UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

IMPACT OF SOCIAL MEDIA ON NATIONAL SECURITY IN KENYA

NAME: JOSEPH VALA MBITHI

REG NO: R47/41716/2022

SUPERVISOR: DR P M MALUKI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF POST GRADUATE DIPLOMA

DATE OF SUBMISSION: SEPTEMBER, 2022

ii

DECLARATION

This research project which I now submit for assessment on the programme of study leading to the award of post graduate diploma is my original work and has not been subjected for research and examination of any other institution of higher learning.

Signature..

Date....06/09/2022..........................

Joseph Mbithi Vala

This research project has been submitted for examination with my approval as the institute's supervisor.

Signature...

Date....15/9/2022..............................

Dr. Patrick Maluki

University of Nairobi

DEDICATION

This research project is dedicated to my family for their support, understanding and encouragement during my studies.

ACKNOWLEDGEMENT

This work has been dependent on the support and contributions from several people. These people have through their commitment, encouragement, constructive criticism and support helped me through the journey to write this project.

I would like to start to thank all individuals at the college that have supported this work through sharing their time, knowledge and interest. Without you this research would not have been possible.

I would like to express my gratitude to my supervisor Dr Patrick Maluki. Through your hard work, you have helped me to turn my work into something worthy to defend and without your guidance and valuable comments, this project would not have been completed.

To my friends and my family thank you for always being there and for making sure that there is more to life than work. Each of you is very special and dear to me and would have liked to mention you all here. But I want you to know that without you I would not have been half as happy as I am.

Anne, my wonderful and supportive wife my warmest thanks to you, for being you and always taking care of me. You have made me understand that there is no meaning running through life and you make me see the joy in everyday events. I love you. Marcus, Marlene and Mandy I would like to thank you for all the joy and love you bring to my life. I love you too. God bless you all.

TABLE OF CONTENTS

ABSTRACT

Kenya is not immune to the dynamics of social media in terms of its use and abuse as a member of the international community. The government and military must deal with severe security and privacy risks raised by the use of social media as a new mode of communication, as well as new cyber-attack vectors. Criminal gangs, terrorist organizations, bad-faith non-state players, and rebellious elements, such as Al-Qaeda and Al-Shabaab, often use social media platforms to disseminate propaganda with the explicit goal of getting to, recruitment, and radicalization of their intended audience. This study aimed at examining the growth of social media in Kenya and its positive effects on security; examining the negative effects of social media on national security and investigating the efforts that the government of Kenya has put in place to deal with threats caused by social media. The study used two theories: the social responsibility theory and the Technological Determinism Theory. The study aimed at answering the following hypothesis: Social media which has well been utilized and can be used to prevent threats to national security and bring peace and growth to a nation and social media if not well controlled it can affect the security of the state negatively. This study was based on a search of publications and papers on the dangers posed by social media in Kenya on the internet. The threats that social media pose to Kenya's national security were examined using a combination of limited literature and documentary evidence. A search for "social media and national security in Kenya," "social media risks in Kenya," and "social media regulation in Kenya" were conducted using Google Chrome. To examine qualitative data, thematic or content analysis was used. The contents of the data were summarized, and this information was utilized to begin the analysis. In order to make conclusions, the similarities and discrepancies in secondary data will be evaluated. According to the findings, over the years the dominance of social media in Kenya has continued to grow and its presence can no longer be ignored. As observed, Social media can be viewed as a double-edged sword not only in Kenya but the entire globe. Positively: Users may quickly connect with one another through social media platforms, which allow them to share various types of material such as videos, photographs, graphics, messages, and sounds, among other things. Social media also aids in the formation and strengthening of numerous networks, including professional, social, cultural, religious, family and political ones, as well as the development and definition of social identities. Terrorist attacks, hacking, sensitive data leaks, cyber bullying, cyber fraud and money laundering, cattle raiding, illegal hunting, tribal confrontations, information warfare, and hate speech are all negative examples. As a result, the research suggests that security apparatus establish automated methods for collecting and evaluating social media that are adapted to certain work contexts. The government of Kenya needs to ensure that the policies that are already in place concerning social media and internet security are fully enforced in order to ensure the perpetrators are fully prosecuted and brought to justice.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

For many years, the growth from print to radio of the media to television to now internet media has influenced public opinion and views.[1] However, the rise of social media sites like Twitter, YouTube and Facebook has taken this concept even further, with some claiming that social media now shapes the opinions, perceptions, and the majority's behavior, whose views had previously been formed by information from conventional and mainstream media outlets.

The potential to create quick communication experiences is underpinned by today's web and new media. A news announcement may go from zero to 20 million views overnight using Twitter, YouTube and Facebook and a collection of blogs. The highly social, user-driven environment's viral nature allows total strangers to join over shared views, desires, or hobbies, and together produce winners and losers.[2]

Our technical achievements in the field of ICT have helped transcend limits of time and distance in communication, information sharing, and networking in what we denote to as the "information age" or "digital era." This has an impact not just on how we engage with others and do business, but also on how we operate in the political arena. Anybody can use media to pass information to the target recipient. The information can be positive or negative. This freedom has given chance to terror groups who are also able to access these platforms. Many questions hence go un-answered. Is it true that providing free access to a wide range of information on the internet increases accountability and transparency? Is the proliferation of unfiltered information leading to more confusion, populism, defamation, and hate speech, or is it leading to more confusion, populism, defamation, and hate speech? The harmful effects of social media on Kenya's national security are investigated in this research.

1.1 Background of the Study

Globally, there is a huge demand for social media by all segments in the society, particularly the youthful generation.[3] Social media has a number of drawbacks that have impacted important sectors, one of which is national security. The facilitation of terrorism is one way that social media

[1] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

[2] Wambua, Immaculate M. "Impact of Social Media on National Security in Africa: Case Study Kenya." PhD diss., University of Nairobi, 2020.

