neo-liberalism. Spreading of false information

[29] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.
[30] Jost, John T., Pablo Barberá, Richard Bonneau, Melanie Langer, Megan Metzger, Jonathan Nagler, Joanna Sterling, and Joshua A. Tucker. 2018. "How Social Media Facilitates Political Protest: Information, Motivation, And Social Networks". *Political Psychology* 39: doi:10.1111/pops.12478.
[31] Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media And Fake News In The 2016 Election". *Journal Of Economic Perspectives* 31 (2): doi:10.1257/jep.31.2.211.
[32] Ibid

through social media to shape national opinion has become commonplace in European politics in the past few years[33]. Russia and China are the main perpetrators of spreading fake news within and outside their borders. China has an extensive program of monitoring social media use and spreading fake rumors and protesting messages against the government as a strategy to solicit more domestic support. The fake news phenomena have further highlighted the negativity of social media in controlling the public against or in support of certain government policies[34].

New media has changed the relationship between parties and individuals using the internet. There is an increasing need for people to remain connected and updated on the latest issues within their borders and in the international sphere[35]. More social networking applications are being developed for cell phones and PCs. The future of mobile technology promises better connection for internet users and more efficient ways to share information. The negative attributes of social media will be amplified as more people get a voice and the flow of information remains unregulated[36]. Studies have shown that increased access to online information by the public, coupled with inability to regulate the accuracy of information will exacerbate the negative impact of social media on society. As online communication replaces real-world face-to-face communication, consensus-building is decreased and it will be harder to form social movements. Web based technologies are further increasing the polarization in society by hosting forums for people with extremely radical and divisive ideas[37]. The purpose of social media is to give everyone a voice. However, it is time to reevaluate its usage in the past few years and the lasting implications to global security.

[33] Ibid

[34] Ibid

[35] Mellen, Roger P. 2012. "Modern Arab Uprisings And Social Media: An Historical Perspective On Media And Revolution". *Explorations In Media Ecology* 11 (2): doi:10.1386/eme.11.2.115_1.

[36] Jost, John T., Pablo Barberá, Richard Bonneau, Melanie Langer, Megan Metzger, Jonathan Nagler, Joanna Sterling, and Joshua A. Tucker. 2018. "How Social Media Facilitates Political Protest: Information, Motivation, And Social Networks". *Political Psychology* 39: doi:10.1111/pops.12478.

[37] Demidov, Oleg. 2012. "Social Networks In International And National Security". *Security Index: A Russian Journal On International Security* 18 (1): doi:10.1080/19934270.2012.634122.

1.8 Theoretical Framework

Several theories can explain how communication through social media influences society and how content shared can impact on national security.

1.8.1 Uses and Gratifications Theory

The uses and gratifications theory by Elihu Katz and Jay Blumler is a subset of the Maslow's Hierarchy of Needs. This theory discusses how people will actively consume specific media for particular purposes and intentional goals. Active audience possess the ability to consciously examine and evaluate media as they target specific outcomes[38]. People on social media seek information that fulfill their curiosity needs or directly influence their welfare. In terms of content on national security, users of social media platforms will interact with content that directly influences their well-being. For example, in the case of a terrorist attack, the images and messages shared through social media will attract interaction from civilians who feel the immediate impact of the terrorist threat[39]. People in large cities will be more active on social media, condemning and sharing their worries over the potential of future attacks on other regions.

The UGT theory assumes that the audience is active, and goal oriented in their media consumption. Further, the different forms of media are in competition with other means of need satisfaction[40]. In recent times, Twitter has become the primary interaction platform for global affairs of security. The audience of content regarding national and international security will remain active in hashtags started on Twitter to bring society together. Some audiences will browse Twitter and other social media just to keep informed on the situation. Others will use the opportunity to express their opinions, views and condolences to the individuals affected by

[38] Moreno, Megan A, and Rosalind Koff. 2015. "11. Media Theories And The Facebook Influence Model". *The Psychology Of Social Networking Vol.1*. doi:10.1515/9783110473780-013.
[39] Ibid
[40] Ibid

a certain security event[41]. The platform that provides the best user experience, content sharing and interaction will have the biggest audiences.

1.8.2 Social Impact Theory

The proponent of the Social Impact Theory was Bibb Latane in 1981 and the theory relies on three main parameters, the strength or the importance of the influencing group to the target audience, the immediacy or proximity of the influencing group to the target audience in terms of time and the number of people participating in influencing. Social media facilitates interaction between friends, colleagues and family. These are the people who have close relationships in real life and whose opinions matter to each other[42]. The impact of content shared is felt more between close relations, people with common goals and similar sentiments.

The availability of smartphones in mass production means that the people connected to social media are never more than a mobile device away. When any essential information is shared through social media, the response is always immediate and will grow with time. The number of people responding to certain pieces of information determines the impact of the content[43]. The greater the number of sources, the greater the impact. Any source that shares information on a national security event therefore garner significant response, regardless of its accuracy. Social media influence is a function of strength, immediacy and number of sources. The most significant impact of any news occurs between zero sources and one source. According to the Social Impact Theory, the more people who are aware of the information, the more deeply the audience involvement and the more impact on the potential of the audience providing a strong response[44].

[41] Ramona, Diana L, and Liana M Marcu. 2016. "Social Media Platforms As A Tool For Sharing Emotions. A Perspective Upon The National Security Agencies". *Management Dynamics In The Knowledge Economy* 4 (1): 141-152.

[42] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

[43] Ibid

[44] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

1.8.3 Resource Mobilization Theory

John D McCarthy and Mayer Zald are the originators and major proponents of Resource Mobilization Theory. The theory posits that resources such as time, money and organizational skills are prerequisites for the successful achievement of political and social goals. The availability of resources and the efficacy of actors in using them effectively are essential to positive outcomes of a social movement[45]. The Egyptian Revolution used social media as a vital resource to motivate citizens and mobilize protests. This revolution was an example of the potential of social media as an instrumental resource that contributes to the birth and sustainability of mass protests in crucial social and political issues[46]. The Egyptian government had invested in ensuring that the citizens had substantial access to social media by expanding information technology capabilities. Increasing internet access centers, availability of low-cost computers and free internet access were vital in expanding the scope of social media as a key tool for initiating a social movement[47].

Social media today is readily accessible to anyone with internet access and a smartphone. It is therefore easy to create and join a movement with the right content targeted at the right audience. Social media has an added element of speed and interactivity that was lacking in traditional media[48]. Citizens can follow events in their country, join social-networking groups and engage in discussions. The cyberspace created a sense of freedom for discussions on important issues on governance, national and international security[49]. Information is available to people globally, which might initiate a domino effect of movements across an entire region.

[45] Eltanawy, Nahed, and Julie B Weist. 2011. "Social Media In The Egyptian Revolution: Reconsidering Resource Mobilization Theory". *International Journal Of Communication* 5.
[46] Ibid
[47] Ibid
[48] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.
[49] Hirschkind, Charles. 2011. "From The Blogosphere To The Street: Social Media And Egyptian Revolution". *Oriente Moderno* 91 (1): doi:10.1163/22138617-09101007.

In the case of Egypt, the movements motivated the revolutions in Tunisia and across the Middle East.

The speed of social media provides a means for disseminating important safety information and how to seek help when in danger. Security agencies and activist groups can engage citizens on identification of any potential threats, contacting emergency services and potential locations that are safe[50]. The Tunisian protestors advised their counterparts in Egypt to protest at night for safety, to steer clear of suicide operations, and to effectively use the media to gain international support[51]. The messages and images shared on Twitter and Facebook strengthened the collective identity of Egyptians worldwide and showed the implications of virtual protests on democracy and national security.

1.9 Hypotheses

i. Social media has a negative impact on the implementation of national security policies in Africa, with specific reference to Kenya.

ii. Security agencies lack defined structures of monitoring the use of social media on issues of national security in Kenya.

iii. Social media has had varying effects on national and international security if the sharing of content is not regulated efficiently.

1.10 Research Methodology

This section addresses the research design, sample size, target population, data collection and data analysis.

[50] Eltanawy, Nahed, and Julie B Weist. 2011. "Social Media In The Egyptian Revolution: Reconsidering Resource Mobilization Theory". *International Journal Of Communication* 5.

[51] Hirschkind, Charles. 2011. "From The Blogosphere To The Street: Social Media And Egyptian Revolution". *Oriente Moderno* 91 (1): doi:10.1163/22138617-09101007.

1.10.1 Research Design

This study adopted a descriptive survey research design. The research objectives define the questions in the survey. The survey method is common in social sciences and seeks to understand the causative relationship between different variables; what, why, when and how. This method is simple to implement and is suited for the descriptive research intended for this study. Systematic analysis involves providing answers to a defined research question through collection and summarizing all empirical evidence fitting pre specified criteria. This method identifies the studies pertaining a certain topic with reproducible methodology and with a systematic presentation and synthesis of the findings[52].

1.10.2 Target Population

The secondary data was collected through an extensive keyword search for related articles on the internet. The selected articles discuss social media, and national security and provide quantitative studies on how the two aspects are connected. The primary data targeted social media influencers, social media users aged 18-28 years, with different exposure to social media, different gender and careers.

1.10.3 Sample Size

The researcher used a sample size of 30 respondents for collecting data. The respondents were selected from across Kenya. For the secondary data, the researcher collected and analyzed 50 articles, which were then eliminated gradually until the articles that fit the standards of the research were collected.

1.10.4 Data Collection Techniques

The research collected data through online surveys and polls. The questionnaire for the online survey were sent to social media users who confirmed their participation in the study. This

[52] Kothari, C. R. 2004. *Research Methodology: Methods And Techniques.*. 2nd ed. New Delhi: New Age International (P) Ltd.

ensured a higher response percentage. The online polls targeted general social media users on Twitter and Facebook.

1.10.5 Data Analysis and Interpretation

The data collected employed a deductive approach to establish the relationship between social media and national security. This approach involves using the research questions to group the data and then determining the similarities and differences. Narrative analysis was adopted to assess the collected data. The survey responses provided unique perspectives of respondents and formulate a coherent conclusion on the meaning of the data[53]. The research questions and conclusions guide the observations of the study and established the recommendations.

1.11 Chapter Outline

Chapter one: This chapter contains introduction, background of the study, problem statement, research questions, objectives of the study, and literature review. Other components include justification of study, research design and methodology.

Chapter two: This chapter highlights the nature of social media in Africa.

Chapter three: Discusses the impact of the use of social media in Africa and how it affects national security.

Chapter four: The chapter examines how social media has been used in Kenya and the impact it has had on national security.

Chapter five: This chapter presents the data collected for the study and its relation to the established hypothesis.

Chapter six: This chapter gives a brief summary, conclusions and recommendation.

[53] Kothari, C. R. 2004. *Research Methodology: Methods And Techniques.*. 2nd ed. New Delhi: New Age International (P) Ltd.

CHAPTER 2

NATURE OF SOCIAL MEDIA IN AFRICA

2.1 Introduction

Social media has become woven into the social and political discourse of Africa. Social networks facilitate online discussions and are forums for socio-cultural, scholarly, and economic debates. Since the Internet was first launched in the 1990s, the ICT sector in Africa has been growing steadily. The ICT revolution in Africa was delayed by several years due to the lack of infrastructure and technical knowledge to understand and operate in the digital sphere. Mobile phones are the primary devices used to access the internet. As smartphones evolved from a luxury to a necessity, the usage of social media in the continent has skyrocketed. In the past decade, social networking has grown worldwide. Forums such as Facebook, Twitter, Instagram, Reddit, and WhatsApp have revolutionized global communication, allowing people from all corners of the world to interact and exchange ideas

2.2 State of Social Media in Africa

When the social media boom began in the West, there were concerns over the possibility of Africa's success in the global media sphere. The main reasons for doubt were widespread poverty and unequal distribution of access to ICT tools. Surprisingly, the use of social media networks in Africa grew at a steady rate, mainly owing to a love of exploration of new technologies from the West. In 2009, South Africa had 1.1 million Facebook users, Morocco 369,000 and Nigeria 220,000[54]. Gradually social media use grew across the continent, to over 46% of the overall population gaining access to mobile services. The World Bank predicted that the growth of ICT had enabled the transformation of local businesses, drove entrepreneurship and promoted economic growth in Africa. Many more countries were

[54] "Social Media In Africa: A Double-Edged Sword For Security And Development". 2017. *Undp.Or*.

developing technological hubs to motivate the young population to join in the push for technological innovation. In Kenya, it led to the development of MPesa, a mobile money platform, in Cameroon the creation of ActivSpaces, in Senegal the establishment of BantaLabs and in Tanzania the development of Kinu. These technologies pioneered a shift in the reliance on mobile technologies, which ushered a majority of the population on to social media.

The growing use of social media sites, Facebook, Twitter and WhatsApp has increased citizens' awareness of political events in their borders as well as the continent in general. In Kenya, the use of Twitter has generated a renewed interest in the politics of misrepresentation of the country in international media. In Nigeria, users on Facebook and Twitter have engaged the mainstream media in reporting on sensitive issues, especially in critiquing the government. As Twitter and Facebook are easily accessible through a mobile phone, more people have found a platform to raise their voice and engage in international online discourse. Social media has been used as a tool to drive positive change and call the government to task on issues of poor governance and corruption. In South Africa, social media has been used as an effective tool for economic development. The high presence of citizens on Twitter and Facebook has forced the government to reconsider some of its economic principles[55].

Kenya is second to South Africa in terms of Twitter activity. Congregation of a diverse community of Kenyans on social media platforms has created a cesspool of hate, online abuse, and hate speech, especially around the election period. On the other hand, the middle class has found a platform to protest the socio-political situation in the country and express their opinions to lawmakers. Online activism has become the standard of political expression in Kenya. The #OccupyParliament demonstrations showcased how social media can mobilize and unite Kenyans against damaged political establishments. Social media has also become the watchdog

[55] Ephraim, Philip Effiom. 2013. "African Youths And The Dangers Of Social Networking: A Culture-Centered Approach To Using Social Media". *Ethics And Information Technology* 15 (4): 275-284. doi:10.1007/s10676-013-9333-2.

for the mass media on the reporting of major issues facing the country[56]. During the Westgate Mall attack, several media houses faced online backlash for lackluster reporting and ignorance of journalistic ethics when covering the crisis. Further, social media monitors the mainstream media on fake news and ensuring the accountability of the national government. The social media platforms allow Kenyans to freely express their opinions and call the government to task on various issues. As the appeal of mainstream media among young people gradually wanes, social media has become the staging point for key political debates and movements that amplify the feeling of citizens towards the government[57].

The Deputy President, William Ruto, has continually used his Twitter handle to address citizens and critique the mainstream media. In the past couple of years, the police department has used social media to alert the public on major arrests and advocating on public participation in solving crimes. This represents the growing role of social media in Kenyan society. Social media has an active audience, allowing users to provide real-time opinions and feelings towards different issues[58]. Recently, the COVID-19 global pandemic has shed light on the importance of social media. The Ministry of Health has regularly updated Kenyans on social media on the spread of the virus, the protective measures, and government initiatives to ensure the safety of all citizens. Social media users are active on the Kenya Power pages to express their grievances on the provision of services. As such, social media has become an important platform for Kenyan communication and socio-economic development.

2.3 Social Media Trends in Kenya

Over the years, Kenya has become the Silicon Savannah of East and Central Africa. Innovations such as mobile money like M-Pesa have shaped the ICT movement in the county

[56] Kaigwa, Mark W. 2013. "Kenya At 50: How Social Media Has Increased The Pace Of Change". *The Guardian*.
[57] Ndlela, Martin N., and Abraham Mulwo. 2017. "Social Media, Youth And Everyday Life In Kenya".
[58] Ibid

and have received global acclaim for the contribution to the digital world[59]. Kenya is among the leaders of Africa in internet access, totaling at 45.7 internet subscriptions by December 2018[60].. Kenya has not been left behind in this movement. According to the Communications Authority of Kenya (CAK), the rapid development of social networking technologies has resulted in the perpetual reconfiguration of ways in which Kenyans access and use social media platforms.

The 2017 elections were a significant coming of age point for social media use in the country. Political parties spent a lot of resources communicating to voters through various platforms, such as Twitter and Facebook, and increasing awareness of the new electronic voting system. Digital marketing teams were employed by various politicians to leverage the presence of young voters on social media to seek votes. Live commentary feeds, Facebook Live, videos, and photos were used by candidates to engage supporters across the nation. This was indicative of the youthful and tech-obsessed country that Kenya was evolving into. The popular movement, Kenyans on Twitter (KOT) are the perfect example of the growth of social media in the country. Twitter is a huge forum among young internet users in Kenya. It is used for sharing memes, addressing current issues in the country, and social commentary on issues affecting the youth. Facebook has grown into a key business platform. It is used to advertise businesses and reach out to clients. Instagram is a photo-sharing application that has revolutionized the events industry. Influencers have taken advantage of the appeal of active social life to promote events and products on their Instagram pages. YouTube hosts Video blogs widely referred as vlogs, educational content, and news channels. These social media platforms have become vital to the youth in Kenya who are growing more attached to the global digital space[61].

[59] Ndlela, Martin N., and Abraham Mulwo. 2017. "Social Media, Youth And Everyday Life In Kenya".
[60] "Social Media Consumption In Kenya: Trends And Practices". 2018. *SIME Lab*.
[61] Nyambuga, Charles. 2014. "The Influence Of Social Media On Youth Leisure In Rongo University".

A report published by SIME Lab USIU established that the most active social media users were aged between 26-35 years. Facebook was used by 34.6% of people in that demographic while Twitter was used by 39.3%. WhatsApp is popular for users aged 26-35 years and Instagram users are mostly aged between 21-25 years. YouTube is used among 26-35 years at 34.1%. Yahoo is mostly used by 26-35 years, at 43.0%. In terms of gender, men mainly use Yahoo, 61.9%, and Twitter, 67.0%. Women are more active on Snapchat at 47.5%, although the men are still slightly above them. Twitter is less popular among females. Facebook, YouTube, and WhatsApp are more popular among high school graduates. University graduates mostly use LinkedIn. People with college-level education prefer to use Yahoo, Google+, and email. Instagram (40.4%), WhatsApp (40.6%) and Snapchat (40.0%) are also common among this demographic. Twitter is commonly used by undergraduates. Generally, social media use is heavy among people with college-level education and least among primary school graduates. Facebook, WhatsApp, and Google platforms are majorly used in rural areas. Urban residents prefer LinkedIn, Instagram, Twitter, and Snapchat. The urban areas in Kenya have developed technological infrastructure which accommodates the use of demanding social media platforms. Telecommunications providers in rural areas offer complementary services that allow users to easily access WhatsApp, YouTube, and Facebook. Safaricom, the major telecommunications network in Kenya, provides several daily packages that allow free use of WhatsApp, and subsidized data bundles that allow rural residents to access Facebook and YouTube services[62].