[3] Nmah, Othello N. *Effects of Social Media on National Security*. US Army Command and General Staff College Fort Leavenworth United States, 2019.

has harmed security. Terrorist organizations utilize social media platforms for communication, recruiting, and training, as well as instruments for ideological radicalization, in the contemporary period. Terrorist organizations also use social media platforms to communicate with other criminals, such as cybercrime gangs, and to plot illicit acts including kidnappings, drug trafficking, and weapon trade. Islamic jihadists are the most recent terrorist groups to use social media to aid their activities. For recruitment and support, these organizations mostly use Facebook and YouTube channels, especially in the west. [4]

All of these actions endanger peace and jeopardize a country's national security. Criminal gangs operating both inside and outside of a specific nation use social media platforms in a similar way to gain support, communicate, and organize their unlawful actions. Another way that social media might harm national security is via the dissemination of propaganda.[5] The rise of social networking sites complements the use of other media such as television, newspapers, and radio to disseminate propaganda and influence deception operations, all of which jeopardizes a country's security. By the same token, protest movements and revolutionists utilize social media platforms to mobilize the masses. In such a case, these sites are used to better unify, organize and spur masses to action, to arrange demonstrations and to coordinate their tactical and operational aspects. [6]

Through use of social media platforms, the revolutionary groups are able to cut on organization, participation, recruitment and training. As a result, these groups are able to propagate their operations which in turn negatively impacts on national security. When social media platforms are used to disseminate and distribute secret, classified, or sensitive information or material, they may have an influence on national security. While individuals should have the right to communicate and express themselves, this should not extend beyond the requirement to protect the integrity and secrecy of secret information in order to protect a country's security.

1.2 Statement of Problem

Kenya is not immune to the dynamics of social media in terms of its use and abuse as a member of the international community. The government and military must deal with severe security and privacy risks raised by the use of social media as a new mode of communication, as well as new

[4] Marima, Tendai. "Zimbabwe: Social media as a toxic tool or a future bridge to peace." In *Social Media Impacts on Conflict and Democracy*, pp. 205-215. Routledge, 2021.

[5] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

[6] Marima, Tendai. "Zimbabwe: Social media as a toxic tool or a future bridge to peace." In *Social Media Impacts on Conflict and Democracy*, pp. 205-215. Routledge, 2021.

cyber-attack vectors. Criminal gangs, terrorist organizations, bad-faith non-state actors, and subversive elements, such as Al-Qaeda and Al-Shabaab, often use social media platforms to disseminate propaganda with the explicit goal of getting to, recruiting, and radicalizing their target audience. People use social media to spread fearful, nasty, and false information about the state of national security issues. Because the bulk of social media users stick together, law enforcement agencies have a tough time tracking them down and prosecuting them. As a consequence, nations have tremendous challenges in tracking, regulating, and controlling social media usage and exploitation in connection to state security.[7]

Monitoring social media conversations and material, and putting in place efficient counter-propaganda and interference strategies, boosting a state's geopolitical position and international reputation through improving the effectiveness of government ministries and entities are all part of a national security strategy. Such programs, however, need sophisticated technology that are both complicated and costly for third-world countries. Social media poses significant dangers to national security and has adverse repercussions. To safeguard Kenya's freedom, security, and prosperity, some serious research should be conducted on how the government might utilize online social networking technologies while also monitoring them in the event that they pose a threat to national security. The military and other security services, like any other national security problem, need to understand how social media undermines national security. It’s against this background that this study investigates how social media threatens national security, with specific reference to Kenya.

1.3 Research Questions

1. To what extent has social media grown in Kenya and how has it positively affected national security?
2. What are the negative effects of social media on national security?
3. What efforts has the government of Kenya put in place in order to deal with threats caused by social media?

1.4 Objectives of the Study

1. To examine the growth of social media in Kenya and its positive effects on security
2. To determine the negative effects of social media on national security.

[7] Bradshaw, Samantha, and Philip N. Howard. "Online Supplement to Working Paper 2018.1 Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." (2018).

3. To analyze the efforts that the government of Kenya has put in place in order to deal with threats caused by social media

1.5 Literature Review

Better and enhanced communication methods have emerged as a result of current technological advancements.[8] The way people communicate and exchange information throughout the globe has changed as a result of this. While contemporary communication technologies, especially social media, have many advantages, they have also become a huge national security threat. [9] This is due to the fact that criminal gangs and terrorist groups have been utilizing social media platforms to gain support and organize their activities in recent years. Individuals use social media platforms to conduct cybercrime and to disseminate misleading information and hate messages to the general population about the condition of national security issues, in addition to terrorist groups and criminal gangs.

Most of the time, the perpetrators of such crimes stay at large since they are difficult to track down by law enforcement authorities and prosecute. As a result, security agencies have a lot of trouble tracking, surveilling, and governing the use and exploitation of the platforms in context of national security. All of this has had an influence on national security in a number of nations throughout the globe. [10]

Stringent regulatory measures are essential due to the negative consequences of social media. As a result, developing a strategy to monitor interactions and communication on social media networks is critical for countering adversary propaganda and interferences, improving the performance of state agencies and institutions, and reinforcing a country's geopolitical position and international credibility. While these measures have the potential to greatly enhance national security, they need sophisticated technology, money, and understanding, which most countries, including Kenya, lack. The country, as one of the countries that has seen remarkable development in information and communication technology, is not immune to the powers of social media.

[8] Marima, Tendai. "Zimbabwe: Social media as a toxic tool or a future bridge to peace." In *Social Media Impacts on Conflict and Democracy*, pp. 205-215. Routledge, 2021.

[9] Bradshaw, Samantha, and Philip N. Howard. "Online Supplement to Working Paper 2018.1 Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." (2018).

[10] Ogola, George. "Social media as a heteroglossic discursive space and Kenya's emergent alternative/citizen experiment." *African Journalism Studies* 36, no. 4 (2015): 66-81.

1.5.1 Social Media

Social media is a computer-based technology that makes it easier for people to share ideas, points of view, and information by setting up virtual networks and groups.[11] Because social media is supposed to be Internet-based by its very nature, individuals may easily transmit content utilizing electronic means. Among the objects in the collection are personal documents, papers, films, and pictures. Web-based software and apps are used by users to engage with social media on a computer, tablet, or smartphone. People may produce and transmit information, ideas, career interests, and other forms of expression with one another via virtual communities and networks, such as social media. While the wide number of standalone and built-in social media services available today makes categorizing social media exceedingly challenging, there are few characteristics that all of them share: The phrase "Web 2.0" refers to interactive Internet-based applications. User-generated content is the heart of social media. This could be written articles or comments, digital photos or videos, and gathered data from all of a person's interactions with social media. Users can set up service-specific profiles on the site. The social media company then develops and manages these profiles. Users can build online social networks by integrating their own profiles with the profiles of other people or groups. This makes it easier to build online social networks.[12]

Social media is used a lot in the United States and Europe, but in countries like Indonesia, it's used the most. Around 3.8 billion people use social media. During the previous two decades, social media has become a global phenomenon. This shift is particularly noticeable among young people, who cannot imagine interacting without the use of social media platforms such as Facebook, Google+, and Twitter. Social media is extensively utilized, and it has both beneficial and harmful aspects in various ways.[13]

Positively, technology allows for instant worldwide communication, connects remote places to civilization, aids e-commerce, and contributes to the democratic process. “Users of the world, unite: The challenges and opportunities of Social Media,” by Andreas M. Kaplan and Michael Haenlein, defined social media as “a collection of Internet-based apps that build on the ideological

[11] Njamuku, Solomon M. "The Impact of Post 9/11 Film and TV Content on the National Security of Weak States: a Case Study of Kenya." PhD diss., University of Nairobi, 2016.

[12] Kaigwa, Mark. "From cyber café to smartphone: Kenya’s social media lens zooms in on the country and out to the world." *Digital Kenya. An Entrepreneurial Revolution in the Making. London: Palgrave Macmillan* (2017): 187-222.

[13] Nothias, Toussaint, and David Cheruiyot. "A “hotbed” of digital empowerment? Media criticism in Kenya between playful engagement and co-option." *International Journal of Communication* 13 (2019): 24.

underpinnings of Web 2.0, and that allow the production and sharing of user-generated content," "Traditionally, people utilized the internet to consume content: they read, watched, and used it to buy things and services," they continued. In line with this understanding, there is a clear difference between traditional media like print or broadcasting where users are more passive consumers and social media. New information equipment, varying behavior in how it is used, and the growing anxieties of information seekers have further expanded the ways individuals and groups engage in the new era of the "many to many" exchange process. [14]

Negatively, with all of the advances, information users have lost control of the information flow and content. Whether he or she is a business or non-profit organization, a politician, or a Chief Executive Officer, one must react to what "the many," the online crowd, is asking.

1.5.2 National Security

The protection and defense of a nation state, including its population, economy, and institutions, is considered a government obligation. The conventional notion of national security emphasized the development of a defense and security staff as well as the acquisition of weapon systems that a state might deploy to respond to and defeat adversaries. In Kenya, national security refers to the protection of Kenya's sovereignty and integrity of its territory, its people as well as their rights, property, freedoms, peace, prosperity and stability as well as other national interests, against both internal and external threats. The following principles will be used to enhance and ensure Kenya's national security: (a) this Constitution and Parliament have jurisdiction for national security, (b) the pursuit of national security must be done in conformity with the law and with the greatest regard for the rule of law, democracy, human rights, and basic freedoms. (c) in carrying out their functions; and (e) in carrying out their responsibilities.[15]

Individuals, political bodies, human associations, and social groupings that make up a nation's security interest are grouped together as national security. The research employs a wide definition of national security, which is defined as the sum of all measures made to safeguard a nation's sovereignty and treasured values. It raises people's living levels while also ensuring that all citizens are free from all types of harm to their lives and property. Natural or man-made calamities are also protected by national security.

[14] Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and national security*. Potomac Books, Inc., 2009.

[15] Wolfers, Arnold. "" National security" as an ambiguous symbol." *Political science quarterly* 67, no. 4 (1952): 481-502.

1.5.3 Social Media and National Security

Due to their mobility and flexibility, as well as their cheap cost, social media are linking and mass communication technologies with a worldwide reach and an ever-increasing degree of usage.[16] The social media (SM) platform has revolutionized peer-to-peer, business-to-business, government-to-government engagement, and so on. Globally, social media platforms are being utilized to advance social and national instability. The twentieth century began with the most symmetric and kinetic wars in history, whereas the twenty-first century began with a plethora of asymmetric and non-kinetic battles. Hundreds of thousands of people died in the First World War for a few yards of physical terrain. However, state and non-state actors are already using multiplex designs in order to gain control of major areas of cyberspace, which has ramifications in the physical realm. These players may now expand their dominance in the social media realm at a size and complexity that was previously considered inconceivable. Social media is a technological life force that has the ability to not only connect, inspire, enlighten, educate, and pleasure people, but also to maim them.[17]

For Kenyans, their government, and national security services like the military and police, social media platforms have far-reaching social and security consequences.[18] To safeguard Kenya's freedom, security, and prosperity, some serious research should be conducted on how the government might utilize online social networking technologies while also monitoring them in the event that they pose a threat to national security.

1.5.4 The Growth of Social Media in Kenya and its Positive Effects on Security

National security in many nations has lagged as the internet and social media continue to expand and change, particularly in most third-world countries. The advent of technical advancements has been heralded as a window of opportunity that, if properly used, will play a key role in finding answers to the problems that are stifling social growth. The importance of ICT in achieving the important pillars of the national development agenda is outlined in Vision 2030. Facebook, Whatsapp, Twitter, and Instagram are some of the most commonly used social media platforms

[16] Sykora, Martin D., Thomas W. Jackson, Ann OBrien, and Suzanne Elayan. "National security and social media monitoring: A presentation of the emotive and related systems." In *2013 European Intelligence and Security Informatics Conference*, pp. 172-175. IEEE, 2013.

[17] Chen, Yu. "Research on Social Media Network and National Security." In *Informatics and Management Science II*, pp. 593-599. Springer, London, 2013.

[18] Thompson, Robin. "Radicalization and the use of social media." *Journal of strategic security* 4, no. 4 (2011): 167-190.

in Kenya, and they are revolutionizing communication and other aspects of the person, community, and country.[19]

Security agencies utilize social media to avoid, control, and eliminate risks to national security; state security agencies use social media platforms to improve national security. They primarily utilize social media to engage with the general public, gather open source information, promote public diplomacy, and combat propaganda. The Kenya Police Service and the DCI are two of the most visible government entities on social media. These bodies mainly use twitter handles to inform the public on security issues and they offer a suitable platform to the public where they can air their opinions and where they can report crimes. A large proportion of the respondents reported that there are bodies that are charged with the responsibility of social media content with Communication Authority of Kenya being in the frontline. However, concerns were raided that not much has been done when it comes to monitoring of social media content since most of these sites are still misused to facilitate criminal activities and there are numerous cases of cybercrime cases.[20]

1.5.5 The Negative Effects of Social Media on National Security

Experts and politicians in national security must now adjust fast to evolving dangers or risk severe national security breaches. Recent occurrences throughout the globe have shown that social media may be used to undermine national security. Social media may be used to expand common space, but it can also be used to destabilize it.