The main uses of social media among Kenyans is entertainment and education. Job searches and social issues are also major areas of focus among users. Google+ is mostly used as an educational forum, YouTube as an entertainment forum, and WhatsApp as a family and social forum. LinkedIn is popular among job seekers and educators. WhatsApp and Facebook have

[62] "Social Media Consumption In Kenya: Trends And Practices". 2018. *SIME Lab*.

the highest daily usage rates. Twitter and LinkedIn have the highest weekly usage rate. The mobile phone is the most used device to access social media sites, Facebook, and WhatsApp. LinkedIn and Yahoo are mostly accessed from the laptop and desktop. The availability of public Wi-Fi and affordable cyber cafes influences social media use in the country. In urban centers, public Wi-Fi spots are frequented by students, job seekers, and individuals seeking cheap internet access options. Cyber Cafes are popularly used to access government services, such as e-citizen. The low-income urban areas and rural areas mainly use the services of a cybercafé. The advancement of home internet services from a provider such as Safaricom and Faiba has made Wi-Fi more affordable for urban residents. This has consequently increased the number of hours spent on the internet and access to social networks[63].

The major motivations for social media use are the acquisition of information, entertainment, personal identity, social interaction, and escape from realities. Facebook is the top forum for entertainment, information, and escape from social realities. WhatsApp is mainly used in the creation of personal identity and social interactions among families and friends. Online debates through social media are common among the 26-35 age group, followed by the 21-25 age group. Blogs are read by a majority of Kenyans, mainly for entertainment or education. There is a clear distinction between social media use habits for people in rural and urban areas and depending on the level of education. Social media users in urban areas are more likely to participate in online debates on social and political issues. College graduates use YouTube and Facebook for entertainment and acquiring information, LinkedIn, Instagram, and Twitter for building personal identity, and WhatsApp for escaping social realities[64].

[63] Wyche, Susan P., Sarita Yardi Schoenebeck, and Andrea Forte. 2013. "“Facebook Is A Luxury”: An Exploratory Study Of Social Media Use In Rural Kenya".

[64] "Social Media Consumption In Kenya: Trends And Practices". 2018. *SIME Lab*.

2.4 Regulating Social Media in Kenya

Kenya Vision 2030 acknowledges the role of ICT in the achievement of its development goals. Social media is key to the technological advancement of the country and the participation in the global digital space. Young people are leading the way in using social media in almost every aspect of their lives. However, the ICT institutions in Kenya have failed to provide guidelines on the safe use of social media and mental health preservation. Global studies have established that unfiltered and unmonitored social media use can have adverse effects on the mental health of young people. In Kenya, social media users are left on their own in use of devices and in understanding and managing their mental health. Impressionable and poorly educated people on social media platforms are vulnerable to abuse, misinformation, and manipulations by politicians and other users. Twitter has become an avenue for cyberbullying and hate speech. The relevant institutions have failed to regulate the negative uses of social media, promoting an environment of hate and online abuse. This is one of the biggest failures of the social media movement in Kenya. Policymakers have the responsibility to assess social media usage habits in the country and provide guidelines to mitigate the associated repercussions[65].

Social media can be used as a tool for empowering or manipulating people. In Kenya, as in the whole of the developing world, there is not enough statistical data on the implications of social media use on society. Policymakers in Kenya struggle to design and implement policies that enable users to harness the positive effects of social media. Numerous private agencies exist to highlight the basics of social media and internet use in Kenya. Applications such as M-Pesa have shown the innovation in the mobile technology sector among the youth is possible through the necessary support infrastructure. However, even as Kenya continues to establish itself as a continental technological hub, there are still areas surrounding social media use that are subject

[65] Nyambuga, Charles. 2014. "The Influence Of Social Media On Youth Leisure In Rongo University".

to more research and policy creation. Home internet services are expanding in the country. Therefore, the internet capacity in Kenya will soon outgrow the existing public policy. Uneven distribution of internet infrastructure in the country will create an unstable digital sphere, which will make it difficult to exploit the full potential of social networking. Consequently, public and private institutions have to collaborate in launching products that better regulate the social media environment in the country. The stakeholders in the ICT industry should know the trends of social media consumption among citizens to determine the implications on social, economic, and political institutions in the country. This provides a framework for better comprehension of the productivity of social media and the associated impact on political stability and national security[66].

2.5 Conclusion

This chapter established that social media has become interwoven into Kenya's society for a while. As internet connectivity increases in the nation, more people are gaining access to social media. This increases interaction on many social and political issues. The online community in Kenya has been very vocal on crucial issues of government and national security. Social media has provided interactive platforms to engage citizens and leaders on governance matters. It is evident that Twitter, Facebook and WhatsApp have become key sources of information for a significant number of citizens. Kenya, being a third world country, is just on the beginning of a technological revolution. According to the Uses and Gratifications Theory, the active audience in Kenya's social media is constantly seeking information that fulfills their curiosity needs. Therefore, people will actively search for government information on social media, rather than through mass media. The sharing of images, videos, and news articles on national security matters drives interactions and allows citizens to communicate and express their opinions. Twitter and Facebook, have the best user experiences, allowing comments and

[66] "Social Media Consumption In Kenya: Trends And Practices". 2018. *SIME Lab*.

likes on posts, and easy access to audiences. National security has become a key issue of discourse on social media platforms.

CHAPTER 3

IMPACT OF SOCIAL MEDIA TO NATIONAL SECURITY IN AFRICA

3.1 Introduction

Social media analytics has become an essential part of advertising and academic research. It has provided an insight into the perspective, thoughts, and communication of a wide range of audiences[67]. Mostly used to inform, educate, entertain, network and for basic purchases of goods and services online, the popularity of social media keeps on spreading all over the world. There have been mixed feelings about these networks and how they impact on different aspects of our lives There are compelling national security reasons to increase the analysis of the social media capabilities of national security agencies. In developing countries there are many inefficiencies in legal and technological structures that hinder the adoption of effective digital communication policies. The structures available to monitor and regulate social media use are key determinants of policies that affect national security. This chapter evaluates the advantages and disadvantages of social media when dealing with matters of national security. The section reviews the analytic approaches valuable for information operations, the ethical, legal, technological and policy implications of social media.

3.2 The Positive Impact of Social Media to National Security

3.2.1 Fast and Effective Means of Communication

Social media platforms allow users to share text, images, and videos as quickly as events occur. When threats to national security emerge, those affected can share information with emergency response services and other people willing to assist[68]. For example, during the Turkish protest movement of June 2013, protestors used social media to spread and receive information on the events in Istanbul. Traditional media such as television and radio are susceptible to bias towards

[67] A.Mishaal, Dareen, and Emad b Abu-Shana. 2015. "The Effect Of Using Social Media In Governments: Framework Of Communication Success". *The 7Th International Conference On Information Technology*. doi:10.15849/icit.2015.0069.

[68] Demidov, Oleg. 2012. "Social Networks In International And National Security". *Security Index: A Russian Journal On International Security* 18 (1): doi:10.1080/19934270.2012.634122.

and against a regime and therefore cannot be trusted to report impartially[69]. Television reports may skewer the extent of a security threat and spread misinformation.

3.2.2 Unlimited Sharing of Information

The social media platforms support the unlimited sharing of information, allowing users to share images of the actual situation of the ground and air their opinions without fear of being silenced. The diffusion of information using online social networks showcases the scope of sharing experiences on social media and the subsequent impact on national security[70]. The Turkish protests exhibited the massive potential of social media in spreading information on protests and how people were coping with the volatile security situation. Twitter was the main platform for sharing specific informational updates, providing information on how to seek medical assistance for injuries, initiating blood donation drives and warning on the locations to avoid. In Ukraine, during the 2014 protests, Facebook was used to provide logistical support to protestors and other people affected by the violence. The users coordinated travel and offered support to victims of violence[71]. The events in Turkey and Ukraine proved that social media is an effective tool for civilians facing security threats to coordinate rescue efforts and provide physical and emotional support. The emergency services in these instances have limited capacity to influence the outcome of national security, but users on social media have the experience to ask for financial or emotional support and solicit international attention on security challenges[72].

3.2.3 Networking Capability

Social media has enabled security agencies to engage with citizens in ways that were not possible before. The active audience of social media means that government agencies can

[69] Moreno, Megan A, and Rosalind Koff. 2015. "11. Media Theories And The Facebook Influence Model". *The Psychology Of Social Networking Vol.1*. doi:10.1515/9783110473780-013.
[70] Demidov, Oleg. 2012. "Social Networks In International And National Security". *Security Index: A Russian Journal On International Security*.
[71] Ibid
[72] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

manage the messages they want to deliver to people and respond in real-time to any public concerns[73]. Security agencies have created social media accounts and websites that allow users to share their ideas on national security, comment on existing policy and provide recommendations for security improvement. In Kenya, the Directorate of Criminal Investigations (DCI) has been active in engaging users on Twitter to report any incidents that threaten public safety. Twitter users have accepted this change and have participated in community policing to identify criminals and ensure justice is served.

3.2.4 Informative and Educative

Security organizations on social media are able to educate people on how to recognize potentially dangerous situations, the emergency response services, or how to act in case of a terrorist attack[74]. Further, social media influences policymakers in assessing how potential security policies will impact the public. Involving the public in policymaking boosts the image of national security agencies and promotes community policing for better public safety.

Social media can help inform on the aftereffects of weapons of mass destruction usage. Security and emergency response services will communicate to those affected through social media on how to handle the disturbance and panic that ensues[75]. Terrorist attacks often result in widespread panic and paranoia on the possibility of more dangerous attacks. Social media reaches those unaffected by the attacks and reassures them of the security measures in place to prevent more disasters. Social media platforms educate the public on how to remain vigilant, target areas to avoid and the actual implications of a significant attack on overall national

[73] A.Mishaal, Dareen, and Emad b Abu-Shana. 2015. "The Effect Of Using Social Media In Governments: Framework Of Communication Success". *The 7Th International Conference On Information Technology*. doi:10.15849/icit.2015.0069.

[74] Marcellino, William, Meagan L Smith, Christopher Paul, and Lauren Skrabala. 2020. "Monitoring Social Media: Lessons For Future Department Of Defense Social Media Analysis In Support Of Information Operations". *Rand.Org*..

[75] Chen, Alan K. 2017. "Free Speech And The Confluence Of National Security And Internet Exceptionalism". *Fordham Law Review* 86 (2)

security[76]. The public needs reassurance that the weapons used by terrorists will not have unmanageable consequences and that security agencies are in control of the situation.

3.2.5 Monitoring and Intelligence Gathering

Social media analytics can provide vital intelligence on adversaries, supporting communities on each side of a conflict and other key populations. The analytic technologies provide location data, social media use behavior and associated individuals or groups. Social media informs efforts to target messages to particular audiences or influence the perceptions and behaviors of a group[77]. Monitoring social media platforms ensures that security agencies identify and intercept any attempted communications between extremist groups. Supporters of radical ideologies on social media and inciters of violence can be geolocated through the content shared online. Security agencies can, therefore, track the instigators of violent uprisings that weaken national security. These institutions can collaborate with community groups and individuals on social media to identify extremists who threaten public safety. National security institutions need to work closely with the public to eliminate any threats to domestic security[78]. Social media offers the best interactive platforms to share and analyze content that will define the national security strategies in a country. Citizens are given an opportunity to police their communities and provide any essential information to security agencies that might be used to improve national security.

3.2.6 Response in Crisis Situations

Crowd sourcing and social media monitoring have a critical role in various humanitarian efforts and other civil security operations. Groups and individuals provide real-time updates necessary

[76] Moreno, Megan A, and Rosalind Koff. 2015. "11. Media Theories And The Facebook Influence Model". *The Psychology Of Social Networking Vol.1*. doi:10.1515/9783110473780-013.

[77] Marcellino, William, Meagan L Smith, Christopher Paul, and Lauren Skrabala. 2020. "Monitoring Social Media: Lessons For Future Department Of Defense Social Media Analysis In Support Of Information Operations". *Rand.Org*.

[78] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

for timely and effective response[79]. Institutions such as the Red Cross and Red Crescent can use social media to coordinate means to reach victims of civil war in very insecure areas. Volunteers can be mobilized through social media to assist in humanitarian efforts. Financial support from social media users boosts the operations of aid groups in war-torn regions. Social media can further help to rally civil forces to serve in fighting against any domestic and international insurgents. The deployment of security agencies in fighting zones can be complemented by joint civil efforts to mitigate the effects of national security threats[80]. Social media analysis supports the prevention efforts of security agencies by reaching out to civilians interested in restoring peace and order in their communities.

3.2.7 Builds Public Trust

Social media is key increasing public trust in governing institutions. Active engagement in these platforms assures the public that the government is transparent and values their contribution. Security agencies using social media to lift the curtain on how security operations are conducted enhances the belief that they are prepared to protect the country[81]. The agencies that associate with users most on social media generate more authenticity and can leverage cooperation in many areas of society. Social media is low stakes and allows instant feedback. Security agencies can test a message with the public to determine their effectiveness and gauge the response of the audience. The strengthened connection with government agencies creates cohesion and boosts collaboration in times of heightened tensions in the country. Security organizations will test different types of messages to see what resonates best with the public[82]. The agencies can rely on social media users to volunteer with information critical to national security. The public, on the other hand, is able to show their trust towards the security agencies.

[79] Ibid

[80] Ibid

[81] Moreno, Megan A, and Rosalind Koff. 2015. "11. Media Theories And The Facebook Influence Model". *The Psychology Of Social Networking Vol.1*. doi:10.1515/9783110473780-013.

[82] Marcellino, William, Meagan L Smith, Christopher Paul, and Lauren Skrabala. 2020. "Monitoring Social Media: Lessons For Future Department Of Defense Social Media Analysis In Support Of Information Operations". *Rand.Org*. https://www.rand.org/pubs/research_reports/RR1742.html.

Hashtags and online polls inform the public opinion on security matters and enlighten on the areas that need streamlining and new policies to adopt.

3.2.8 Promotes Freedom of Expression and Democracy

The emergence of new media has rejuvenated civil society and empowerment movements. The cyberspace is seen as a safe place for citizens to express their political opinions. The promise of freedom of expression means that individuals with different viewpoints can reach out to other similar minded people[83]. In the events of national events such as general elections or international conflicts, social media platforms are filled with people airing their opinions on government and the political process. Government critics and activists have adopted the cyberspace as the primary medium for criticizing the government[84]. Bloggers and social media influencers have more impact on social opinions today than ever before. However, the freedom of expression in social media has been characterized by the marginalization of certain groups of people and individuals through economic and political designs[85]. Suppressing certain voices has become commonplace in the recent past

3.3 The negative impact of social media on national security

3.3.1 Recruitment into Criminal Groups

Social media abuse is a significant challenge to national security. Terrorist groups such as Boko Haram have used social media platforms such as YouTube to relay secret messages to their followers. Terrorist organizations have a sophisticated knowledge of social networks and can create chat rooms, dedicated servers, and websites to communicate with the public[86]. Boko Haram has established social networking tools as propaganda machines to boost the

[83] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

[84] Gunawan, Budi, and Barito M Ratmono. 2020. "Social Media, Cyberhoaxes And National Security: Threats And Protection In Indonesian Cyberspace". *International Journal Of Network Security* 22 (1).

[85] Ibid

[86] Meloy, J. Reid, Alasdair M. Goodwill, M. J. Meloy, Gwyn Amat, Maria Martinez, and Melinda Morgan. 2019. "Some TRAP-18 Indicators Discriminate Between Terrorist Attackers And Other Subjects Of National Security Concern.". *Journal Of Threat Assessment And Management* 6 (2): doi:10.1037/tam0000119.

recruitment, organization and fund-raising schemes by targeting impressionable and sympathetic users on online platforms. The Taliban and Al Qaeda have Facebook pages and YouTube channels used to reach out to Western-based sympathizers.

3.3.2 Main Communication Platform for Terror Groups

These networks also act as a means of correspondence between the organized networks of the terrorist organization. In Pakistan, the local Taliban have been contacting friendly citizens through social media and instructing them on what they need to do and how to do it. Governments across the world have increased their efforts to track the activities of terrorist groups on social media. However, these groups have mustered sophisticated knowledge on the operations of social network communications, managing to evade the counter-intelligence systems created by world governments[87]. International terrorists communicate with each other on how to organize their attacks and escape security agencies. They have developed specific codes that can be used in public social media platforms without raising any suspicion. Further, they advise their followers on effective ways of designing weapons and evade arrest at the borders. Terrorist groups are recruiting technologically savvy individuals who can help them build communication platforms that cannot be detected by various states' security computer technology.

3.3.3 Propaganda Channel

Social media platforms have evolved into a haven for extremists to groom vulnerable people. They create posts to generate sympathy from users and consequently solicit financial support for their operations. They also look to international public opinion to legitimize their actions. Groups such as ISIS and the Taliban rely on their sentiments against Western regimes to gain members from African forces. Increased use of social media in the modern world has resulted in a loneliness epidemic and anxiety among users[88]. These young impressionable individuals

[87] Ibid

[88] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

are more vulnerable to radicalization and make up a significant portion of the fighters in the extremist organizations. The internet content these groups created caters to the fears of young people about government control, surveillance and harmful policies. Communication through social media is generally subtle and genuine, which evades detection by security agencies[89]. The use of social media as a key recruiting tool for terrorist organizations underlines the importance of better monitoring of communications from extremist groups.

3.3.4 Cyberbullying

Social media has facilitated the rise in the proportion of dreadful acts such as identity theft and cyberbullying. People using social media sites update their information regularly which leads to the loss of privacy[90]. The users, therefore, become easy targets for hackers, who can manipulate their online presence to spread their radical ideologies and propaganda undermining the government.

3.3.5 Creation and Sharing of Manipulated Content

The creation of dummy social media profiles of celebrities and political figures can contribute to disinformation. The sites can be used to distribute false and junk information or malware that might hinder national security agencies' operations. Social phishing can be used to target specific high-ranking individuals in security organizations[91]. The attacker seeks to obtain sensitive information from a target user through fake data and websites. Unmonitored use of internet use in security agencies can make the organization vulnerable to phishing scams and pave the way for hackers to steal information. Links shared through social media can track the locations and other metadata for users which can be manipulated for nefarious reasons. Cyber attackers can access important government websites and hold them hostage for ransom.