Social media is as easily adaptable to support diffusing propaganda, prejudicial related speech, and violence inciting content. Any discussion of the function of social media must thus include a discussion of the relationship between information flows and a state's stability. It is amply evident that unconstrained social media could present security risks to nations. Non-state actors such as terrorist groups and unscrupulous individuals are now using social media to export hate messages. Groups like Boko Haram in the western African region are using Facebook and other platforms as conduits to recruit fighters and increase its support base. In addition to using these platforms for

[19] Bradshaw, Samantha, and Philip N. Howard. "Online Supplement to Working Paper 2018.1 Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." (2018).

[20] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

recruitment purposes, these groups and individuals are effectively using this medium for propaganda activities to create panic.[21]

Social media platform is also used to conduct criminal activities. This website is used by criminal organizations to communicate information and organize unlawful actions. Among the illicit acts that take place over the internet include child pornography, virtual identity theft, spoofing, drug dealing, the spread of computer viruses, human trafficking, financial fraud, and the transmission of data from industrial espionage.[22] People are sharing personal and private information through social media without permission, like in print, audio, and picture. This is not illegal, but it is becoming more common. These actions could put the country's security at risk.

1.5.6 Efforts that Government of Kenya has put in Place to deal with Threats caused by Social Media

Governments throughout the globe, as well as social media corporations, are now engaged in a heated discussion over how to regulate social media platforms. The government plays a critical role in creating regulations to guarantee that information published on social media platforms meets public decency standards. When objectionable information is discovered to be in violation of state legislation, the government takes action to remove it from social networking networks. The public and social media firms cannot take their obligations seriously without such restrictions. Because social media firms have such a large influence over what is conveyed in cyberspace, they are assuming responsibility for their material by preventing the spread of misinformation and incorrect information. Facebook, for example, expressly discourages and prohibits hate speech. Facebook's purpose is to provide possibilities for individuals to form personal bonds while also bringing the globe closer together. To do so, Facebook bans hate speech, which includes any content that publicly attacks someone for their colour, ethnicity, national origin, religious preference, sexuality, or gender identity, as well as significant physical defects or diseases.

1.6 Justification of the Study

This study is critical because it provides a deeper understanding of social media’s role in promoting terrorist and criminal activities. Since the rapid growth of social media, terrorists, and terrorist organizations, including criminal networks, have increased their activities. Social media

[21] Bradshaw, Samantha, and Philip N. Howard. "Online Supplement to Working Paper 2018.1 Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." (2018).

[22] Ibid p.56

platforms give terrorists and criminals easy access to potential adherents and victims. Additionally, this study will offer some crucial strategies that decisions makers can employ to enhance national security.

1.7 Theoretical Framework

This research is supported by a robust theoretical foundation. The social responsibility theory is one of the theories.[23] The media, as per the social responsibility theory, has an important part in serving the public interest and, in order to do so, it must be free of all types of manipulation. According to this view, well-defined principles should be in place to ensure that the media performs its responsibility of keeping the public informed. Both the media and the customers must be socially accountable, according to the notion. [24]

As a consequence, if both the media and the general population become more socially responsible, the government will find it simpler to establish regulatory frameworks. Technological Determinism Idea is another theory that underpins this research.[25] According to the theory, as technology and people's behavior evolve, media technologies impact how society functions. This theory describes how information is consumed, retrieved, and transmitted in contemporary society as a result of Information Communication Technologies. The hypothesis is based on the idea that changes in communication modalities influence the path of history to a considerable degree. The social information frenzy is seen as a direct effect of the explosion of data made possible by information and communication technologies, according to the notion.

1.8 Hypotheses of the Study

The study aims at answering the following hypotheses

i. A proper controlled Social media can be used to prevent threats to national security which in turn bring peace and growth to a nation.

ii. Social media if not well controlled it can affect the security of the state negatively.

iii. Government has not taken enough measures against the security threats posed by social media.

[23] Nerone, John C. *Social responsibility theory*. na, 2002.

[24] Windsor, Duane. "Corporate social responsibility: Three key approaches." *Journal of management studies* 43, no. 1 (2006): 93-114.

[25] Bimber, Bruce. "Karl Marx and the three faces of technological determinism." *Social studies of science* 20, no. 2 (1990): 333-351.

1.9 Methodology

1.9.1 Study Design

In this study, the exploratory study approach was employed to conduct a thorough investigation of the relationship between social media usage and national security. Exploratory design is quite simple to comprehend and explain. Furthermore, data acquired via exploratory design may be easily used to identify possible explanations and provide conceptual models of these correlations.

1.9.2 Study Site

The study was carried out in Nairobi County. This is because Nairobi is the capital city of Kenya hence hosting the biggest population and especially social media users. In additions it's one of the most affected cities by the terrorist groups which use social media to carry out their agendas.

1.9.3 Target Population

The whole collection of things or a group of persons from whom the researcher seeks to collect data is the target population. The study's target group included members of the general public as well as personnel of Kenya's Communications Authority, National Cohesion and Integration Commission (NCIC) official, Directorate of Criminal Investigation official, and an official from the National Intelligence Service.

1.9.4 Data Collection Methods

The study used secondary data. This study was based on a search of publications and papers on the dangers posed by social media in Kenya on the internet. On Google Chrome, a search for "social media and national security in Kenya," "social media dangers in Kenya," and "social media regulation in Kenya" was done.

1.9.5 Data Analysis and Presentation

To examine qualitative data, thematic or content analysis was used. The contents of the data were summarized, and this information was utilized to begin the analysis. In order to make conclusions, the similarities and discrepancies in secondary data was evaluated.

1.9.6 Ethical Considerations

Ethics are important in research because they spell norms that guide any research activity, particularly the way researchers will gain authorization to collect data and the behavior expected from them in the field. During the process of data collection, informed consent will be the mainstream criteria of each respondent participating in the study. In addition, the researcher ensured that the respondents and the organizations are protected by keeping their identity and all the information gathered confidential. Before data collection permission was sought National Commission for Science, Technology & Innovation (NACOSTI). The research ensured that the project had the minimal percentage of plagiarism as required by the university. That means the work was unique and has never been submitted to any other university.

1.10 Scope and Limitations of the Research

The study provided a view of the current in terms of state, movement, terrorist groups, crime syndicates, and individual usage of social media, as well as how it affects national security.

1.11 Chapter Outline

Chapter one: presents the introduction which entails: the background of the study; statement of problem, objectives of the study, research questions, literature review, theoretical framework, methodology, and justification of the study and chapter outline.