[89] Ibid

[90] Zhang, Zhiyong, and Brij B. Gupta. 2018. "Social Media Security And Trustworthiness: Overview And New Direction". *Future Generation Computer Systems* 86: doi:10.1016/j.future.2016.10.007.

[91] Ibid

Many societies across the world today rely on digitized systems for services such as air, and road traffic control, coordination of medical services, banking and energy, and government and national security[92]. Cyberterrorism has risen as a significant threat to national security. Criminal organizations hold user data hostage to demand ransoms from social media companies and governments. Information shared between friends and family can be used for blackmail and harassment. When senior officials in security agencies post sensitive information on public platforms, they can jeopardize national security. Hackers can obtain personal information about people using social media platforms by catfishing and blackmailing their close friends[93]. National security information held hostage for ransom by hackers highlights the shortcomings of computerized systems of government. Many third world countries lack the technologies to secure sensitive information and monitor social media platforms. This creates vulnerabilities in online operations through social media and other websites that threaten national and international security.

3.3.6 Cyber Espionage

Cyber espionage incorporates the theft of confidential information from social media without the permission of the owner. Countries at war can develop hacking technologies and malicious software intended to steal confidential information[94]. Cyberwarfare refers to the politically motivated internet-based attacks on information and information systems using social media. These attacks target vulnerable government websites, seeking to cripple communication and financial stability. The purpose of cyber warfare is to cause improper functioning of another

[92] Couldry, Nick. 2012. *Media, Society, World: Social Theory And Digital Media Practice*. Cambridge: Polity.

[93] Gunawan, Budi, and Barito M Ratmono. 2020. "Social Media, Cyberhoaxes And National Security: Threats And Protection In Indonesian Cyberspace". *International Journal Of Network Security* 22 (1).

[94] Parlakkılıç, Alaattin. 2018. "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach". *International Journal Of Information Security Science* 7 (4):

country by targeting the cyber defense systems[95]. Future wars will be fought by individuals sitting in a room rather than going to the battlefront.

The rapid advancement in cyber technologies and social media algorithms creates more opportunities for malicious individuals to attack entire countries[96]. This threat to national security can have unprecedented effects on countries that lack the technologies and facilities to suppress and respond[97]. The increasing use of social media in third world countries increases the risk of such attacks in the future. Moving into a purely digital future creates several hurdles for the development and implementation of national security policies in third world countries.

3.3.7 Political Escapism, Fake News Phenomena and Character Assassination

In the early stages of the internet, it was a forum for free discussion on key social issues. The internet has evolved into a global communication platform for governments, corporations and terror organizations. These entities create and disseminate information to fit specific agendas, either for good or bad. Those in power use their position to pass laws that prohibit critical speech against government agencies. Corporate-owned mainstream media further enhances the marginalization of these groups resulting in undermining democracies and government operations[98]. This has seen an increase in the instances of fake news on online social networks.

Fake news is divided into four categories: disinformation, misinformation, entertainment and falsehoods for financial gain. Certain groups on social media spread falsehoods and rumors intended to undermine national security[99]. State-sponsored disinformation campaigns create certain narratives meant to spread propaganda and conceal the failures to uphold national

[95] Parlakkılıç, Alaattin. 2018. "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach". *International Journal Of Information Security Science* 7 (4).

[96] Ibid

[97] Ibid

[98] A.Mishaal, Dareen, and Emad b Abu-Shana. 2015. "The Effect Of Using Social Media In Governments: Framework Of Communication Success". *The 7Th International Conference On Information Technology*. doi:10.15849/icit.2015.0069.

[99] Belova, Gabriela, and Gergana Georgieva. 2018. "Fake News As A Threat To National Security". *International Conference KNOWLEDGE-BASED ORGANIZATION* 24 (1): doi:10.1515/kbo-2018-0002.

security. Misinformation involves rumors propagated as part of a political agenda by a political group to offer a differing interpretation of facts based on ideological bias. Additionally, entertainment sources use parody, satire and humorous pieces to critic government and spread certain biased ideologies.

Another category of falsehoods involves widespread fear-mongering in the wake of a terror attack[100]. Social media is used to circulate fake statistics and stories on the aftermath of an attack. For instance, after the 2017 Manchester terrorist attack, there was the widespread circulation of fake news, hoaxes of missing individuals, and misinformed trolls. This category of fake news harms public order and safety.

Social media has led to the rise of online vigilantism. Social media users and activists use the online platforms to track down suspected criminals, release their personal information online and harass them. This is often done with malicious intent and limited information on the supposed crime. Easy access to information has motivated social media users to contribute to national security by aiding in the identification of criminal elements[101]. While this is a good thing, viral vigilantism has led to the arrests of innocent people. The Boston Marathon bombing of 2013 was the first example of the negative implications of online vigilantism. Through images shared online, well-meaning users crowdsource information to establish an identity of the perpetrator on online forums. Reddit was the staging ground for the identification of the suspected bomber. The mass media agencies abetted the development of the false narrative leading to the identification of an innocent student[102].

Viral online vigilantism lacks repercussions to those who made the accusations and the platform hosting the users making the accusations. The protection of user privacy and

[100] Ibid

[101] Chen, Alan K. 2017. "Free Speech And The Confluence Of National Security And Internet Exceptionalism". *Fordham Law Review* 86 (2).

[102] Belova, Gabriela, and Gergana Georgieva. 2018. "Fake News As A Threat To National Security". *International Conference KNOWLEDGE-BASED ORGANIZATION* 24 (1): doi:10.1515/kbo-2018-0002.

anonymity of social media means that individuals can make unfounded claims, mobilize support and initiate a response from security agencies. This type of vigilantism may be well-intended but is rooted in the ideals of mob justice. There are no social media police to regulate how people use social media. Therefore, in the case of terrorist attacks, the unfiltered flow of information will have unpredictable effects on the protection of national security.

Fake news through social media is used as a vehicle for increasing political support during the elections period. Political actors and supports spread propaganda and fake stories to tarnish the image of their opponents[103]. Facebook and Twitter are used to carefully plan and systematically influence public perception of the individuals deemed as obstacles. During the elections period, these platforms host opinions by certain leaders while censoring their competitors. In the 2016 US election, Facebook was notorious for running campaign ads supporting Donald Trump while at the same time hosting negative coverage of his competitor, Hilary Clinton. This turns people against their leaders and may result in widespread violence. In January 2012, the Federal Government of Nigeria under the leadership of the People's Democratic Party was hit by a fake news campaign by the opposition party. The opposition managed to convince the public by claiming that the fuel subsidy which the government promised to remove did not exist. They stated that it was an attempt by the PDP government to loot the national treasury. This led to a massive revolt, demonstrations and an economic crisis that affected the nation for several days. The opposition won the subsequent elections and increased the prices of petroleum products. This was a successful fake news campaign that resulted in the loss of lives and property and slander. The fabricated stories decreased public trust in the media. Unscrupulous politicians propagate half-truths which are detrimental to the welfare of the people and undermines national harmony[104]. The extent of fake news in mainstream and social media highlights a huge

[103] Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media And Fake News In The 2016 Election". *Journal Of Economic Perspectives* 31 (2): doi:10.1257/jep.31.2.211.

[104] Belova, Gabriela, and Gergana Georgieva. 2018. "Fake News As A Threat To National Security". *International Conference KNOWLEDGE-BASED ORGANIZATION* 24 (1): doi:10.1515/kbo-2018-0002.

challenge for security agencies in controlling narratives and the creation of content detrimental to national welfare. Misleading content undermines ethical journalism, establishes a precedent for false reporting and compromises the implementation of national security policy.

Deep fakes are the next frontier in altering audio and video recordings on the internet. A deep fake is synthetic media which replaces an existing video or image of a person with another's likeness. Deep fake technology will introduce significant change in how we differentiate what is real from what is fake[105]. It enables the insertion of people's faces and voices into audio and video saying and doing things they never said and did. The videos and images created are incredibly realistic and to the common social media user, they are indistinguishable from real events. The breakthroughs in deep fake technology create a new challenge in the detection of fake content circulating on social media. Deep fake videos and images can target politicians, celebrities and common users of social media. The technology has not become mainstream yet so its use is limited. However, the implications for social media use cannot be underestimated. In the era of fake news, the ability to falsify video and audio 'evidence' calls for more vigilance in the use of social media.

Deep fake videos can be used to sabotage corporate CEO's, government officials and companies. Social media algorithms allow the sharing of content on a wide scale within a short period. When a deep fake appears on social media, users often share content without verifying its authenticity and the results are devastating. In terms of national security, faking videos and images of attack victims or politician speeches can be detrimental to national safety. Within a short time, the consequences of a terror attack can be manipulated to fit the narrative of certain

[105] Chesney, Robert, and Danielle K Citron. 2019. "21St Century-Style Truth Decay: Deep Fakes And The Challenge For Privacy, Free Expression, And National Security". *Maryland Law Review* 78 (4).

state and non-state actors[106]. If terrorist groups adopt this technology, it is impossible to predict how they will use it to undermine government and security agencies.

Deep fakes subvert our sense of reality. As more people become aware of the scope of deep fake technology, wrongdoers will find it easier to cast doubt on the authenticity of real recordings of their mischief[107]. Terrorist organizations may impede governments by jeopardizing the truth of government reports. They might claim that videos and images of their attack were faked by security agencies.

The public is not sensitive to the issue of deep fake content therefore it is easier to manipulate their perspective on the occurrence of certain events[108]. By the time a deep fake is debunked, the damage would be irreversible. Both state and non-state actors could avoid accountability for their actions by claiming genuine audio and video content was impaired by deep fake technology[109]. The disinformation that results from deep fakes is very dangerous as social media users respond better to videos and images. The images and videos shared through these platforms are unverifiable to the users and therefore their impact cannot be undermined. Deep fake technology is still changing and adapting to social networking and internet advancements. The technology undermines the possibility of having conversations about a shared reality and exacerbates the fake news phenomena that disrupt democracy.

Social media companies have a notable influence on domestic and international politics. Facebook, the largest social media company, has come under fire in the past few years because of its involvement in politics[110]. The US 2016 election and the Brexit campaign were heavily influenced by Facebook's involvement in creating and distributing content[111]. These companies

[106] Chesney, Robert, and Danielle K Citron. 2019. "21St Century-Style Truth Decay: Deep Fakes And The Challenge For Privacy, Free Expression, And National Security". *Maryland Law Review* 78 (4).
[107] Ibid
[108] Ibid
[109] Ibid
[110] Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media And Fake News In The 2016 Election". *Journal Of Economic Perspectives* 31 (2): doi:10.1257/jep.31.2.211.
[111] Ibid

hold significant user data that can be analyzed and manipulated to favor certain political candidates. Location data, political affiliation, purchasing habits and hobbies of an individual can be determined by social media companies. This information can be sold to politicians to send targeted messages to favor certain policies or individuals in the election period[112].

Facebook is a global company that cannot be regulated by any single policy. The integration of social media in campaign politics has shed light on the destructive impact of social engineering. Social media analytics determines the content people interact with most and tailors it to fit certain narratives[113]. The lack of controls for social media companies means users are at the mercy of individuals using their power to influence social politics. The average social media user is bombarded with messages favoring specific politicians and negative advertisements on political adversaries. This increases polarization in national politics, especially in Western nations.

3.3.8 Data Mining

This is the process of examining any patterns or anomalies within a large data set as a means of predicting outcomes. Data mining from social media creates psychological profiles for users of various social media platforms. Loss of privacy due to lack of awareness facilitates the unlawful application of user data to advocate for certain government policies[114]. If a politician wants to support a national security policy, they pay a social media company to create a campaign focused on users in their platform. This creates a tactical advantage for policymakers, who appeal to the fears and expectations of the public to get their laws approved. Security agencies can also use social media user data as a surveillance tool to target suspected criminals and terrorists[115].

[112] Chen, Alan K. 2017. "Free Speech And The Confluence Of National Security And Internet Exceptionalism". *Fordham Law Review* 86 (2).
[113] Ibid
[114] Ibid
[115] Gunawan, Budi, and Barito M Ratmono. 2020. "Social Media, Cyberhoaxes And National Security: Threats And Protection In Indonesian Cyberspace". *International Journal Of Network Security* 22 (1).

This may be well-intentioned, but the fallout from unchecked surveillance has a negative impact on public trust. The public seeks to feel safe when using social media, with the assurance that their data will not be used by the government for unauthorized purposes[116]. Social media networks accommodate large amounts of data with personal information on users. When unchecked, this data can be used by totalitarian governments to modify opinions, intimidate opponents and transform national security policy in favor of a few individuals.

3.4 Conclusion

Social media has many advantages to national security. Online platforms foster communication, unlimited sharing of information, allow education, provide sources of intelligence for national security agencies, and acts as a platform for response in crisis situations. Social media also builds public trust by promoting freedom of expression and democracy. On the other hand, social media is a hotbed of a variety of crimes. Criminal groups use social media as recruitment grounds, especially for communication among terror groups. Non state actors can also use social media to spread propaganda and misinformation to undermine the government. Cyberbullying and hate speech is also rife in Kenyan social media. This chapter reveals that the disadvantages of social media outweigh the advantages to national security. For third world countries, criminal elements take advantage of poor network infrastructures to set up and operate criminal enterprises without detection by security agencies. This chapter proves that social media has varying effects on national and international security of sharing online content is not regulated efficiently. Uses and Gratifications Theory states that people will actively consume media that fulfils their curiosity and reinforces their worldview. When people share information with relatives, peers and colleagues, they are likely to be influenced towards certain opinions and viewpoints on matters of government. It is clear that misinformation and fake news is propagated through the principles of Katz and Blumler's

[116] Zhang, Zhiyong, and Brij B. Gupta. 2018. "Social Media Security And Trustworthiness: Overview And New Direction". *Future Generation Computer Systems* 86: doi:10.1016/j.future.2016.10.007.

theory. Social media users will seek information that justifies their worldview, without questioning the origin of the information. This has contributed to the persistence of fake news and misinformation forums on social media platforms. Overall, the chapter reveals the increasing threats of social media to national security in Kenya and the third world in general.

CHAPTER FOUR

THE USE OF SOCIAL MEDIA IN KENYA AND ITS IMPACT ON NATIONAL SECURITY

4.1 The Application of Social Media by Security Agencies

The use of social media in Africa has increased in the past few years. Twitter, Facebook, and other news apps have become the core sources of information, especially for the younger generation. Social media use has changed the way citizens interact with political events and altered the perceptions of Africa in the international forum. In Kenya, Twitter has become the main platform for citizens to challenge the misrepresentation by the international media in reporting violence and election campaigns[117]. The reach of Twitter and the impact of the hashtag trends means that sensitive issues get to a wider audience within and outside the continent. On the other hand, social media has been exploited by criminal elements in the continent to promote activities such as sexual exploitation of children, payment fraud, cybercrime, and terrorist radicalization. Consequently, social media has increased opportunities for both state and non-state actors to advocate for both good and harmful security policies. The volatility of African politics means that social media users are prone to misinformation and radicalization to violent political and religious movements[118]. In Kenya, social media has played a role in the development of security policy, especially after Al-Shabaab launched its campaign against the nation. In the past decade, we have witnessed both the good and bad of social media when reporting on terror attacks, responding to security operations and mobilizing citizens against terrorists. It is important to evaluate the repercussions of social media on domestic security through an in-depth review of the various social media movements that have shaped national security policy in Kenya today.

[117] Cox, Kate, William Marcellino, Jacopo Bellasio, Antonia Ward, Katerina Galai, Sofia Meranto, and Giacomo Persi Paoli. 2020. "Social Media in Africa: A Double-Edged Sword for Security and Development". *Africa.Undp.Org*.

[118] Cox, Marcellino, Bellasio, Ward, Galai, Meranto, and Persi Paoli. 2020. "Social Media in Africa: A Double-Edged Sword for Security and Development". *Africa.Undp.Org*.

4.2 The Application of Social Media in Policy Matters in Kenya

According to Gianni De Genarro, the Director-General of the Security Intelligence Department in Italy, "the higher the informatization level of a certain country's population, the more widespread the use of IT devices by its citizens, companies and public agencies, the more frequent the use of web for information sharing, acquiring or transfer, the higher that state's vulnerability is"[119]. Kenya has one of the highest social media populations in Africa. The Communications Authority of Kenya stated in 2019 that mobile phone penetration had surpassed 100%. The number of internet subscriptions in 2019 stood at 45.7 million. 88.5% of social media users are on Facebook, 27.9% on Twitter, 88.6% on WhatsApp, 39% on Instagram and 51.2% on YouTube[120]. Most active social media users are aged between 26-35 years. Many Kenyans use social media to acquire information, followed by entertainment, social interactions, and personal identity as well as a form of escapism. The threats for national security and unfavourable consequences for the country's strategic interests can arise from social media use. Information shared through these mediums can be used by competitors and state apparatus to influence security decisions. The use of social media in Kenya is growing annually, as internet prices continue to drop. More people are using social media as their primary source of information and news updates. Security agencies on social media have been prompted to adopt strategic communication techniques to relate to the active audience.

The government of Kenya uses social media to communicate with citizens on issues affecting them to generate support before making any major decisions. After the 2013 General Election, elected officials opened social media accounts on Facebook and Twitter to engage with Kenyans. The official Twitter and Facebook accounts of the President and Deputy President always ask for the views and support of Kenyans before signing major bills into law. President Kenyatta used social media to inquire about the opinions of Kenyans on the terror bill. During

[119] Montagnese, Capt. CC Alfonso. 2012. "Impact of Social Media on National Security". *Difesa.It*..

[120] "Social Media Stats Kenya | Statcounter Global Stats". 2020. *Statcounter Global Stats*.

Operation Linda-Nchi, the KDF regularly updated citizens on the operation progress through the official Twitter handles. In the Judiciary, the Chief Justice and President of the Supreme Court communicate to the country on the happenings in the courts through official social media accounts. The adoption of social media as a subset of official communication channels has allowed the government to motivate the participation of the public in major political and social issues[121]. Social media opinions hold weight in determining the outcome of certain bills and contribute to the discourse on how security policies affect the common Kenyan.

Social media in Kenya is used as a tool for generating mass support. The government uses social media platforms to educate citizens on essential policies that affect their daily lives. Interaction on social media forums enables the marginalized groups to participate in discussions and present their point of view[122]. This improves the political position of marginalized groups, women, minorities, and youth. These groups advocate for increased government funding and better socio-economic opportunities. The Kenyan government has been criticized for long due to the marginalization of certain communities and members of society from the policymaking process. For example, when discussing issues of the terrorist threat in the coastal region, those affected most are not provided with adequate opportunities to present their perspectives and opinions on policy. Further, the marginalization of communities in the northern and north-eastern regions of Kenya leaves them prone to terror attacks and tribal violence. Poor governance in the marginalized North-Eastern region has increased the level of insecurity. Annual attacks in the north-eastern region close to the Somalia border highlight the failures of the government in ensuring the safety of all citizens[123]. Social

[121] Montagnese, Capt. CC Alfonso. 2012. "Impact of Social Media on National Security". *Difesa.It*.
[122] Kimotho, Stephen Gichuhi, and Carolyne Nyaboe Nyarang'o. 2019. "Role of Social Media in Terrorism Crisis Communication". *International Journal of Information Systems for Crisis Response and Management* 11 (1): doi:10.4018/ijiscram.2019010104.
[123] Stephen, and Carolyne. 2019. "Role of Social Media in Terrorism Crisis Communication".

media is an effective tool for policing the government and demanding for accountability for the perpetual terror threat in north-eastern Kenya.

Social media is a good community policing tool. The “tweeting chief” Chief Kariuki hit the headlines due to his use of Twitter to combat crime in Lanet, Nakuru County. The chief collaborated with other local leaders in the area to assist stop crime in their jurisdictions. This move supported the 'Nyumba Kumi' initiative meant to boost security in small communities[124]. It involved a collection of ten households in a neighbourhood to form a cluster of security administration. This cluster should be politically neutral but tackles an array of security issues such as gender-based violence and crime. The level of trust generated between the households and security providers would help curb weapons proliferation and inter-ethnic tensions fuelled by political differences. Government administrators, such as chiefs and police officers work closely with the head of each cluster to tailor effective strategies to handle crime. Nyumba Kumi members communicate through Facebook and WhatsApp. These platforms are effective in strengthening the cohesion between households and sharing of content important to enforcing security in a neighbourhood. The "tweeting chief" captured Twitter's ability to reach across the nation to seek support for security initiatives in his jurisdiction. The Nyumba Kumi security initiative has not reached the expected heights. There is still distrust between people from different ethnic groups, religions and political affiliations. Social media can help bridge the collaboration gap between these people by introducing them to the benefits of the initiative, national security challenges and assist the government in achieving the domestic security objectives[125].

The polarization of Kenyan politics, especially around general elections, presents a huge challenge to security officials. In 2008, the country was plunged into deadly violence following

[124] Koigi, Bob. 2020. "Kenya’s Tweeting Chief Fights Crime and Improves Community Lives | Fairplanet". *Fair Planet*.

[125] Koigi, Bob. 2020. "Kenya’s Tweeting Chief Fights Crime and Improves Community Lives

a hugely controversial election. The extent of the inter-ethnic clashes in various regions of Kenya proved that political differences are a danger to domestic security. Mass media platforms, TV, radio and print media, were used to spread propaganda and incite violence across the country[126]. In the peak of social media, such clashes would be much more devastating. Social media has allowed the quick spread of misinformation and public bashing. Unrestricted access to information on social media can result in sharing personal information of an individual without their consent. Criminals can identify people based on their social media profile and content shared leading to actual violence or damaging their reputation. Social media users are capable of uncovering a lot of information on a person based on their social media activity. In times of heightened political tensions, the data can be applied to segregate individuals and promote mob action.

Impersonation has become a big ethical issue for social media users. The presence of prominent politicians on social media has prompted the rise of faux social media accounts posting misleading information. Most social media users are young and gullible and therefore will believe any content shared by politicians or celebrity accounts. In Kenya, various accounts are impersonating the President, Deputy President, and other prominent politicians. Most of these have been identified and taken down, but some remain active. In the event one of these fake accounts discusses sensitive security issue, the unprecedented response of users can affect public safety. In modern media, the opinions of celebrities and public figures hold significant weight in determining public perception on certain issues. Therefore, when the likeness of celebrities is abused on social media, it has the potential to influence major political and social decisions in the country[127]. To solve this issue, government and security officials should

[126] Makinen, Maarit, and Mary Wangu Kuira. 2008. "Social Media and Post-Election Crisis in Kenya". *Information & Communication Technology - Africa* 13.
[127] Stephen and Carolyne. 2019. "Role of Social Media in Terrorism Crisis Communication".

promote positive content in their social media platforms and steer clear of polarizing issues that negatively impact public safety.

Cybercrime has emerged as a huge problem for social media users in recent years. Social media platforms such as Instagram and Facebook allow users to post personal information such as birthdates, addresses, and family members. This information compiles a single, comprehensive portrait of the social media user. Cybercriminals can exploit this feature of social media for identity fraud, online harassment and malicious hacking of online accounts. Phishing scams and social engineering techniques are used by hackers to solicit social media user's confidential information to commit crimes or send them to third parties[128]. Social media companies require personal details to allow a person to open an account. Most of this information remains in the public forum and the platforms lack privacy controls. The personal information can be sold to gaming companies, foreign governments, and malicious businesses. Cybercriminals can also create fake social media profiles to target a specific demographic of users. User data on social media can be manipulated by politicians to shape public opinion on security matters[129]. Cambridge Analytica was a company that used Facebook user data to compile personality information that would be sold to politicians for their election campaigns[130]. This company was accused of collecting information on social media users to facilitate the campaigns in the 2013 general election. The involvement of social media companies on political matters means that people can be manipulated and hypnotized to accept certain leaders and policies. The appeal of social media means that many young people are creating accounts and engaging with the national and international public[131]. When social media companies begin shaping the opinions on young users, it can have long-lasting effects on governance and national security. Social

[128] Lee, Newton. 2015. *Counterterrorism and Cybersecurity: Total Information Awareness*. 2nd ed. Cham: Springer.

[129] Newton. 2015. *Counterterrorism and Cybersecurity: Total Information Awareness*.

[130] Confessore, Nicholas. 2018. "Cambridge Analytica And Facebook: The Scandal And The Fallout So Far". *Nytimes.Com*.

[131] Ibid

media can destroy the traditional fabric of society, resulting in political systems where opinions are created and propagated online, and individuals are stripped of their autonomy.

4.3 Kenya's National Security and Social Media

The external threat from Somalia, Al-Shabaab, and the pirates have defined the biggest challenges to national security in Kenya. The internal threats include cattle rusting, urban crime, poaching, communal violence, and criminal gangs. The menace of terrorism and criminal gangs has driven the nation to take a more active role in regional security[132]. Military operations such as Operation Linda Nchi in Somalia showcased the dedication of Kenya to reinforce domestic security by promoting stability and good governance in the neighbouring nation. The porous borders with Somalia and parts of Ethiopia have seen a growth in communal violence and entry of terrorists into the country. The politicization of sensitive issues facing the citizens means that there is still no solution to urban crime, cattle rustling and communal violence in Kenya. Politicians and policymakers have not established any frameworks for public participation in Kenyan politics. However, with government involvement in social media, there is hope that citizens will be more informed and engaged in national security policymaking.

4.3.1 Al-Shabaab on Social Media

Al-Shabaab disseminated propaganda, recruits followers and coordinates their activities through social media. The group established itself as a technologically advanced radical Islamist group in 2007and adopted the internet as part of their strategic means to plan for and further their political and operational goals. The group has remained active online, streamlining the communication channels and reaching the wider Somali population in the diaspora. It is active on Twitter and YouTube and its al-Kata'ib news channel[133]. The online presence of Al-

[132] Nzau, Mumo, and Mohammed Guyo. 2018. "The Challenge of Securing Kenya: Past Experience, Present Challenges and Future Prospects". *The Journal of Social Encounters* 2 (1).
[133] Cox, Marcellino, Bellasio, Ward, Galai, Meranto, and Persi Paoli. 2020. "Social Media in Africa: A Double-Edged Sword for Security and Development".

Shabaab has changed over time. When social media was still in its infancy stages, the group used written communications and reports to communicate with followers and international media. From 2007 to 2009, Al-Shabaab began producing video content meant to showcase their activities and to attract recruits, especially foreign fighters from Western nations. In subsequent years, the group continued releasing regular videos centred on battlefield tactics and recruitment. The production of videos established the organization as a strong presence in the media, which culminated in the formation of the Al-Kata'ib media foundation in 2010[134]. This move meant to increase the importance of the group to the international community and reach more potential recruits.

Al-Shabaab used Twitter to communicate with the media from 2011. The group reported on the Westgate shopping mall attack in Nairobi in 2013, in real-time. This was a strategy to become the main narrator of the event and distract from any official reports by the Kenyan government. The official page of the group @HSMPress gained notoriety in 2011 through its tweets in both English and Arabic. The Westgate attack was covered by the new Twitter account @HSM_Press[135]. These Twitter accounts were suspended a few weeks after they were flagged for dangerous content. As the number of internet users in Somalia has grown, the group has adapted to the wider audience. To complement its news and radio station, Al-Shabaab has engaged with local communities and international media through social media campaigns. The publications of its activities worldwide have fuelled the Al-Shabaab propaganda machine. It promotes operational successes and critiques of the Somalia government and the AMISOM troops. Twitter supports "sound bite" messages that facilitate the easy sharing of video and audio messages to the mainstream media[136]. Al-Kata'ib evolved into a quasi-news documentary

[134] Ibid

[135] Molony, Thomas. 2018. "Social Media Warfare and Kenya's Conflict with Al Shabab In Somalia: A Right to Know?". *African Affairs* 118 (471): doi:10.1093/afraf/ady035.

[136] Stephen and Carolyne. 2019. "Role of Social Media in Terrorism Crisis Communication".

channel targeted towards the Somali population, domestic and foreign reporters and to promote its activities to sympathizers and financers.

Twitter is used to report on the narrative of events according to Al-Shabaab. It has selected Twitter as the major outlet for propaganda messaging. The global response to the Westgate mall attack of 2013 showcased the growing ability of the group to capture international media attention[137]. The group uses Facebook to promote violent extremist ideologies and propaganda. YouTube was used to promote recruitment videos, However, You Tube's content management policies have hampered the production and spread of such videos. The group turned to more private and closed channels to engage with potential recruits. The recruitment strategy relies on appealing to the young Somali people living abroad and preying on their sense of alienation, lack of purpose and identity crisis. The growing poverty levels in the East African region means that more young people are vulnerable to such recruitment messages. The private chatrooms on various internet platforms, run by Al-Shabaab commanders, evade the scrutiny that comes from public forums like Twitter and Facebook. These chatrooms play to the anti-state grievances of Kenyan Muslims regarding marginalization and persecution of the government[138]. The success of these recruitment campaigns is evident in the number of attacks in the coastal region in Kenya and the border towns with Somalia.

The internet has enabled Al-Shabaab to solicit support and raise funds from international sympathizers. Operatives in Somalia have been linked to sympathetic Salafi networks who have offered financial support. Independent jihadists use Facebook and Twitter to release their messages of support for various causes[139]. This has undermined the group’s control over

[137] Simon, Tomer, Avishay Goldberg, Limor Aharonson-Daniel, Dmitry Leykin, and Bruria Adini. 2014. "Twitter in The Cross Fire—The Use of Social Media in The Westgate Mall Terror Attack in Kenya". *Plos ONE* 9 (8): e104136. doi:10.1371/journal.pone.0104136.

[138] Thomas. 2018. "Social Media Warfare and Kenya’s Conflict with Al Shabaab In Somalia: A Right to Know?".

[139] Thomas. 2018. "Social Media Warfare and Kenya’s Conflict with Al Shabaab In Somalia: A Right to Know?".

centralized messaging. The free sharing of propaganda messages through social networks has led to a wider range of incoherent messaging which has increased scrutiny and criticism of the group by internal and external voices. Nevertheless, the group has been successful in connecting with other global jihadists who have offered financial and ideological support. Online fundraising events have facilitated the growth of the group and strengthened the spread of propaganda messages. Generally, Al-Shabaab has been able to exploit the loopholes on social media platforms and Internet forums to support extremist messages, promote propaganda, obtain recruits and secure financing for their operations in East Africa[140].

4.3.2 Terror Attacks Experienced through Social Media

Al-Shabaab has conducted several attacks on Kenyan citizens and the military in Somalia. One such famous attacks was the El-Adde attack conducted in January 2016. The attack was reported through various social media platforms, where there were differing accounts on the nature of the attack and the number of casualties. Citizens flocked on Twitter to learn more about the attack, give condolences and debate on the nature of national security in Kenya. Various bloggers used their large following on social media to discount official accounts from security agencies on the extent of the El-Adde attack[141]. The official account of KDF on Twitter did not provide real-time updates, instead opting for regular press releases. A year later an attack in Kulbiyow saw the military change their approach to communicating with the public. The official Twitter account provided regular updates on the attacks and readily engaged the curious public about the security protocols in place. The different communication response to the two attacks showed the growth in social media presence in Kenya and the need to develop a closer relationship with the Kenyan public.

[140] Ibid

[141] Stephen and Carolyne. 2019. "Role of Social Media in Terrorism Crisis Communication".

Twitter communications by the Kenyan military aimed to counter online propaganda by Al-Shabaab terrorists. The terrorists had severally disputed the official accounts by security agencies in Kenya concerning the extent of their attacks. This led to a lot of misinformation and conflicting explanations from bloggers, politicians and official government accounts[142]. The lethargy of the security organizations to relay information on terror attacks facilitated the spread of propaganda by the terrorists. At Kulbiyow, the Ministry of Defence successfully killed the misinformation campaign spread by individuals purporting to have information from the ground. Some social media users shared images from past events claiming to be from the attack at Kulbiyow. The social media response from security agencies in Kenya quickly challenged the false information and urged the public not to believe the propaganda peddled by terrorists. Security agencies were able to better manage the fallout from the fake news spread through social media, by reaching Kenyans through the platforms where they were most active[143]. Official communication through social media helped regain the public trust in the dedication of security agencies in upholding national security and curbing the terrorist threat.

The September 2013 attack on the Westgate shopping mall led to a four-day siege resulting in the deaths and injuries of several people. Al-Shabaab took responsibility for the attack through one of their Twitter accounts. The terrorist organization was primarily concerned with controlling the account of the events at the mall and retaining an audience to their narrative[144]. They targeted a specific geographical audience as part of their strategy to appeal to the Western population. Security agencies in Kenya were active in providing an accurate narrative of the attack through various social media platforms. International response increased pressure on media agencies to provide correct information to the Kenyan public. The images posted on social media on the casualties and attackers disputed official accounts presented by security

[142] Ibid

[143] Stephen and Carolyne. 2019

[144] Tomer, Goldberg, Aharonson-Daniel, Leykin, and Adini. 2014. "Twitter in The Cross Fire—The Use of Social Media in The Westgate Mall Terror Attack in Kenya".

officials in Kenya. The propaganda spread by terrorists increased the paranoia on potential future attacks and the preparedness of the country to deal with such a significant security issue[145]. Security officials released several statements on Twitter to reinforce their dedication to dealing with the terrorist threat and reassure Kenyans on the trust and commitment needed to resolve the crisis. They reached out to the victims' families and the general public to show compassion, empathy, and concern. Further, security agencies discussed the sensitivity of the information on the terror attack. They urged social media users to refrain from sharing graphic images and unverified news to support crisis response initiatives. The real-time sharing of photos, videos and conversations on the international forum surrounding the attack was a significant challenge for security agencies. It highlighted the different preparedness levels of security agencies and emergency response services in handling such a massive threat to public safety[146].

The public perception of responsibility after the Westgate Mall attack underlined the role of security agencies in upholding national security policies. On Twitter, most users viewed Kenya as a victim of terrorism. Users acknowledged that the country had an increased threat of radical terrorism since 2011. The upsurge of attacks by Al-Shabaab was met by criticism of security agencies who had failed to plan for potential retaliatory attacks due to the African Union Mission in Somalia (AMISOM). Twitter users lamented that security agencies were at fault for negligent failure to plan. Law enforcement officials were blamed for incompetence and lack of enthusiasm in responding to national security[147]. The differing reports from various sections of government further increased the anger of Kenyans online, who felt that security organizations had failed them. The increased scrutiny of the government emphasized the impact of social media in forcing the accountability of security agencies in Kenya. For the first time, Kenyans

[145] Ibid
[146] Mumo and Guyo. 2018. "The Challenge of Securing Kenya: Past Experience, Present Challenges and Future Prospects".
[147] Tomer, Goldberg, Aharonson-Daniel, Leykin, and Adini. 2014. "Twitter in The Cross Fire—The Use of Social Media in The Westgate Mall Terror Attack in Kenya".

could respond to real-time news updates and call out public officials for misinformation or negligence. Social media took centre stage during the terror attacks and security agencies were under pressure to improve their performance and end the siege as soon as possible. The Westgate Mall attack was a turning point in the way the public responded to national security threats and the accountability of security agencies in providing accurate information.

Social media has been used for good in assessing crises in Kenya. Official Twitter accounts provide the public with situational awareness updates. An organization such as the Red Cross uses social media to promote blood drives and recruit volunteers during times of crisis as well as mobilize for humanitarian assistance to alleviate unnecessary suffering. Law enforcement organizations provide risk communication and public warnings in the event of an attack. The police identify the dangerous regions and ask Kenyans to keep away from them[148]. This engagement of the public in an active security situation helps to promote cohesion, prevent more casualties and hasten the emergency response process. Security agencies also use social media to control rumours and other communications. Social media users are urged to be responsible for the information shared. False information can potentially escalate the impact of the attack and cause more public fear. Taking control of the narrative allows the security organizations to reinforce their response efforts for any crisis. Condolences and verbal reinforcements through social media improve public trust in the security agencies and their dedication to upholding national security. Citizens on social media can also mobilize humanitarian assistance such as food and water for the affected, possible organ donations and volunteers to maintain order in the community[149]. Social media also serves as a stage to unite the nation to overcome a common challenge or threat. Users of Facebook and Twitter come

[148] Stephen and Carolyne. 2019. "Role of Social Media in Terrorism Crisis Communication".

[149] Ibid

together through grief and patriotism to urge security agencies to respond and share comforting messages.

4.3.3 Cybercrime and National Security in Kenya

The Communications Authority of Kenya, under the mandate of the Kenya Information and Communications Act of 1998 is required to develop a national cybersecurity management framework. The government established the National Kenya Computer Incident Response Team- Coordination Centre (National KE-CIRT/CC) to coordinate national efforts of cybersecurity in Kenya[150]. This multi-agency organization facilitates the key facets that sponsor national cybersecurity resilience in the country. The functions of the team include implementation of national cybersecurity policies, laws and regulations, providing early technical advisories and warnings on cyber threats and cybersecurity awareness and capacity building. In addition, they promote and facilitate the efficient management of critical internet resources and support research and development in cybersecurity[151]. Kenya seeks to be at the forefront of intercepting any online threats to national security through internet monitoring and collaboration with local and international actors. Cyber attackers have become more aggressive and complex and the common Kenyan lacks the tools to protect themselves from such a threat. Malware attacks in 2019 increased from 8.9 million in January to 21.1 million in July. A Microsoft Security Intelligence report of 2018 claimed that "Information security is still seen as an expense rather than a return on investment"[152]. Financial institutions have increased cyber vigilance which has driven the government to create laws to protect Kenyan cyberspace.