Chapter two: will discuss the growth of social media in Kenya and its effects on security

Chapter three: will analyze the negative effects of social media on national security.

Chapter four: analyze the efforts that the government of Kenya has put in place in order to deal with threats caused by social media

Chapter five: will present the conclusion and recommendations

CHAPTER TWO

THE GROWTH OF SOCIAL MEDIA IN KENYA AND ITS POSITIVE EFFECTS ON SECURITY

2.0 Introduction

The Nailab and iHub in Kenya, AppLab and Hive Colab in Uganda, BantaLabs in Senegal, Cameroon's ActiveSpaces in addition to Tanzania's Kinu are among the continent's technology hubs that are providing new venues for collaboration, innovation, training, software and content production. These new technology centers are being used by African companies and governments to assist drive advances in the agricultural and financial sectors, as well as advancements in climate change, education, and healthcare policy.[26]

The dramatic increase in mobile phone usage, according to experts, is the technical advance with the largest influence on the continent. Between 2000 and 2011, Africa's mobile phone market grew at the highest rate in the world, from 10 million to 647 million users.[27] In Africa, demand for mobile phones continues to rise, owing to the low cost of mobile services. The mobile phone market is claimed to have a larger expanding effect on per capita income in Africa than other communication technologies such as fixed telephone main lines. Mobile phones are stated to be used in Africa to maintain family and friend networks, to conduct mobile banking, to compare market pricing, to gather health data, to advertise, and to locate employment. Furthermore, the fast increase of social media usage across the continent has been facilitated by the widespread availability of mobile phones.

However, in Africa, the rise of social media has proved to be a double-edged sword. While social media has aided economic growth and increased political participation, it has also had a number of unfavorable consequences, such as providing terrorist organizations with an easily available medium to spread their message and recruit adherents.

Twitter, WhatsApp, Facebook, Skype, blogs, MySpace, YouTube, Instagram, and Weechat are examples of social media platforms. In the topic of governance and ethics, social media is now gaining traction. Governance and ethics need a high level of principled attention to other people's rights. On the one hand, good governance is concerned with striking a balance between policies

[26] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

[27] Wambua, Immaculate M. "Impact of Social Media on National Security in Africa: Case Study Kenya." PhD diss., University of Nairobi, 2020.

and people' respect and duty. This equilibrium is critical because good governance and good ethics go hand in hand.

This chapter seeks to analyze the extent to which social media has grown in Kenya and how this growth positively affects security. Security in this session is associated with growth in business, job creation (employment), peace especially political peace, good communication, good and acceptable governance among others.[28]

2.1 Social Media as a Force for Good

Kenyan social media has also contributed significantly to the continent's economic prosperity. The government has used and may continue to utilize social media as a warning or trend prevention tool in networking sites. When utilized as a monitoring tool, security services are able to detect the earliest indicators of any hostile or potentially dangerous conduct and take the appropriate countermeasures. This may be accomplished by collecting and analyzing communications and other material published on social media, which aids in the detection and prevention of events that might jeopardize national security. [29]

The government could employ social media for defense reasons including preventive, detection, forecasting, organizational interaction, crisis response, and counter-propaganda. Furthermore, since social media users leave traces of their identities, abilities, predilections, movements, relationships, and other qualities that can be easily retrieved and assessed, the government may be able to exploit social media as a valuable source of information.[30] Increased use of social media in Africa has elevated citizens' awareness of political developments, changing perspectives both locally and internationally, and providing a voice to "less celebrated actors" in international and local dialogue. Increased Twitter usage in Kenya, for example, is thought to be connected to residents' desire to challenge the foreign media's distortion of violence and election campaigns.

Twitter, unlike other platforms, is readily accessed through mobile phone and may provide regular folks with a voice in worldwide online debate. In Kenya, a large amount of tweeting has been done using photographs to refute incorrect allegations from the worldwide media and to change global opinions of Kenya and its residents.

[28] Omanga, Duncan. "'Chieftaincy'in the social media space: Community policing in a twitter convened baraza." *Stability: International Journal of Security and Development* 4, no. 1 (2015).

[29] Mutahi, Patrick, and Brian Kimari. *The impact of social media and digital technology on electoral violence in Kenya*. IDS, 2017.

[30] Ibid p.34-36

2.2 Social Media and National Security in Kenya

The rise of social media, fueled by the internet boom and mobile technologies, is transforming society. The television screen and the computer screen have been the two major screens for the last several decades. A variety of smaller displays, such as those seen on a mobile phone, iPod, or iPad, have entered the lineup in recent years. New trends have emerged as a result of the tiny screen's introduction; mass media has become more mobile. The rise and usage of wireless computers and mobile phones, sometimes known as "social media," is a contemporary trend that has taken the globe by storm. Simply said, they are online communications that use unique approaches such as participation, dialogue, sharing, cooperation, and linking.[31]

Today, social media channels are engrained in many people's everyday lives, acting as one of the key avenues of social interaction and participation throughout the world, either among individuals, businesses, or governments. The emergence of Web 2.0, its global reach, and the possibilities for upgrading its use and acceptability suggest that modern social networking constitutes a significant transition in communication that should not be overlooked. From education to health care, and many other fields, online social networks have had a significant influence. There is no exemption when it comes to national security. As a result of globalization, attention has switched to evaluating the impact of non-state actors. Terrorists, criminals, demonstrators, hate-mongers, and rioters may now have a greater influence on national and international security because to advances in social media. From nations to organizations and people, power is continually changing and diminishing.

Because social media is rapidly growing and is interacting with a variety of geo-economic and socio-cultural factors, it is critical to continually watch how they evolve, study how they operate, and assess their potential. This method strives to ensure that nations are not caught off guard in the event of possible abuse by adversaries is vile and repulsive, and to transform such new technologies into main resources for all authorities concerned in national security protection.

For Kenyans, their government, and national security institutions like the military and police, social media platforms have far-reaching social and security ramifications. The study's main concerns are social media and Kenya's national security challenges. Advances in computer technology have allowed social media to expand to the point that the flow of information, for good

[31] Tagi, Allan Mark Kipkoech. "Effects Of Social Media Use By Public Administrators On Community Mobilization And Security Enhancement In Nakuru County, Kenya." (2019).

or ill, now takes place on a worldwide basis. This information superhighway presents several hurdles to Kenya's national security strategists. In a world of "active worldwide listening," intelligence services' capacity to sift background "chatter" from more vital and valuable information that creates intelligence for security agencies and decision-makers is valued more highly. Despite the fact that social media is unaffected by government regulation and is non-discriminatory. Nonetheless, the research will show that their usage may assist states to predict how emergent risks would manifest in the future and devise strategies to counteract their consequences.[32]

Because social media poses a danger to national security, research to establish the harmful effect of social media on Kenya's national security is required. Kenya's territorial integrity, people, laws, values, and national interests are all protected by national security, which includes both foreign and internal threats.[33] As a result, the purpose of this research is to present the current state of affairs in Kenya in terms of the nature and usage of social media, as well as the challenges and hazards it poses to the military and national security in general.

2.3 Social Media Content Management Strategies at the National Police Service (NPS), Kenya

Content creation is one of the most important communication strategies used by the NPS to reach out to its public.[34] It emerged from the FGDs that the NPS uses three main types of social media to create content and disseminate it to the public. These are Facebook, Twitter and Web blogs. The type of content created by NPS as mentioned by the participants includes photographs, videos, online commentary, and tweets. The content includes original information that they post through the NPS social media sites, but some originate from the people they interact with. The participants had the following to say about content creation: “It is unrealistic to create content that is original at all times. Therefore, we share posts that have been created by the public if it is of importance to the functions of the NPS. Approximately 60% – 80% of content created at the NPS comprises content shared and interactions. The NPS regards all content and links created through our social networks whether original or shared as appropriate so long as the content aligns with our agency

[32] Mugaza, John Jirah. "The Impact of Social Media Use on the Productivity of Employees in Private Universities in Kenya: A Case Study of the United States International University Africa." PhD diss., United States International University-Africa, 2018.

[33] Constitution of Kenya, Article 238

[34] Ogolla, Erick Odhiambo, and Tom Kwanya. "Social Media Content Management Strategies at the National Police Service, Kenya." (2019).

guidelines." During the discussion it emerged that not every employee at the NPS may post anything on social media sites used for interacting with the public (Twitter, blogs and Facebook) without approval since the NPS has a strict communication policy. Updating the social media information at the NPS meant for the public is mainly the responsibility of the Communications Officer with assistance from the ICT personnel. However, there are social media tools for internal interaction such as WhatsApp which can be used by any employee to communicate internally.[35]

Cloud-based backups, such as Backupify, cloud-based information services, web analytics or dashboard tools, generic third-party, cloud-based reporting tools, such as Storify, RSS feeds, and the usage of screenshots are among the technologies employed.[36]

The use of cloud-based backup solutions (like Backupify), which provides free basic online services and supports a broad range of social media apps, was highlighted by the ICT professionals present. "Information may be frequently transmitted and brought back under corporate control," they said. Some, such as the production of Twitter reports in PDF, may be exported in open, non-proprietary formats. They can easily export information from social media programs, but they can't get data from the cloud." "These services may be used on a variety of social networking platforms, including Google applications," says the company. These are, however, backup utilities rather than information management tools. Their user interfaces and information transfers are intended to meet the demands of IT and backup, not of companies or information management." "The manual, scheduled process of downloading and collecting content into company servers must continue, and each time you do a backup, the same legacy data will be downloaded, resulting in significant amounts of duplication for major transaction accounts." These services are also subject to modification. As a consequence, we aren't too reliant on them.[37]

While commenting on the use of local backup system Digi.me, one of the ICT staff mentioned the following: "We use local backup systems such as Digi.me to support a wide variety of social media applications. We create snapshot copies of our data and store them locally. This information, on the other hand, is static and not dynamically accessible for reuse or repurposing..."

[35] Ibid p. 28

[36] Dwyer, Maggie. "Reimagining police engagement? Kenya National Police Service on social media." *Policing and Society* 30, no. 7 (2020): 760-776.

[37] Hensel, Kyle, and Michael H. Deis. "Using social media to increase advertising and improve marketing." *The Entrepreneurial Executive* 15 (2010): 87.

Many third-parties, free cloud-based solutions which may help companies combine information from many social media networks, were mentioned by the participants. However, as one of the ICT personnel pointed out, their use by the NPS was limited: "These solutions may offer reporting and listening services to assess the efficacy and impact of social media presence, piggybacking information management demands on current reporting or monitoring arrangements." However, if a log-in is necessary to see or use information, they have restricted access to it, and the data exportability of their data must be validated. There may be restrictions on the reporting and analysis data that may be sent, and deployment and maintenance might be costly. As a result, we don't utilize them very often."[38]

All records management and ICT workers were aware of and employed social media programs reporting tools, such as Facebook activity logs, to govern their social media content. Social media material was often transferred to PDF and other broadly open, accessible formats using these technologies. They also record all activities that take place on social media platforms. They did point out, however, that the export must be done manually, and that the information is flat and not dynamically accessible for reuse or repurposing.

Analytical tools such as Google Analytics and blog software analytics have been highlighted as free web services. They've shown to be helpful for tracking blog use, search engine phrases, referring sites, and top articles and pages, which is why they're so popular. They make it possible to export data. However, their utility is limited. It may not, for example, export reports in business-ready forms. As a result, they must be accompanied with screenshots, written reports, or other methods of recording business data. The excerpt below documents this. "Our ICT web team demonstrated how to use Google Analytics to acquire detailed and free information on traffic on our site to assist us with correspondence reporting. When our seniors asked for frequent progress reports on open public submissions, this came in handy a lot. This allows us to keep them up to date depending on the feedback we get, allowing us to make choices and track progress. Regular reporting also allows us to reflect as a team and consider new techniques to use when engaging with the general audience."[39]

[38] Ogolla, Erick Odhiambo, and Tom Kwanya. "Social Media Content Management Strategies at the National Police Service, Kenya." (2019).

[39] Ochieng, I. A., and Richard J. Otieno. "The Kenya national police service burnout intervention strategies." (2018).

Screenshots is also another strategy that was noted as popular among Records Management, ICT staff and Communications Officers. They explained that: “The screenshot photographs show the material exactly as it appeared in the social media program and have been used as evidence in court proceedings; however, the data is static and not dynamically accessible for reuse or repurposing. Because information must be manually updated for active users, there is a considerable expense in terms of staff time. It requires ongoing commitment from employees to stay current.”