Social media supports the diffusion of confidential information which is prone to manipulation by criminal elements. In the recent past, cybercrime has emerged as a significant threat to Kenya's national security. The Computer and Cyber Crime Act, signed into law in May 2018

[150] "Cyber Security Overview - Communications Authority of Kenya". 2020. *Communications Authority of Kenya*.
[151] Ibid
[152] "Microsoft Intelligence Security Report: Volume 23". 2018. *Info.Microsoft.Com*.

was a response to the high-profile cyber-attacks that faced the government in the preceding years[153]. The Kenya Information Communication Act and the Penal Code regulated cybercrime legislation prior to the new law. The law served to criminalize the publishing and distribution of fake news through internet forums. It also criminalizes the online publication of hate speech. This act responded to the growing social media presence of celebrities and public figures who held significant power in influencing public opinion through social networks[154]. The law allowed for search and seizure of computer data, access to the seized data and real time collection and interception of the data. It deals with offences such as cyberterrorism, cyber espionage, child pornography, unauthorized access, false publications and hate speech. Hate speech has been a huge problem for Kenya, especially around the politically saturated electioneering periods. The act aims to curb inciting utterances on social media and regulate any spread of false information. The policymakers behind the Act meant to manage the increased connectivity in the nation and safeguard social media users from actions that may threaten national security. However, the Act was met with criticism for vague definitions and the potential of increased government surveillance. The law set a precedent for future legislations, where policymakers would be required to consult available research on the basics of free speech. Developing strict laws against online hate is the right thing to do. It should however not be used as an excuse to undermine the freedoms of expression.

4.4 National Security Goals in Kenya

Kenya has come a long way since independence in terms of national policy strategies. The country inherited many strategies from the colonialists which guided various policies of governance. The new government was faced with new problems including upholding domestic policy and conducting positive diplomatic relationships with other countries. Consequently, a

[153] Muendo, Mercy. 2018. "Kenya's New Cybercrime Law Opens the Door to Privacy Violations, Censorship". *The Conversation*.
[154] Muendo. 2018. "Kenya's New Cybercrime Law Opens the Door to Privacy Violations, Censorship".

rise in insecurity faced the country in the post-independence period, calling into question the efficacy of the colonial policies[155]. Tribal clashes, the Shifta uprising, election violence, and labor unrest rocked the nation[156]. In the following years, the security challenges evolved and policymakers were called upon to reevaluate the security strategies in place. In the 21st century, Kenya has faced a new external threat of radical terrorism. The challenge has highlighted the disconnect between security policy determinants and the general threats to national security. At the peak era of social media, security agencies are facing an unprecedented hurdle towards the application of existing national security policies. The discourse on the concept of security in Kenya has intensified in the past few years. It is therefore important to evaluate the current security policy strategies and how they can be tweaked to accommodate the implications of social media to national security.

4.5 Principles of National Security in Kenya

Chapter Fourteen of the constitution addresses national security. Article 238 outlines the principles of national security that guide policymakers. First, national security is defined as the "protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity and other national interests"[157]. Terrorism negatively impacts the identified criteria and is, therefore, a significant national security threat. Social media acts as a medium through which the activities of the terrorist organizations are promoted. It is therefore important to consider social media as a key aspect of national security which should be incorporated into the policy-making decisions.

Article 239 recognizes the national security organs as the Kenya Defense Forces, the National Intelligence Service, and the National Police Service. These agencies are primarily tasked with

[155] Kimutai, J. K. (2014). Social Media and National Security Threats: A Case Study of Kenya. *Unpublished MAThesis: University of Nairobi*

[156] Nzau, Mumo, and Mohammed Guyo. 2018. "The Challenge Of Securing Kenya: Past Experience, Present Challenges And Future Prospects". *The Journal Of Social Encounters* 2 (1).

[157] "239. National Security Organs - Kenya Law Reform Commission (KLRC)/238. Principles Of National Security". 2020. *Klrc.Go.Ke*.

the promotion of national security per national security principles[158]. These enforcing organs depend on the Legislature and Judiciary to create and reiterate laws and regulations influencing national security. Depending on the Constitutional and Parliamentary suggestions, national security organs in Kenya will develop their security policies to complement national policy[159]. National security policy is driven by the perceived impact of a national security threat to domestic stability. The administration of the national security organs advises the policymakers on the magnitude of a specific security threat, the most efficient strategies to curtail the threat and how to respect civilian authority when doing so[160]. The national security policymaking process relies on the government's domestic and foreign policy, the response of civilians and the availability of resources and personnel to enforce the policies.

4.6 Determinants of National Security in Kenya

4.6.1 Kenya's Porous Border

The porosity of the Kenya-Somalia border is vital to Kenyan security. Kenya signed the UN Refugee Convention of 1951 and the OAU Refugee Convention of 1969[161]. The country has become host to refugees from South Sudan, Somalia, DR Congo, and Burundi. The Dadaab refugee camp is the largest in the region. The country allows an open-door policy for all refugees coming from neighboring nations[162]. Kenya has yet to establish a robust border security plan that prevents the entry of potentially dangerous extremists to the country. The Kenya-Somalia border is still very porous and a major entry point for small weapons and criminals into the country.

[158] Ibid

[159] Ibid

[160] Ibid

[161] Korwa, Adar G. 1994. *The Significance Of The Legal Principle Of Territorial Integrity As The Modal Determinant Of Relations: A Case Study Of Kenya'S Foreign Policy Towards Somalia 1963-1983*. Lanham:University Press of America.

[162] Nzau and Guyo. 2018. "The Challenge Of Securing Kenya: Past Experience, Present Challenges And Future Prospects".

Domestic law enforcement in Kenya can use Twitter to broadcast information on essential policies on migration. Social media is also an effective platform for managing impressions and enlisting public assistance. Further, the border security officials can tailor messages with themes that prompt greater user response. The immigration officers and border officials through social media can take advantage of the presence of Kenyans on Twitter to assist in identification of potential illegal immigrants who might be endangering national security.

4.6.2 Cyberspace

Kenyan cyberspace accommodates social, economic and national security activities. Government activities through online platforms include registration for services and advertisement of recruitment for security agencies. The nature and security of cyberspace determine the vulnerability to hacking, the potential for misinformation and the influence on critical infrastructure. The cyberspace in Kenya is growing as more people are using the internet each day. The country faces a challenge in using the structures available to support the growing internet presence and maintain national security[163]. Cybersecurity has evolved into an international security problem in the past years. For a country such as Kenya, the resources available to national security agencies determine the preparedness for online threats. The connectedness of critical infrastructure and online systems and the government's use of online communication platforms is vital in identifying the potential extent of a national security threat. Kenya is moving in the right direction in adopting the digital environment for most government activities[164]. There is however a long way to go in ensuring the digital space is safe from any nefarious attacks and improves the capabilities of national security agencies to respond to cyber threats.

[163] "Cybersecurity Strategy: Government Of Kenya". 2014. *Ict.Go.Ke*.

[164] Ibid

4.6.3 Security Intelligence

Security agencies in Kenya have to remain alert of any internal and external security threats. This requires the establishment of a complex network of sources, communication channels, and intelligence analysis technology. In the digital age, the collection of intelligence has been made easier[165]. Most social media users post all of their information on the internet, names, addresses, age, religious beliefs, and contact information. Other users also keep their geolocation active on their phones, making it possible to track their location every time they are using social media. This social media use behavior creates a giant web of intelligence that can be beneficial for security agencies in Kenya. However, the security agencies need to have sophisticated social media monitoring technology to analyze and interpret the data collected. In Kenya, the intelligence collection agencies lack adequate resources to invest in such technologies. Further, there is limited scientific research on how social media contributes to national security outcomes. The existing cybersecurity laws allow the security organs to monitor social media user behavior in the interest of national security[166]. This is, however, a grey area, as it fails to address the invasion of privacy of innocent social media users. Government surveillance can cause public unrest if unregulated. When security agencies lack accountability on the use of public data from social media platforms, such data can be manipulated for social engineering or sold to other nations. Recently, the Huduma Number initiative caused an uproar from Kenyans on Twitter, over fears that the government was collecting civilian data for nefarious purposes. Kenya lacks the appropriate legal structures to examine such cases and hold security agencies accountable for how they use social media data. This creates a huge vacuum in the realization of national security goals through social media monitoring.

[165] Aggarwal, P., P. Arora, and R. Ghai. 2014. "Review On Cyber Crime And Security". *International Journal Of Research In Engineering And Applied Sciences* 2 (1).
[166] "Cybersecurity Strategy: Government Of Kenya". 2014.

4.7 Social Media and the Achievement of National Security Goals

The response of social media users to various national security threats can guide the policymaking process. After the Garissa University attack in 2015, the images of the suspected terrorists were shared on different platforms, and the public was engaged to assist security agencies to identify them. Kenyans took the opportunity to air their grievances over the deteriorating state of security in the nation and the lack of adequate facilities for security agencies to respond swiftly to such an attack[167]. The responsible security organs were called to task over the scarcity of emergency response officers in the region which is a hotbed for Al-Shabaab activity. This initiated a reaction from security institutions in the country, who took to social media to offer explanations for the deficiencies in emergency response services in the country. Kenyans expected the government to improve its efforts against terrorism by increasing police presence in the northeastern region. For a few weeks after the attack, there was increased security in Nairobi and other highly populated areas. Security agencies anticipated more attacks in these regions. However, as the situation died down in public discourse, the security protocols were relaxed. Kenyans still called on security agencies to reinforce security processes on the coast and northeastern Kenya to prevent such attacks in the future. The history of terror attacks in the country calls into question the preparedness of security organs against Al-Shabaab. Policy makers in the country need to place additional emphasis on strict border security policies as one key aspect of curtailing the Al-Shabaab problem. Parliament has a responsibility of developing effective security strategies for the country which will provide long term solutions against the external terror threat.

Monitoring and surveillance are key aspects of the public sector. They can predict future strategic and tactical contexts which reduce the probability of being caught unaware by

[167] "Security Questions As Kenya Mourns". 2015. *BBC News*.

different security threats[168]. The increased use of the internet and social networking platforms by citizens has prompted security agencies to design several online surveillance strategies. Security agents can track transactions and movements of individual's online, intercept communications and data. The social media platforms are an invaluable resource for the security agencies since users leave digital fingerprints that can be easily gathered and analyzed. The use of social media sites by criminals and adversary states is on the rise. Security agencies in Kenya are therefore having to adapt to the changing crime environment. Through Twitter, Kenya Police and the DCI inform citizens on their security operations and strategies to reduce crime. Further, progressive analysis of social media platforms by these security organs serves as an early warning which can help in the promotion of national security. The response of the public to the posts from security agencies can help them gauge the applicability of any new policies and security tactics. Active engagement of social media users in these operations informs the security agencies on the aspects they need to improve on and the policy advocacy needed to fulfill the national security goals.

Security agencies in first world countries have advanced technologies that have enabled development on various tools that help to monitor online communication. In these nations, security policy has evolved to capture the essence of technology and its role in upholding national security[169]. Kenya remains behind in the adoption and implementation of such technologies on a wider scale. The available social media platforms in the country can provide a vast library of data that can be used to reinforce border security and curb the entry of small arms from Somalia. Social media monitoring technologies enable security agencies to aggregate, filter and analyze information, trace the location of origin of certain social media communications and monitor the potential of people creating posts that compromise

[168] Brelsford, Paul. 2013. "Employing A Social Media Monitoring Tool As An OSINT Platform For Intelligence, Defense & Security."

[169] Fuchs, Christian, Kees Boersma, and Anders Albrechtslund. 2012. *Internet And Surveillance: The Challenges Of Web 2.0 And Social Media*. New York, N.Y: Routledge.

security[170]. Fake news, inciting speech and hate speech emerge around the elections period when the country is heavy on political campaigns. During these times, security agencies are faced with increased tensions in urban centers, tribal violence and online misinformation which can potentially spill out to real life. The use of social media in such times compromises the efforts of security agencies to maintain peace during politically volatile periods in the country.

In the hotly contested 2017 general elections, Kenyans on social media were exposed to a plethora of fake information on possible election tampering. Social media was used as a staging point for various demonstrations demanding electoral transparency. Users actively advocated for violent protests and targeting of people from specific regions in the country. When violence broke out, the images of police harassing civilians were posted online. Security agencies were forced to take responsibility for the actions of their officers and readjust their policies on how to handle protestors. There were successful campaigns on Twitter calling for the termination of officers who were suspected of injuring or killing civilians during the demonstrations. The TJRC report of 2013 highlighted the extent of extrajudicial killings in the country and the role of security agencies in protecting the perpetrators[171]. The report published the various injustices committed on civilians since Kenya gained independence and how the national security organs were compliant. When the report was released Kenyans online were prompted to question the credibility of security officials in the country and their responsibility for providing reparations for the various injustices. The report acknowledged that the legal system in Kenya is insufficient to prevent extrajudicial killings and enforced disappearances. This has increased impunity among perpetrators in security organs who escape prosecution due to vague laws[172]. The presence of the national security organizations on social media allows Kenyans to inquire about the prosecution of the perpetrators. The official accounts of these agencies on social

[170] Ibid
[171] "Summary: Truth, Justice And Reconciliation Commission Report". 2013. *Knchr.Org*.
[172] Ibid

media are obligated to provide an accurate state of events to Kenyans online. Consequently, social media users can mobilize and bombard social media accounts with queries and suggestions on how justice can be served for those affected by the injustices committed by security officers.

Social media is used for psychological operations and public diplomacy. Security agencies in the country create content that seeks to impact peoples' objective reasoning, motives, and emotions[173]. In developed countries, the security apparatuses conduct psychological operations as part of the information warfare strategy to influence the sentiments of people. This, in turn, determines the national security policies implemented and the resources allocated for their application online. Cutting edge technological innovations at the disposal of security agencies distribute content through blogs, chatbots, and virtual reality programs[174]. The organs convey specific messages meant to elicit certain reactions and behavior that affects the achievement of security goals. Psychological operations are vital in interfering with divulging propaganda and artifact messages from opponents. These operations are essential when dealing with terrorist misinformation campaigns and propaganda targeting certain groups of citizens. This strategy can be implemented in Kenya, to curb the perpetual attacks from Al-Shabaab in the coastal region. Security agencies have to create information campaigns meant to increase public trust in their forces and reiterate their dedication towards securing the region and nation as a whole. Information warfare is the next frontier of international conflicts[175]. Security agencies have to always be prepared to manage the entry of information from outside sources. Information communication policies define the preparedness of any nation to deal with the threat of information warfare from social media networks.

[173] Reuter, Christian, Amanda Lee Hughes, and Marc-André Kaufhold. 2018. "Social Media In Crisis Management: An Evaluation And Analysis Of Crisis Informatics Research". *International Journal Of Human–Computer Interaction* 34 (4): doi:10.1080/10447318.2018.1427832.

[174] Brelsford, Paul. 2013. "Employing A Social Media Monitoring Tool As An OSINT Platform For Intelligence, Defense & Security."

[175] Ibid

The COVID-19 pandemic has shown the importance of social media in maintaining harmony and peace of mind during a crisis. Images circulating worldwide have helped people understand the extent of the virus, the appropriate protective measures. Further, social media has facilitated the spreading of positive messages across the globe and the exchange of vital safety information. Kenyans, through Twitter and WhatsApp, have been keeping track of the spread of the virus and in the identification of potential hotspots of the virus. Social media has been effective in encouraging people to stay home and enforce social distancing measures to slow down the effects of the pandemic[176]. The #StayatHome movement on Twitter is an example of how the scope of social media can be exploited for positive purposes. However, misinformation on the virus is rife on social media platforms. The WHO, CDC, and other health organizations are fighting the spread of fake news by providing accurate scientific and medical information on the spread of the virus. In Kenya, the Ministry of Health is active on social media, generating awareness, updating the public on the spread of the virus, and the various protective measures available. As COVID-19 continues to threaten the health and national security in many countries, social media remains a vital tool for global communication and information.

4.8 Information Security

Strategic communication is a vital component of any policy. The EU has a Strategic Agenda that targets the information threat towards the domestic security of its member states. This policy advocates for the reinforcement of strategic communications in Europe through increased attention to the production of common narratives and factual representation of conflicts[177]. To deal with national security threats among member states, the EU has set up measures to promote counter-narratives in social media networks. The security and defense sectors in Europe posit that strategic communication is an effective approach towards

[176] Volkin, Samuel. 2020. "Social Media Fuels Spread Of COVID-19 Information—And Misinformation". *The Hub*.
[177] Carrapico, Helena, and André Barrinha. 2017. "The EU As A Coherent (Cyber)Security Actor?". *JCMS: Journal Of Common Market Studies* 55 (6): doi:10.1111/jcms.12575.

information threats from outside the union[178]. The European External Action Service, in 2015, recommended strategic communication as a lasting solution to disinformation coming from state and non-state actors from the east. The commission suggested an action plan that would strengthen security within the EU by pushing positive and effective messages on EU policies. The union also acknowledged the impact of developing coordinated communication mechanisms to counter externally produced disinformation. These mechanisms would incorporate better management of messages spread through social media on the state of European security and filtering the information flowing into the union from the Middle East[179].

The EU has established strategies to combat the spread of fake news and manage the ensuing consequences. Media pluralism strategies targeted towards the digital markets seek to champion the diversity of information as the main principle driving action against online discrimination[180]. The High-Level Expert Group on Fake News was founded in 2017 funds projects in Europe focusing on advocating for media freedom in the member states. Media pluralism endorses the implementation of information security tools in online platforms. As fake news continues to spread through mass and social media, the EU is prepared to safeguard European security[181]. Social media forms an important part of security policies for the EU, especially in the management of information from extremist groups. Anti-discrimination and fake news detection technologies are essential for the EU's security policies. The biggest hurdle remains to unite the member states in the discourse and instituting a blanket policy that addresses the diversity of security problems in the continent.