RSS feed was another technique whose usage was noted among the ICT staff. It may be used for a variety of social networking applications, according to them. It's handy for auto-posting blog changes to Twitter and Facebook. It may be set up to send an email to a certain account including a whole blog post, a tweet, or a comment, among other things. It enables NPS to link visitors back to its organizational blog for comment when requesting information from the community or consulting through social media. The NPS blog was set up using an RSS feed so that any comments were automatically forwarded to the appropriate staff members. As a result, depending on current processes and procedures, employees may collect these emails into the corporate records system. However, it was reported by the participants that its application on emails requires manual intervention to capture it into corporate systems for usability. As such it was tedious to use and hence not popular.

2.4 Strategies Used By the Military to Reduce Threats of Social Media to National Security

When used properly by governmental institutions especially, security agencies like the military, social media may help protect national security and/or achieve a state's strategic objectives. "If social media offers a demonstrated threat to nations, it may be necessary for security agencies to continually refine and update plans for disrupting future Internet technologies," according to the Strat for analysts Papic and Noonan. Furthermore, governments may use these technologies for content creation, external collaboration, civic engagement, and other objectives, and a refusal to accept them may over time reduce a firm's relative abilities. More importantly, Social Media may be utilized for offensive as well as defensive objectives, such as preventive, early warning, counter-propaganda and more so forecasting.[40]

[40] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

2.5 Kenyan Military use of Social Media for Counter-Propaganda Strategies

The fact that Al- Shabaab's ideological content is disseminated in several directions necessitates any investigation of the technique utilized to disseminate it. Al- Shabaab's hinges on its capacity to sustain an active core capable of carrying out showy attacks, as well as its ability to get finance and recruits. Any activity aimed at countering Al-Shabaab's campaign should aim to erode and neutralize this image of a formidable stronghold.

Turn Al-Shabaab's Violent Discourse into an Unjustifiable discourse: The problem is to dispel the notion that terrorism is an acceptable means of achieving one's goals, regardless of their validity.[41] Seating the concept that terrorist violence delegitimizes those who use it among Muslim people might assist to weaken the alleged popular representation that terrorists constantly claim. Long-term, a worldwide rejection of this form of violence is required. Kenya's military operation against Al-Shabaab in Somalia, nicknamed "Operation Linda Nchi" (Swahili meaning "Defend the Country"), has devolved into a Twitter battle. This happened after the official military spokesman, Major E. Chirchir, shared old images stating that a Kenyan Al Shabaab recruit had just been stoned to death by the organization members over a "change of opinion." The images were eventually discovered to have been shot by a Somalian journalist in 2009 and do not even include a Kenyan Al-Shabab recruit.

Terrorism is defined in law in certain nations that have suffered for years, such as Spain, and is penalized by imprisonment. This method may be used in other nations as well. Working against terrorist apologists does not violate the public's right to free speech since expressing sympathy for the murder of innocent people is akin to condoning those who perpetrate such crimes. Furthermore, in an interconnected world where there are no actual controls on the flow of information on social media platforms, addressing this issue simply on a national level are futile. Anti-terrorist messages should be broadcast via the media, as was done during the Cold War with anti-Soviet Western radio broadcast on the opposite side of the Berlin Wall. It's tough to see these tools as foreign manipulators in the present situation. Al-Jazeera's success demonstrates the necessity to divert attention away from these channels and participate in expressing alternative viewpoints and

[41] Cabinet Office. *A strong Britain in an age of uncertainty: the national security strategy*. Vol. 7953. The Stationery Office, 2010.

disseminating opposite information; otherwise, the mass media would become easy victim to terrorist influence.[42]

Any informative effort aimed at counteracting the impacts of terrorist images must make advantage of symbols' mobilizing potential. Public announcements of terrorist detainment, the publishing of their testimonies, and any act demonstrating their absence of commitment and other indicators that cast doubt on Al- Shabaab's image can all help erode the terrorists' fortress image.

In the terrorist network's propaganda effort, rumors and disinformation play a significant role. Al-Shabaab uses them to cast doubt on the legitimacy and dignity of its opponents without having to prove that their claims are true. Rumors might include a wide range of bizarre claims, conspiracy theories, and strange recommendations. Though the public first gives these types of assertions very limited credence, the long-term consequence implies an internalization of skepticism about all parties involved: leaders, security organizations, and terrorists. The authorities' sometimes secretive character, their frequent lack of cooperation, and the severity of the claims all contribute to the “fire spreading.

The detrimental consequences of these assertions might be neutralized by establishing an organization or foundation dedicated only to rejecting the disinformation in an educated way and giving clear and compelling evidence to put an end to rumors. Its legitimacy and effectiveness would be enhanced if it had a neutral makeup, including academics and experts from outside the political and military realms.

Terrorist propaganda makes extensive use of particular visual materials' emotional power. On terrorist-sponsored scant Web sites, crude photographs of deaths and mutilations, including crippled and maimed males displayed as claimed proof of the outcomes of Kenya Defence Forces (KDF) military operations, may be obtained without any form of accessible or effective restriction.[43] Terrorists are well aware that appealing to emotions is one of the quickest and most successful means of changing public and personal views, and they will use whatever form of material they believe would help them achieve this goal. The Kenya counter-informative approach cannot overlook the emotional viewpoint of this information battle without resorting to excesses and always adhering to ethical norms. One of the most effective methods of delegitimizing

[42] Obama, Barack. *National security strategy of the United States (2010)*. Diane Publishing, 2010.

[43] Sarts, Janis. "Disinformation as a Threat to National Security." In *Disinformation and Fake News*, pp. 23-33. Palgrave Macmillan, Singapore, 2021.

terrorists is to show the consequences of their actions via genuine photos of their victims and the accompanying human sorrow. The exposure of particular photos, when combined with respect for the victims and their families, may be a much more effective protest against terrorists than a lengthy series of official communique demanding punishment. Indeed, hiding the true consequences of terrorism only contributes to the creation of an idealized caricature that is far distant from what terrorism is.