[178] Mälksoo, Maria. 2018. "Countering Hybrid Warfare As Ontological Security Management: The Emerging Practices Of The EU And NATO". *European Security* 27 (3): doi:10.1080/09662839.2018.1497984.
[179] Mälksoo. 2018. "Countering Hybrid Warfare As Ontological Security Management: The Emerging Practices Of The EU And NATO".
[180] Carrapico and Barrinha. 2017. "The EU As A Coherent (Cyber)Security Actor?".
[181] Mälksoo. 2018. "Countering Hybrid Warfare As Ontological Security Management: The Emerging Practices Of The EU And NATO".

Kenya can take lessons from the policies in the EU to further the strategic communication policies to support national security. Kenya's Vision 2030 has set a plan for the expansion of ICT capabilities in the nation. The development seeks to increase interconnectivity among businesses and individuals across the country. This will open up the nation to more cyber threats from criminal organizations, enemy nation-states, and hacktivists[182]. The National Cybersecurity Strategy created in 2016 by the ICT Ministry defines the cybersecurity vision for Kenya, and the commitment to support national priorities through encouraging ICT growth and protection of critical information infrastructures. Cybersecurity is a key component in the national goals to secure and foster the prosperity of the country. The government plans to increase private-public partnerships, academic partnerships and NGO's to implement an effective building process for cybersecurity infrastructure. Kenya aims to become a trusted partner and cybersecurity within East Africa and the world[183]. The National Cybersecurity Strategy focuses on four strategic goals: building national capability through increased cybersecurity awareness, and workforce to address cybersecurity needs; enhancing the national cybersecurity posture; foster sharing of information and collaboration among stakeholders to facilitate an open information sharing environment; and provide national leadership by defining the national cybersecurity goals, objectives and coordinating cybersecurity initiatives at the national level. In collaboration with security agencies, the government will work with academia to develop cybersecurity programs and specialized training to boost competency for cybersecurity professionals[184]. This will facilitate the transition to a digital world, where the nation will be prepared to deal with any online information threats.

Intelligence agencies in the US rely heavily on social media and other open-source intelligence to collect critical information on terrorist groups and criminal threats. Open-source intelligence

[182] "Cybersecurity Strategy: Government Of Kenya" 2014
[183] Ibid
[184] Ibid

has grown into a crucial source of actionable data in the past decade. Security agencies have been using social media to identify suspects and key eyewitnesses to various strategies in and outside the country[185]. Intelligence agencies such as the CIA have adopted social media as a key tool for their data collection strategies. The MH17 flight tragedy was solved through social media. The Boston Bomber was caught through open-source intelligence. The security agencies within the US observe global public sentiment and political climates through social networks[186]. The intelligence collected informs national security policy and international relations. The Department of Homeland Security (DHS) adopted social media as a way to provide the public with more information on the state of domestic security[187]. The DHS actively engages with users on social media to update on security policy and the nature of domestic security. The agency has expanded social media monitoring programs in the recent past to collect a vast amount of user information. The DHS collects data on political and religious views, physical and mental health information, and identity of close relatives. This information is analyzed and vetted, especially for people seeking entry into the US[188]. Twitter, Instagram, Facebook and LinkedIn accounts of the DHS are actively seeking to communicate with the public, offer their perspective on national security, and popularize community policing measures. DHS social media monitoring programs have expanded at par with the proliferation of social media information and the growth of companies creating products to interpret the information.

Kenya Vision 2030 National Security and Policing Reform aims to enhance the effectiveness of national security and policing services and operations across Kenya. One of the strategies incorporates enhanced crime data collection, analysis, and storage. The reforms aim to integrate

[185] Blanken, Leo J, Hy S Rothstein, and Jason J Lepore. 2015. *Assessing War: The Challenge Of Measuring Success And Failure*. Washington: Georgetown University Press.
[186] Ibid
[187] "Social Media Directory". 2020. *Department Of Homeland Security*.
[188] Cavelty, M D. 2007. *Cybersecurity And Threat Politics: US Efforts To Secure The Information Age*. New York: Routledge.

focus for national security and police agencies by reviewing security and policing laws and improving data collection and analysis methodology[189]. Similar to the US, security agencies in Kenya are working towards establishing online monitoring technologies that fit within the context of security and crime in Kenya. Crime prevention is a big part of the Vision 2030 program. Improved facilities, equipment, and technology will improve the security institutional frameworks and address the capacity challenges facing the law enforcement sector. Social media monitoring programs and strategic communication policies are the way forward in securing the information future for Kenya. The ICT ministry established a plan to help the government secure its information-sharing capability. Sharing cybersecurity information between different government organizations and sectors will cultivate a culture of information that facilitates the achievement of national cybersecurity goals[190]. As security agencies enhance their efforts against terrorism, urban crime, and tribal clashes, they should recognize the impending threat to Kenya's cybersecurity. The ICT future of Kenya is bright. The lingering question is whether the country is ready to harness all the capabilities of digital technology and protect itself in the digital space.

4.9 Conclusion

This chapter reveals the legal framework established in the nation in response to cybercrimes. Kenya lags in the implementation of effective laws against online crimes. President Kenyatta's government has made significant strides in developing policies to curb online crime and reinforce the cybersecurity infrastructure in the nation. The chapter proves that security agencies in Kenya lack defined structures of monitoring the use of social media and the effects on national security. Al Shabab, the main international threat to Kenya's national security has used social media in the past to carry out their attacks. Security agencies in Kenya have successfully intercepted communications between the groups and thwarted the attacks.

[189] "National Security And Policing Reform | Kenya Vision 2030". 2017. *Vision2030.Go.Ke*.
[190] Ibid

However, social media companies are doing the lion's share of the work, monitoring communications, and collecting data on suspicious interactions between possible criminal elements. Kenya has not established adequate infrastructure to facilitate the management of information through social media and the prevention of crimes originating in the digital sphere. Information security in Kenya is not guaranteed under the existing legal frameworks. Following advancements in the EU, Kenya, and Africa as a whole can take lessons on how to create institutions that regulate online communications and develop policies that promote the development of a strong cybersecurity environment.

CHAPTER FIVE

DATA PRESENTATION AND ANALYSIS

5.1 Introduction

This chapter presents data analysis, presentation and discussion of the findings. The chapter draws from the study objectives, drawing on descriptive statistics, and presented in the form of graphs.

5.2 Response Rate

The study initially targeted 55 respondents from across the country. The study created 55 questionnaires, of which 40 were filled and returned. However, only 30 questionnaires were deemed to fit the criteria selected for the study. The response rate was 54%, as exhibited in the chart below:

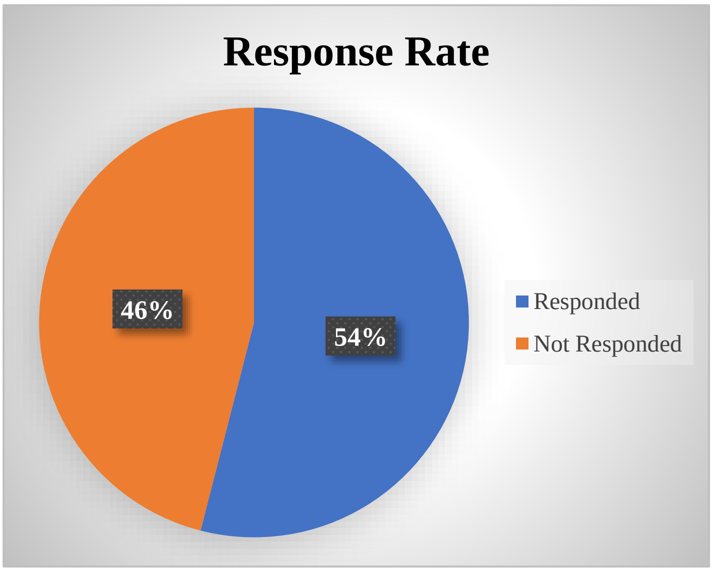


Figure 5.1:Response Rate

The 30 responses used for the study proved adequate for data analysis and fulfillment of the study objectives.

5.3 Demographic Information

The study focused on the age of respondents, gender, and career fields.

5.3.1 Age

The age distribution is summarized in the table below:

Table 5.1: Age Distribution

Age	No of Respondents
18	2
19	1
20	2
21	5
22	3
23	2
24	3
25	4
26	2
27	3
28	3

5.3.2 Gender

17 respondents were male and 13 were female. The distribution is presented in the chart below:

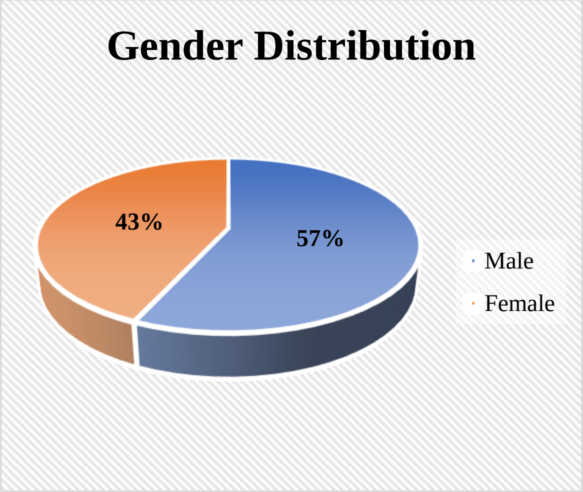


Figure 5.2:Gender Distribution

5.3.3 Careers

The careers of the respondents were classified on whether they worked for the government or the private sector. 15 respondents were government employees and 10 were employed in the private sector and 5 were unemployed at the time of the survey.

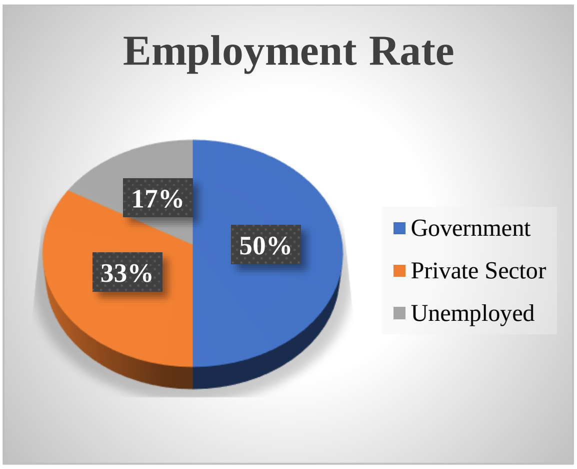


Figure 5.3:Employment Rate

5.4 Social Media Usage in the Country

The respondents were asked to categorize the social media sites active in Kenya and their use in regard to national security matters. The graph below shows the five main social media sites in the country, Twitter, Facebook, YouTube, Instagram, and WhatsApp, on their usage to spread information crucial to national security. Facebook had the highest interaction rate at 32%, WhatsApp at 26%, Twitter at 22%, Instagram at 15%, and YouTube at 5%.

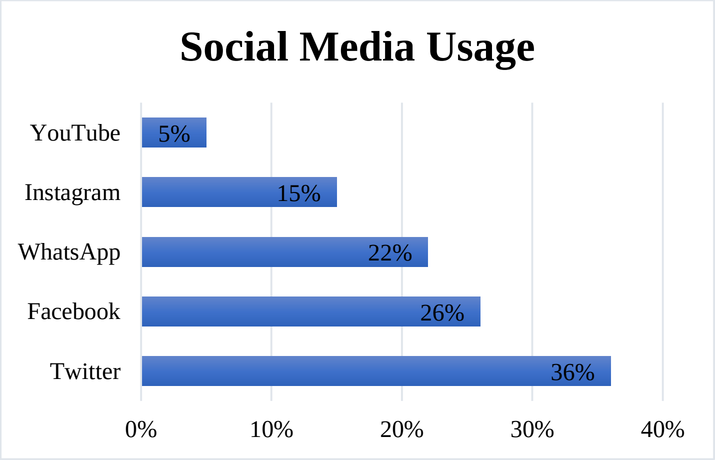


Figure 5.4: Social Media Usage

5.5 Age Distribution of Social Media Users

The respondents were asked to rank each of the five social media sites and the frequency with which they use for news information. The questionnaire asked the respondents: If there were to be a major national security issue at the moment, which social media site would you open first?

The most popular platform was for users aged between 24-28 was Twitter, 30%, followed by Facebook, 27%, WhatsApp, 23%, Instagram, 11%, and YouTube, 9%. Users aged between 18-23, preferred WhatsApp, 33%, then Twitter, 25%, Facebook, 25%, Instagram, 11%, and YouTube, 6%.

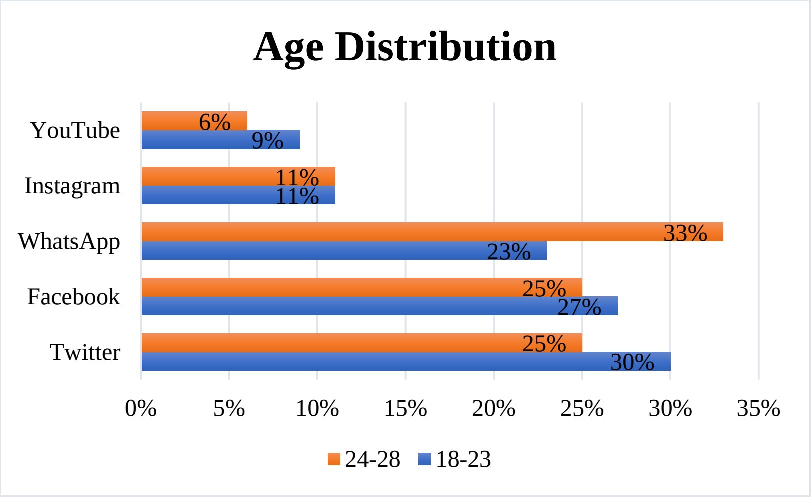


Figure 5.5: Age Distribution

5.6 Threats of Social Media

This section focused on current and future threats of social media technology to the national security landscape in Kenya. The survey began by inquiring whether the respondents considered social media as a legitimate threat to Kenya's national security. 85% of the respondents concurred with the hypotheses of the paper, that social media is a threat to national security. 15% believed that social media was not an adequate threat to national security.

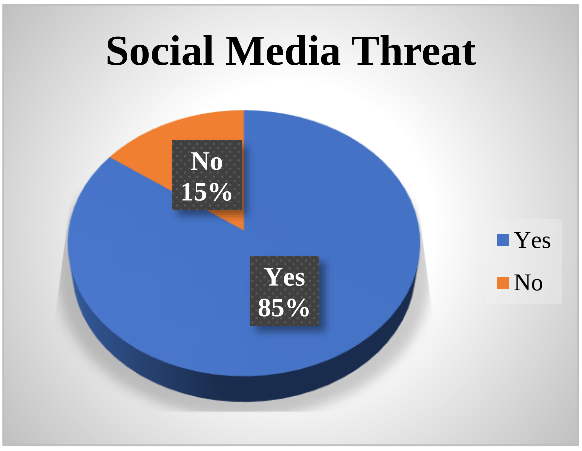


Figure 5.6: Social Media Threat

5.7 Negative Impact of Social Media on National Security

The respondents were asked to identify the biggest threats to national security from social media. The table below represents the distribution of the results:

Table 5.2: Negative Effects of Social Media on National Security

Negative Effects of Social Media	Frequency
Recruitment into criminal groups	12
Terrorist communication and radicalization	23
State and non-state actors' propaganda	23
Cyberbullying	25
Misinformation	24
Government surveillance	10

5.8 Use of Social Media by Security Agencies in Kenya

The questionnaire required the respondents to rank the use of social media for national security matters on a scale of 0-5, 0 being poor and 5 being excellent.

Table 5.3:Use of Social media by Security Agencies in Kenya

	0- Poor	1- Unsatisfactory	2- Moderate	3- Satisfactory	4- Good	5- Excellent
Communication with the public				Satisfactory		
Promote Public Diplomacy			Moderate			
Open-Source Intelligence		Unsatisfactory				
Counter-Propaganda Services				Satisfactory		
Fighting Crime					Good	

5.9 Cybercrime incidences

The respondents were asked to indicate whether they had come across any incidences of cybercrimes on their own, in the workplace, or from their peers. The findings are presented in the table below:

Table 5.4:Cybercrime Incidences

Cybercrime	**Frequency**
Phishing Scams	15
Malware Attacks	17
Trojans	9
Identity Theft	5
Fraud	20

The questionnaire had a section that prompted the respondents to provide recommendations on how to improve cybersecurity in the country. They acknowledged the need for stricter rules in the digital space. The government should install better regulations that manage the operations of social media companies in Kenya, control online information, and curbing the spread of misinformation. Further, the respondents reported that the government should invest more in research and development of cybertechnologies in the country. This would allow better data management and prevention of fake news and hate speech through social networks. The respondents indicated that academia has to be more involved in developing the technical skills essential in the management of internet technologies. The government needs to increase the monitoring of social media, but not at the expense of privacy and freedom of speech. The respondents highlighted concerns over the future of government surveillance but stated that more digital laws would effectively police the digital space and reduce the occurrence of cybercrimes.

CHAPTER SIX

SUMMARY, RECOMMENDATIONS, AND CONCLUSION

6.1 Summary

Social media has become a staple of communication in modern society. Users on these platforms engage with others by sharing content, videos, and images of various public and private moments. While the consumption of social media across the globe increases, it has resulted in different impacts on society. Several theories explain the dissemination of social media content on the issue of national security. The Uses and Gratifications Theory suggests that people have specific intentions and purposes behind the consumption of social media. As users seek to satisfy their curiosity needs, they will spend varying amounts of time on social networks. Social Impact Theory posits that online interactions between strangers are different from those between family members. Therefore, any information shared by a family member, or people with common interests whether true or false, is more believable than information shared by a stranger. Finally, Resource Mobilization Theory holds that political movements can be more successful through the efficient mobilization of resources such as money and organizational skills. Social media offers a platform to unite people from different backgrounds, motivate revolutions, and sustain longer periods of political protests. These theories explain how social media has been effective in the political movements of Egypt, Tunisia, and Syria. These countries began online mobilization, which was effective in the achievement of the goals of various social movements.

The third chapter examines the impact of social media on the achievement of national security goals. The different ethical, legal, and technological implications of online networks shape how users interact and initiate change in the modern world. One of the benefits of social media is the ability to share text, images, and videos quickly, and sometimes in real-time, as events occur worldwide. The world followed the Turkish Protests of 2013 through social media. Twitter and Facebook supported the sharing of updates, communication of essential logistical information on medical assistance, and the capacity of emergency services. Social media manages to escape the biases of traditional media as it allows unlimited sharing of content by anyone with internet access. The dissemination of information by social media users affected by different conflicts across the world shapes the response of the global community on the national security policies in different states.

Social media is used by security agencies to engage the public on important security matters. Organizations such as the DHS have effectively harnessed the potential of social media to communicate security information with the citizens. Social media reaches a wide range of people. During times of crisis, the public needs constant reassurance from security agencies and updates on emergency operations. The national security agencies will use social media platforms to extract vital intelligence on adversaries. Security institutions collaborating with community groups through social media can identify extremists who threaten national security. The research examined the Nyumba Kumi initiative in Kenya and how it has been effective through social media. Community leaders have taken the mandate to mobilize neighborhoods to maintain local security, which in turn upholds the national security goals for the country.

The research examined the various negatives of social media to national security, especially regarding terrorism. Social media is a tool used by terrorist organizations for ideological radicalization, recruitment, showcasing training tactics, spreading propaganda, and communicating operational strategy. Kenya's main terrorist threat is Somalia-based Al-Shabaab. The radical group has conducted several deadly attacks within the Kenyan borders. Al-Shabaab took advantage of the wide scope of social media to communicate its agenda to potential recruits and coordinate activities with their followers. This research has established that nefarious actors exploit social media platforms to undermine national security. Terrorism is one of the main national security threats in Kenya. Twitter, Facebook, and WhatsApp have been used as staging grounds for different attacks in the country.

Identity theft and cyberbullying have become commonplace in the era of social media. Social media platforms require users to upload personal information such as family, education level, age, and gender. This information is used to create a profile that forms a user's online personality. Hackers often take advantage of this to steal information and sell it to third parties, spread propaganda, and distribute false information. In the recent past, fake news has invaded the online space. Both state and non-state actors are involved in the sharing of falsehoods and rumors are meant to undermine the policymaking process. Many countries lack the necessary tools to trace the origin and spread of fake news on social media, which is often detrimental to national security. Unverified information often from trolls on social media propagates certain narratives on sensitive matters, spreading fear especially in the event of a terror attack. Complimented by the invention of deep fake technology it is clear that fake news will continue being a problem for national security in the years to come. The research has revealed the need for social media monitoring technologies that counter the effects of fake news and deep fakes to maintain national harmony.

Chapter four has evaluated the implications of social media on national security in African countries. The government of Kenya has been working on the digitization of many services to offer Kenyans a better platform to participate in government. These online services have enabled the adoption of social media communication strategies that resonate with most Kenyans. The government uses social media to inform the public on critical information on national security and other policies. During the various terror attacks in the past, the government has used social media as an official communication channel to reach out to Kenyans. The security agencies in Kenya, the DCI, and Kenya Police maintain regular updates on Facebook and Twitter on the state of security in the nation. They encourage members of the public to offer information on bad elements and assist them in developing essential security policies.

Further, the chapter highlighted the deficiencies within the national security institutions in the application of social media tools. Kenyans on social media have been active in calling the government to task on various national security matters, especially the Al- Shabab threat. The security agencies in the country, however, lack the necessary expertise and technologies to fully monitor the use of social media by nefarious actors. The adoption and implementation of these essential technologies are crucial in weathering the perpetual terrorist threat to the nation. It is clear that Kenya has a long way to go in understanding and analyzing social media for the benefit of national security. This challenge can be solved by adopting technologies from developed countries and tailoring them to fit into the unique needs of Kenya's security.

Chapter five analyzes the respondents' answers to the questionnaires. The respondents acknowledged the significant role of social media in Kenya's national security, with the associated benefits and threats. The chapter indicates that Twitter is the most popular social media platform in the country, especially among the younger population. Users are likely to open Twitter for information whenever a news story breaks. Further, the respondents indicated that there was a high probability of misinformation on social media, owing to a lack of regulations in the digital space. The study further revealed that a majority of social media users are wary of cyberbullying and terrorist presence on social media platforms. The respondents indicate that the government is doing a satisfactory job communicating with the public and countering propaganda through social media. The main cause of concern was the lack of investment in and utilization of open-source intelligence in social media. The respondents indicated that phishing scams, malware attacks, and fraud were the most common cyber-crimes in the country. When the respondents were asked to provide recommendations for the government, they indicated the need for more investment in cybersecurity, focus on research and development, and integration of academia in cybertechnology advancement in the country.

6.2 Recommendations

In the 21st century, political economy is essential in understanding and regulating the impact of social media on society. The global digital sphere promised free communications in exchange for widespread data collection and analysis. Through this, companies can access user data and sell it to advertisers and other businesses. Social media companies are encouraged to surveil, addict, and manipulate users to strike deals with third parties who further perpetuate the manipulation. A company such as Facebook has come under criticism due to the exploitation of user data for business and political reasons. The Cambridge Analytica scandal highlights the dangers of giving social media companies free reign over user data. Twitter, Facebook, WhatsApp, and Instagram have essential roles in organizing and curating public discussion. They are responsible for the protection of public data and safeguarding the privacy and freedom of users online. However, the rapid growth of social media users has given these platforms too much power and influence over political economies across the world.

In the EU, strategic communication and censorship are used to counter the information threat. Coherence and efficiency in the digital sphere are critical techniques for the management of the information space. Kenya lags in the management of online communication, especially in matters of governance. The EU should serve as a benchmark for an effective unified message that mitigates the threat of online extremism. Europe has created a strict agenda, enforced through coordination and consistency. Information management encompasses different strategic communication and censorship techniques that reduce accessibility to terrorist content and increase the volume of alternative narratives online[191]. The key to information management in the EU is the dissemination of credible truths to counter extremist propaganda online. Taking control over the digital information space through efficient intervention has been effective in promoting national security in Europe. One of the technologies applied in the EU is the

[191] Ördén, Hedvig. 2019. "Deferring Substance: EU Policy And The Information Threat". *Intelligence And National Security* 34 (3): doi:10.1080/02684527.2019.1553706.

automatic detection of undesired content and algorithms that recognize illegal and offensive messages on social networks. The values of coherence and efficiency have driven the EU's online security protocols, which have helped to curb the terrorism threat from the Middle East.

Kenya has the potential to adopt the EU approach to weather the ever-present Al-Shabaab threat. However, it will require significant investment, government dedication, and public engagement to achieve this goal. More research is needed to understand the growing role of social media on national security. Law enforcement agencies in Kenya should exploit the free range of social media to educate the public and enhance their security operations against potential threats. Kenya's vision of security should acknowledge the prospects of strategic communication and censorship as anti-terrorism approaches. The government's investment in IT for the past few years shows the willingness to invest in the digital space and utilize all the capabilities for governance. National security should be included in the digital movement of the Kenyan government. Security agencies have to understand the information vacuum on social media and create a communication flow that suppresses lies, rumors, and disinformation generated by adversaries. They have to safeguard the information space from the negative sway of extremist elements. A coherent approach by security authorities will undermine the propaganda by enemies and reinforce the achievement of national security goals in Kenya.

Countering online radicalization in Africa is plagued with a number of challenges. Governments struggle in creating a balance between regulation of online space and protecting individuals' freedom of expression. Further, certain social media and messaging services such as WhatsApp have high levels of end-to-end encryption which makes it difficult to design and deliver interventions to fight online radicalization. Social media companies also have resource limitations that constrain their ability to continuously monitor online content, even with the willingness to commit. The field of countering online radicalization is relatively new to many African governments. Kenya and Somalia have partnered with the EU and UNDP to introduce national strategies that aim to counter the threat of Al-Shabaab[192]. Kenya is at the forefront of addressing radicalization in the region more broadly. Despite these efforts, the cyberspace in Kenya remains vulnerable to fake news, disinformation, and the spread of terrorist propaganda. As a result, security agencies have to review the national cybersecurity strategies and dedicate more resources to develop online counter-narratives. The legislature should develop better laws that govern the operations of social media companies in the country. It is vital to have a defined legal structure that counters online crimes and other atrocities perpetrated through social media forums.

Kenya needs to develop a bespoke national security strategy to counter online radicalization. The various stakeholders, social media providers, law enforcement, community organizations, and the UNDP, should be consulted to ensure effective implementation of the strategy[193]. The national strategy should consider the context of the threat to Kenya, and develop clearly defined objectives towards a target population, with desired outcomes. Law enforcement agencies should audit the state of security in the country and provide an estimation of the resources in terms of financial costs, organizational needs, human resources, and infrastructural requirements. The stakeholders will provide a template for the national government to follow and the contextual application of the proposed strategies. The strategy would only work if the three arms of government are united in facilitating the implementation of digital media policies. The legislature develops the policies, the executive provides the framework for the implementation and the judiciary enforces the application of the laws. The judiciary has in the past blocked the implementation of digital security policies, which has further hampered the future of digital laws in Kenya. The government has a responsibility to unite the three arms in

[192] "Social Media In Africa: A Double-Edged Sword For Security And Development", 2017.
[193] Ibid

the discourse on online laws and create a definite plan to facilitate the digital laws environment in the country, through a Multi- Agency approach.

Kenya needs to bridge the gap between technical knowledge, internet use and technological innovation to foster a strong foundation on which to build a national security infrastructure. Focusing mainly on the use of Facebook, Twitter, You Tube and WhatsApp, the impact of social media on national security remains largely unassessed. The civil society and academia have a responsibility to reinforce the digital framework in Kenya by educating the public and instilling the necessary technical skills to navigate the digital world. As incidences of cybercrime increase in the country, it is essential to provide the public with access to knowledge on phishing scams, misinformation and fake news. With the implementation of the new curriculum, the civil society has to emphasize on the importance of digital skills in schools and potential employees. As more people become technologically aware and informed on the dangers of social media, the country will have a better foundation on which to build its digital future.

Counter radicalization programs should not only focus on offering reactive social media responses after major terrorist attacks but also on developing proactive and continuous counter-narratives online. Social media platforms are relied on as reliable sources of news during a security attack. Analysis of the various platforms reveals a growing sense of uncertainty over the news circulating on social media. The institutions are therefore obliged to share and promote reliable news and carefully crafted messages in times of crisis. The strategies against misinformation through social media in Kenya should consider several factors. The strategies based on multiple social media platforms using multiple languages and targeted messages across multiple sectors to maximize the visibility of accurate information. The counter-radicalization programs should be tailored to the local context, by engaging with community groups and religious organizations. Effective anti-terrorism messages are sensitive to local communities and relatable to the target audience.

Kenya should collaborate with national, regional, and international actors in countering online radicalization. Terrorist organizations across the world operate social media in similar ways and present definite challenges to national security. Information exchange and cooperation between governments is a compelling anti-terrorism approach through social media in Multi - Agency Cooperation. Social media is borderless meaning that the successes and failures of national security systems can be broadcast to the entire world. National security agencies from different countries should follow each other on social media, tag, and retweet information critical to mitigating the online threat of terrorism. Creating online communities that provide official narratives and accurate content can further motivate counter-radicalization activities across the globe. In Africa, the UNDP could coordinate annual conferences on the lessons learned on the functioning counter-radicalization techniques and individual success stories. Countries can also exchange ideas on how to address the key challenges and risks and future opportunities for learning and collaboration. Yearly reports on the state of counter-terrorism initiatives through social media will provide a reference framework for the essential investments needed in the digital information management sphere. Political and technological scholars can provide their expertise on the constructive use of social media by security agencies to curb the threat of extremist groups online.

Security agencies in Kenya should boost their efforts in monitoring terrorist activity on social media and implement a variety of activities to counter them. The surveillance programs that monitor online activity and track potential terrorists are not available in the public domain. The sensitive nature of anti-terror operations necessitates covert actions, which are often kept from the public. This results in distrust from the public on access to private data and potential government surveillance. Security agencies have the responsibility to monitor social media responsibly, identify significant security threats without infringing on the privacy of social media users. The cybersecurity vision in Kenya should focus on policy development, public awareness campaigns, and public-private sector coordination. Information from the social media platforms should inform and advise the entities responsible for safeguarding geographical areas targeted by terror groups. In Kenya, this involves identifying the most at-risk areas and evaluating the role of social media on the growing insecurity. Security agencies can, therefore, leverage this information to design a social media monitoring program, tailored towards preventing attacks and respecting the liberties of local communities. The DCI, Kenya Police, and NIS have to establish a working relationship that encourages open sharing of information and development of monitoring technologies that will boost the capability of the country to monitor social media. This will ultimately define the counter-terrorism approach in Kenya for the future and inform the development of sound national security policies.

Delivering better security in Kenya requires an imaginative, robust way of combating online terrorism. The resilience of the security organs in Kenya to the threat of Al-Shabaab is indicative of the future directions of security policy in the region. The government should construct a systematic big picture perspective on social media intelligence. First, security agencies should understand the signs of hostile activity against the security institutions in the country. This defines the preparedness in mitigating any consequences of enemy states or terrorists threatening the harmony of Kenya. The ability to pre-empt attacks, identify hate speech, intercept terrorist propaganda, and infiltrate online recruitment platforms is vital in fighting any form of extremism in the country. Security agencies should be transparent in their social media monitoring, by constantly updating the public on the nature of their operations and their accountability in safeguarding user data[194]. Second, security agencies should liaise with policymakers on the regulation of hate speech. The regulatory process should not infringe

[194] Reuter, Hughes, and Kaufhold. 2018. "Social Media In Crisis Management: An Evaluation And Analysis Of Crisis Informatics Research".

on the freedom of expression of social media users and freedom of speech. Social media platforms should provide guidelines on how to identify hate speech online, the appropriate reporting procedure, and the protection of other users' data. The key to this method is striking a balance between the threat of violence, hate speech, and free expression of the public.

Most developing countries lack data protection and privacy legislation related to internet use. The digital spaces are highly unregulated and social media companies are largely responsible for the policing of the users. These countries should recognize the importance of data protection and privacy, and the massive role of social media in shaping society. Users should have avenues to report violence and politically sensitive issues to security agencies through social media. The security institutions should take the responsibility to uphold information security and operational security in ICT platforms. Public trust in security agencies is key to the achievement of information management goals through social media. In Kenya, the security organs need to invest in awareness and public participation programs through social media. These programs educate the public on information security, data protection, and the role of social media monitoring in the promotion of national security goals. Policymakers should redefine the vision for national security to include all aspects of the digital space. The policies should acknowledge the future growth of communication technology and the different impacts on national security. Cybersecurity should be an important facet of legislation on domestic security and counter-terrorism strategies.

Security agencies should hold their officials to a higher standard on the use of social media. The protection of sensitive information and responsible use of social media for security officers is vital for the maintenance of integrity in security organs. A multi-agency policy on social media is the first step in ensuring the accountability of the security apparatus in the country. Such a policy should cover the wide scope of social media, the future developments in social media technology, and the evolving security threats for Kenya. The policy should not, however, curtail the freedom of speech of the officers. It would allow officers to use social media to their discretion, and on their own devices. There should be strict disciplinary measures for the officers who compromise national security by disclosing sensitive matters on social media. The military and police agencies have the right to restrict the speech of their employees under certain circumstances. If social media use of an officer compromises their professionalism and that of the agency, the institution can censor their online activity. Administrators in the agencies should have a stringent filter for information that can and cannot be shared on social media to prevent reckless social media use.

Security organs in Kenya should train their officers and the general public on the threats of social media on national security. Higher education institutions should incorporate social media training into their curriculum. Emphasis should be placed on the identification of fake news, hate speech, and deep fake technology. Security agencies should define legitimate accounts to provide credible information in a time of crisis. The government should identify sites responsible for extremist agendas and the dissemination of fake news. The security agencies in the country should collaborate with the private sector to design intelligent systems for collecting and analyzing social media data for a specific work environment. Research and development, driven by universities and colleges, on the analytic tools for social media should focus on technologies that filter sensitive information on national security and terrorism. The human and financial capital invested in strategic communication is indicative of the government's dedication to securing the information space. Kenya has already laid the groundwork for the development of strategic communication management systems. The synchronized efforts to mitigate misinformation and online radicalization should foster the development of a constructive cyber and national security vision.

The spread of fake news surrounding COVID-19 on social media reflects the dangerous potential of social media in times of global crisis. Security agencies should adopt measures that track the trend of misinformation through social media and provide alternative and credible sources of accurate information on a threat. While countries continue to deal with the virus, the scourge of fake news embers over an already volatile situation. At times of such calamity, regulation of the spread of information through social networks is critical to the performance of emergency services. In Kenya, the police and emergency responders should embark on an extensive campaign to curb misinformation. COVID-19 is a national security threat, which is exacerbated through rumors and disinformation in the channels of social media. The world needs to unite in managing the information surrounding the virus, to ensure accurate reporting and reassurance of the public afraid of the consequences of the pandemic. The WHO recommends balanced and contextualized reporting based on evidence in order to combat the rumors and misinformation that could hamper the efforts of fighting the current predicament[195].

6.3 Conclusion

Social media has varying effects on national security. When used responsibly it is an essential tool that complements the national security apparatus. However, it is prone to abuse by adversaries who seek to disrupt the governance infrastructure in a country. Kenya has not harnessed the full capabilities of social media in the field of national security. In Africa, social media usage is on the rise and governments are increasingly engaging citizens through online platforms. Similarly, terrorists and other non-state actors are using the platforms to spread propaganda and compromise national security. The readiness of security organs to deal with the online threat is critical in today's world. Developing countries are leading the way in social media monitoring technology and open-source intelligence collection. A country like Kenya shows promise in the digital sphere but still severely lacks in investment and technological expertise. This creates an informational vacuum that impedes the achievement of national security goals.

[195] "Coronavirus Disease 2019 (COVID-19) Situation Report – 35". 2020. *Who.Int*.

The cybersecurity future of Kenya is bright. The government has shown the willingness to adapt and implement social media technology in its operations. This research has shown the counter-propaganda technologies applied in the EU have been successful in hindering terrorism in the continent. Information management is effective in curbing the spread of fake news and extremism. Kenya is still grappling with the issues of fake news, hate speech, and online radicalization. This research paves the way for a more scientific approach to the analysis of social media platforms and their dynamics in the political economies of developing countries. The varying approaches of governments in countering online threats is essential to the growing global informational threat. The future of security will depend on the ability of countries to collaborate and tailor strategies to fit specific national security contexts.

References

"239. National Security Organs - Kenya Law Reform Commission (KLRC)/238. Principles of National Security". 2020. *Klrc.Go.Ke*. http://www.klrc.go.ke/index.php/constitution-of-kenya/155-chapter-fourteen-national-security/.

"Coronavirus Disease 2019 (COVID-19) Situation Report – 35". 2020. *Who.Int*. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200224-sitrep-35-covid-19.pdf?sfvrsn=1ac4218d_2.

"Cyber Security Overview - Communications Authority of Kenya". 2020. *Communications Authority of Kenya*. https://ca.go.ke/industry/cyber-security/overview/.

"Cybersecurity Strategy: Government of Kenya". 2014. *Ict.Go.Ke*. https://www.ict.go.ke/wp-content/uploads/2016/04/GOKCSMP.pdf.

"Microsoft Intelligence Security Report: Volume 23". 2018. *Info.Microsoft.Com*. https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf.

"National Security and Policing Reform | Kenya Vision 2030". 2017. *Vision2030.Go.Ke*. http://vision2030.go.ke/project/national-security-and-policing-reform-2/.

"Security Questions as Kenya Mourns". 2015. *BBC News*. https://www.bbc.com/news/world-africa-32177123.

"Social Media Consumption in Kenya: Trends and Practices". 2018. *SIME Lab*.

"Social Media Directory". 2020. *Department of Homeland Security*. https://www.dhs.gov/social-media-directory.

"Social Media in Africa: A Double-Edged Sword For Security And Development". 2017. *Undp.Org*. https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf.

"Social Media Stats Kenya | Statcounter Global Stats". 2020. *Statcounter Global Stats*. https://gs.statcounter.com/social-media-stats/all/kenya.

"Summary: Truth, Justice and Reconciliation Commission Report". 2013. *Knchr.Org*. https://www.knchr.org/Portals/0/Transitional%20Justice/kenya-tjrc-summary-report-aug-2013.pdf?ver=2018-06-08-100202-027.

A.Mishaal, Dareen, and Emad b Abu-Shana. 2015. "The Effect of Using Social Media in Governments: Framework of Communication Success". *The 7Th International Conference on Information Technology*. doi:10.15849/icit.2015.0069.

Aggarwal, P., P. Arora, and R. Ghai. 2014. "Review on Cyber Crime and Security". *International Journal of Research In Engineering And Applied Sciences* 2 (1):

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election". *Journal of Economic Perspectives* 31 (2): doi:10.1257/jep.31.2.211.

Belova, Gabriela, and Gergana Georgieva. 2018. "Fake News as A Threat to National Security". *International Conference KNOWLEDGE-BASED ORGANIZATION* 24 (1): doi:10.1515/kbo-2018-0002.

Blanken, Leo J, Hy S Rothstein, and Jason J Lepore. 2015. *Assessing War: The Challenge of Measuring Success and Failure*. Washington: Georgetown University Press.

Brelsford, Paul. 2013. "Employing A Social Media Monitoring Tool as An OSINT Platform for Intelligence, Defense & Security."

Carrapico, Helena, and André Barrinha. 2017. "The EU as a Coherent (Cyber)Security Actor?". *JCMS: Journal of Common Market Studies* 55 (6): doi:10.1111/jcms.12575.

Cavelty, M D. 2007. *Cybersecurity and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

Chen, Alan K. 2017. "Free Speech and The Confluence of National Security and Internet Exceptionalism". *Fordham Law Review* 86 (2):

Chesney, Robert, and Danielle K Citron. 2019. "21St Century-Style Truth Decay: Deep Fakes and The Challenge for Privacy, Free Expression, And National Security". *Maryland Law Review* 78 (4):

Chukwuere, Joshua Ebere, and Francis Onyebukwa Chijioke. 2018. "The Impacts of Social Media on National Security: A View from The Northern and South- Eastern Part of Nigeria". *International Review of Management and Marketing* 8 (5). doi:10.32479/irmm.6852.

Confessore, Nicholas. 2018. "Cambridge Analytica And Facebook: The Scandal and The Fallout So Far". *Nytimes.Com*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Couldry, Nick. 2012. *Media, Society, World: Social Theory and Digital Media Practice*. Cambridge: Polity.

Cox, Kate, William Marcellino, Jacopo Bellasio, Antonia Ward, Katerina Galai, Sofia Meranto, and Giacomo Persi Paoli. 2020. "Social Media in Africa: A Double-Edged Sword for Security and Development". *Africa.Undp.Org*. https://www.africa.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf.

Demidov, Oleg. 2012. "Social Networks in International and National Security". *Security Index: A Russian Journal on International Security* 18 (1): doi:10.1080/19934270.2012.634122.

Eltanawy, Nahed, and Julie B Weist. 2011. "Social Media in The Egyptian Revolution: Reconsidering Resource Mobilization Theory". *International Journal of Communication* 5.

Fuchs, Christian, Kees Boersma, and Anders Albrechtslund. 2012. *Internet and Surveillance: The Challenges of Web 2.0 And Social Media*. New York, N.Y: Routledge.

Gunawan, Budi, and Barito M Ratmono. 2020. "Social Media, Cyberhoaxes And National Security: Threats and Protection in Indonesian Cyberspace". *International Journal of Network Security* 22 (1)

Hirschkind, Charles. 2011. "From the Blogosphere to The Street: Social Media and Egyptian Revolution". *Oriente Moderno* 91 (1): doi:10.1163/22138617-09101007.

Jost, John T., Pablo Barberá, Richard Bonneau, Melanie Langer, Megan Metzger, Jonathan Nagler, Joanna Sterling, and Joshua A. Tucker. 2018. "How Social Media Facilitates Political Protest: Information, Motivation, And Social Networks". *Political Psychology* 39: doi:10.1111/pops.12478.

Kaigwa, Mark W. 2013. "Kenya at 50: How Social Media Has Increased the Pace of Change". *The Guardian*. https://www.theguardian.com/global-development-professionals-network/2013/dec/13/kenya-social-media-mark-kaigwa.

Kimotho, Stephen Gichuhi, and Carolyne Nyaboe Nyarang'o. 2019. "Role of Social Media in Terrorism Crisis Communication". *International Journal of Information Systems for Crisis Response and Management* 11 (1): doi:10.4018/ijiscram.2019010104.

Kimutai, J. K. (2014). Social Media and National Security Threats: A Case Study of Kenya.

Koigi, Bob. 2020. "Kenya’s Tweeting Chief Fights Crime and Improves Community Lives | Fairplanet". *Fair Planet*. https://www.fairplanet.org/story/kenyas-tweeting-chief-fights-crime-and-improves-community-lives/.

Korwa, Adar G. 1994. *The Significance of The Legal Principle of Territorial Integrity as The Modal Determinant Of Relations: A Case Study Of Kenya’s Foreign Policy Towards Somalia 1963-1983*. Lanham:University Press of America.

Kothari, C. R. 2004. *Research Methodology: Methods and Techniques.* 2nd ed. New Delhi: New Age International (P) Ltd.

Lee, Newton. 2015. *Counterterrorism and Cybersecurity: Total Information Awareness*. 2nd ed. Cham: Springer.

Lerner, Jennifer S. 2019. "Decision Science Meets National Security: A Personal Perspective". *Perspectives on Psychological Science* 14 (1): doi:10.1177/1745691618815822.

Makinen, Maarit, and Mary Wangu Kuira. 2008. "Social Media and Post-Election Crisis in Kenya". *Information & Communication Technology - Africa* 13. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1012&context=ictafrica.

Mälksoo, Maria. 2018. "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of The EU And NATO". *European Security* 27 (3): doi:10.1080/09662839.2018.1497984.

Marcellino, William, Meagan L Smith, Christopher Paul, and Lauren Skrabala. 2020. "Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations". *Rand.Org*. https://www.rand.org/pubs/research_reports/RR1742.html.

Mellen, Roger P. 2012. "Modern Arab Uprisings and Social Media: An Historical Perspective on Media and Revolution". *Explorations in Media Ecology* 11 (2): doi:10.1386/eme.11.2.115_1.

Meloy, J. Reid, Alasdair M. Goodwill, M. J. Meloy, Gwyn Amat, Maria Martinez, and Melinda Morgan. 2019. "Some TRAP-18 Indicators Discriminate Between Terrorist Attackers and Other Subjects of National Security Concern.". *Journal of Threat Assessment and Management* 6 (2): 93-110. doi:10.1037/tam0000119.

Molony, Thomas. 2018. "Social Media Warfare and Kenya's Conflict with Al Shabab In Somalia: A Right to Know?". *African Affairs* 118 (471): doi:10.1093/afraf/ady035.

Montagnese, Capt. CC Alfonso. 2012. "Impact of Social Media on National Security". *Difesa.It*. http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Documents/Ricerche/2012/Stepi/social_media_20120313_0856.pdf.

Moreno, Megan A, and Rosalind Koff. 2015. "11. Media Theories and The Facebook Influence Model". *The Psychology of Social Networking Vol.1*. doi:10.1515/9783110473780-013.

Muendo, Mercy. 2018. "Kenya's New Cybercrime Law Opens the Door to Privacy Violations, Censorship". *The Conversation*. https://theconversation.com/kenyas-new-cybercrime-law-opens-the-door-to-privacy-violations-censorship-97271.

Ndlela, Martin N., and Abraham Mulwo. 2017. "Social Media, Youth and Everyday Life In Kenya". *Journal of African Media Studies* 9 (2): doi:10.1386/jams.9.2.277_1.

Nyambuga, Charles. 2014. "The Influence of Social Media on Youth Leisure in Rongo University". *Journal of Mass Communication & Journalism* 04 (09). doi:10.4172/2165-7912.1000223.

Nzau, Mumo, and Mohammed Guyo. 2018. "The Challenge of Securing Kenya: Past Experience, Present Challenges and Future Prospects". *The Journal of Social Encounters* 2 (1).

Ördén, Hedvig. 2019. "Deferring Substance: EU Policy and The Information Threat". *Intelligence and National Security* 34 (3): doi:10.1080/02684527.2019.1553706.

Parlakkılıç, Alaattin. 2018. "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach". *International Journal of Information Security Science* 7 (4):

Ramona, Diana L, and Liana M Marcu. 2016. "Social Media Platforms as A Tool for Sharing Emotions. A Perspective Upon the National Security Agencies". *Management Dynamics in The Knowledge Economy* 4 (1):

Reuter, Christian, Amanda Lee Hughes, and Marc-André Kaufhold. 2018. "Social Media In Crisis Management: An Evaluation And Analysis Of Crisis Informatics Research". *International Journal of Human–Computer Interaction* 34 (4): doi:10.1080/10447318.2018.1427832.

Simon, Tomer, Avishay Goldberg, Limor Aharonson-Daniel, Dmitry Leykin, and Bruria Adini. 2014. "Twitter in The Cross Fire—The Use of Social Media in The Westgate Mall Terror Attack in Kenya". *Plos ONE* 9 (8): e104136. doi: 10.1371/journal.pone.0104136.

Tufekci, Zeynep, and Christopher Wilson. 2012. "Social Media and The Decision to Participate in Political Protest: Observations from Tahrir Square". *Journal Of Communication* 62 (2): doi:10.1111/j.1460-2466.2012.01629.x.

Unpublished MAThesis: University of Nairobi.

Volkin, Samuel. 2020. "Social Media Fuels Spread Of COVID-19 Information—And Misinformation". *The Hub*. https://hub.jhu.edu/2020/03/27/mark-dredze-social-media-misinformation/.

Walsh, James P. 2019. "Social Media and Border Security: Twitter Use by Migration Policing Agencies". *Policing and Society,* 1-19. doi:10.1080/10439463.2019.1666846.

Wyche, Susan P., Sarita Yardi Schoenebeck, and Andrea Forte. 2013. "“Facebook Is A Luxury”: An Exploratory Study of Social Media Use in Rural Kenya". *Computer Supported Cooperative Work - CSCW '13*. doi:10.1145/2441776.2441783.

Zhang, Zhiyong, and Brij B. Gupta. 2018. "Social Media Security and Trustworthiness: Overview and New Direction". *Future Generation Computer Systems* 86: 914-925. doi:10.1016/j.future.2016.10.007.

Appendix 1: Questionnaire

Part A: Demographic (Tick as appropriate)

1. Age
   - a. 21-30 ( )
   - b. 31-45 ( )
   - c. 46-60 ( )
2. Gender
   - a. Male ( )
   - b. Female( )
3. Education Level
   - a. High School Graduate ( )
   - b. College/University Graduate ( )
   - c. Post Graduate ( )

Part B: Nature of Social Media in Kenya

1. Do you have a social media account? Yes ( ) No ( )
2. List the top five social media platforms you use, in order of frequency.
   - a. ………………………………………………………………………..
   - b. ………………………………………………………………………..
   - c. ………………………………………………………………………..
   - d. ………………………………………………………………………..
   - e. ………………………………………………………………………..
3. How do you access social media? (Select all appropriate responses)
   - a. Through mobile phone [ ]
   - b. Through laptop [ ]
   - c. Office computer [ ]
   - d. Public Wi-Fi [ ]
   - e. Home internet [ ]

4. What activities do you conduct on social media daily? (Rank in order of frequency)

a. ………………………………………………………………………………….

b. ………………………………………………………………………………….

c. ………………………………………………………………………………….

d. ………………………………………………………………………………….

e. ………………………………………………………………………………….

5. Do you think social media use in Kenya is well regulated? Yes ( ) No ( )
Please specify.

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

Part C: Advantages and Disadvantages of Social Media to National Security

1. From your experience, list five advantages and five disadvantages of social media use

ADVANTAGES	DISADVANTAGES
a.	
b.	
c.	
d.	
e.	

2. How would you categorize the impact of social media on national security?

a. Not significant ( )

b. Mildly significant ( )

c. Neutral ( )

d. Significant ( )

e. Very significant ( )

3. Have you encountered any fake news on social media? Yes ( ) No ( )

4. Can you differentiate between fake and real news while on social media?

Yes ( ) No ( )

5. Have you witnessed any cases of cyber bullying on social media? Yes ( ) No ( )

If yes, specify. (No details needed)

……………………………………………………………………………………………

……………………………………………………………………………………………

6. Is the government doing enough to curb the spread of fake news?

( ) Yes ( ) No

7. What is your opinion on the strategies needed to combat fake news and misinformation in Kenya?

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

…………………………………………………………………………………………..

Part D: Use of Social Media and its Impact on National Security

1. Rate Kenya's state of national security in relation to threats from social media. (A scale of 0-5, 5 being excellent and 0 being very poor)……………………………………….

2. Classify each of the following national security threats based on the contribution of social media.

	No Impact	Limited Impact	Neutral	Great Impact	Very Great Impact
Terrorism					
Cattle Rustling					
Poaching					
Information Warfare					
Hate Speech					

3. Provide suggestions on how to improve the state of national security in Kenya through social media.

……………………………………………………………………………………………

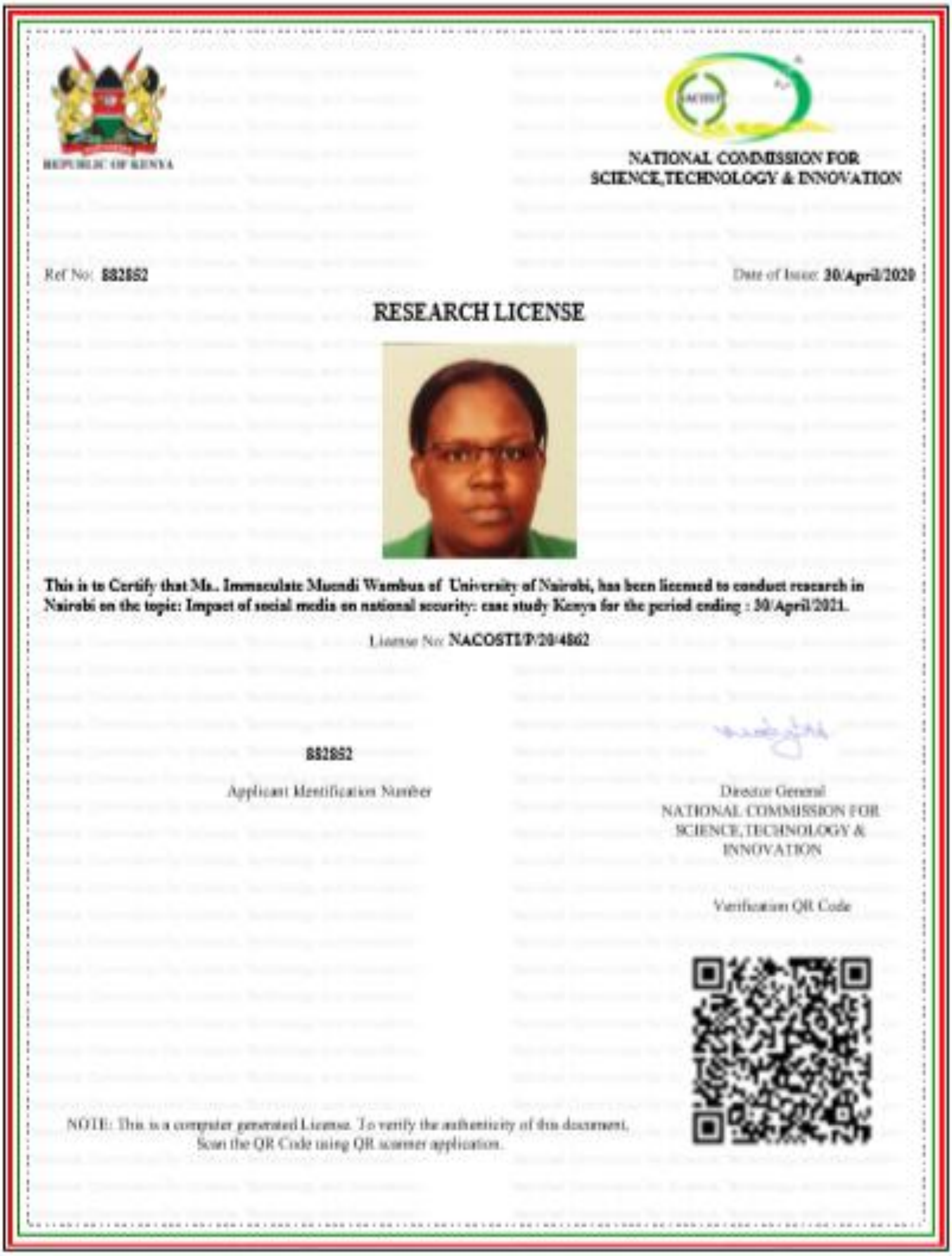
……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

4. Do you think the security agencies in Kenya have the capability to effectively monitor social media for national security purposes? Yes ( ) No ( )

Appendix 2: Research Permit



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **882852**

Date of Issue: **30/April/2020**

RESEARCH LICENSE

This is to Certify that Ms.. Immaculate Muendi Wambua of University of Nairobi, has been licensed to conduct research in Nairobi on the topic: Impact of social media on national security: case study Kenya for the period ending : 30/April/2021.

License No: **NACOSTI/P/20/4862**

882852

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY &
INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.