2.6 Kenya News Management by the Military

As much as the media despises being "managed," all governments use the media to influence the public, putting a good perspective on their own activities and weakening opponents' positions, such as during critical talks. It is difficult to handle news because of the availability of global information networks that allow for fast dissemination of news to worldwide audiences. Some democratic regimes recognize that the official establishment's relationship with the media is inherently antagonistic. It's almost hard to tailor news to a single audience since it bleeds over to others. Politicians, on the other hand, address home audiences with subjects that will connect with them, such as during elections, while international viewers are expected to partake in such rhetoric.[44]

The military often has the finest news management; they have a variety of alternatives for presenting their point of view. Leaders with media abilities have a distinct edge. As a result of the growing prominence of domestic publics, foreign ministry spokespeople now concentrate primarily on domestic responses to foreign affairs problems, with less emphasis paid to projecting domestic policies to the international media. This is a reversal of the function of foreign ministries in the past. Similarly, even while traveling abroad, Leaders care much more about what their local press has to express than they do about extending out to worldwide audiences via the media of the countries they visit. In an ideal world, the two should be balanced, and foreign ministries will have their hands full ensuring that the latter is given equal importance.

In terms of conveying messages on originality and assisting in appearance forecast, the Diaspora is often a vital multiplier. Because public diplomacy attempts to influence mind space abroad and is being defined by a society's trust in itself, people and diaspora populations that have

[44] Katzenstein, Peter J. *Cultural norms and national security: Police and military in postwar Japan*. Cornell University Press, 2018.

consciousness and lack faith in their government will not be partners in a state's public diplomacy endeavors.

Mughal wa Mungai said that media coverage of events that focuses primarily on national concerns and ignores people's daily realities does not do credit to people or peace. He said that coverage of Kenyans' conflict experiences failed to adequately depict the crisis scenario and the people's plight. He went on to say that just presenting the voices of authorities and government agents who may not be present at war scenes, rather than spotlighting the thoughts and experiences of people on the ground, particularly women and children, gives a biased picture of the violence.[45]

In February 2008, CITIZEN TV sent footage of life in camps for people who had been displaced by post-election violence to the homes of Kenyans. This was the first time that a TV station had shown footage of the aftermath of the violence. The voices of people who had been hurt, as well as the households of people who lost children or other relatives, were on the channel. It was easy for Kenyans to understand why their relatives had to flee their country. They did this through churches, mosques, social clubs, non-profit groups, and the foreign society. They gave food, clothes, and other necessities to people residing in the camps.

2.7 Military Intelligence and Social Media Analytics

To avoid being caught off guard by threats and to be more resistant to them, it is important to be able to forecast possible strategic and tactical situations. Nicola Gelao, head of the Italian Defense General Staff's Information and Security division, said that the capacity to "hypothesize" the fate isn't an exact science, and that it's hard to predict how, when, and where a threat will show up in the future. From this perspective, Social Media can be a valuable intelligence-gathering tool for the military, because all Social Media users leave traces regarding their individuality, competences, propensities, movement patterns, contact details, and so on, that can be comfortably gathered and processed, regardless if their profile is no longer active or updated.[46]

Because organized criminals, terrorists, foreign governments, and other adversaries are increasingly using social media, persistent and broad monitoring of these platforms might be employed as a warning system in the case of existing or future threats to national security. As a consequence, military social media monitoring might serve as a strong alert system.

[45] Arora, Jaya, Shaily Goyal, and Kishan Gopal Ramawat. "Biodiversity, biology and conservation of medicinal plants of the Thar Desert." *Desert plants* (2010): 3-36.

[46] Arora, Jaya, Shaily Goyal, and Kishan Gopal Ramawat. "Biodiversity, biology and conservation of medicinal plants of the Thar Desert." *Desert plants* (2010): 3-36.

Another crucial part is tactical alert and horizon scanning, which tries to identify threats' long- and medium-term trends to determine the opposing factions' attitudes and foresee their decisions.

To avert national security threats such as political upheavals, migrations, diseases, humanitarian crises, demonstrations, and economic instability, the US military has created a research initiative called Open Source Indicators (OSI). OSI, in particular, assumes that changes in population behavior always foreshadow big social events. Plotting and observing such behaviors might help you predict what will happen next. Monitoring data that is publicly accessible and comes from several sources, the first of which is Social Media, may be used to observe and quantify such changes.[47]

To better understand the environment in which some US military units are deployed, the US Department of Defense developed a program called "Social Media in Strategic Communication" (SMISC) through DARPA, which aims to monitor social media in order to gain a better understanding and collect useful information that can be used in military missions. As a result, the commanders of US deployed sites were able to better comprehend the socio-political, religious, economic, and cultural features of the areas they worked in, as well as identify potential dangers, thanks to the use of social media.

"Maintaining a Social Media presence in deployed places helped commanders to recognize possible risks and developing trends," said Thomas Mayfield, a US army colonel. Moods and difficulties are often well-represented in the internet community. So, for example, SMISC's goal was to "create a new science of social networks that is based on new technologies that include, but aren't limited to, information theory, massive-scale graph analytics, and natural language processing." This was done through the development of both automated and semiautomated support processes and approaches for analysts who use Social Media in military contexts on a regular basis.

Intelligence gathered from publicly accessible sources is known as open-source intelligence (OSINT). In the intelligence community (IC), the term "open" refers to sources that can be seen by the public. This is not the same as open-source software or public intelligence. Getting OSINT in Kenya for a wide range of intelligence, counter-terrorism, and risk mitigation efforts has become a very difficult and time-consuming task for both the government and the risk management

[47] Gray, Chris Hables, and Ángel J. Gordo. "Social media in conflict: Comparing military and social-movement technocultures." *Cultural Politics* 10, no. 3 (2014): 251-261.

industry. This is because it takes a lot of resources. Kenya's government is a part of a lot of open-source projects. It doesn't matter what such open-source actions are called. They are all freely available.[48]

Following a big terrorist or crisis occurrence, an excellent example displays an obvious and anticipated jump in OSINT due to the projected boom in media and internet user-created information. In this example, the Al Shabaab assault on Kenya's Westgate Mall in September 2013. New leads and sources might be uncovered from within the material by studying the outcomes around this increase in activity. Individuals that contribute information indicating inside knowledge of the event or proximity to a Person of Interest, as well as individuals with ties to terror organizations, may be identified via data analysis and then added to social network analysis (SNA) and link analysis.

There are other source varieties that may be interesting after looking at this data segment. Even if someone is using fake credentials online, they are likely to have written other material that gives away critical info or links to other online sites or people of interest, all of which help build a more accurate intelligence image and scan the horizon.

2.8 Military use of Social Media for Public Diplomacy

Despite the fact that multiple US Army reports warn of the possibility for terrorists to utilize social media, new government policies are developing that encourage the use of social media platforms for targeted communications and public relations. The federal government has started to embrace the use of such technologies to promote free speech, democratic values, and ideas, as well as counteract disinformation propagated by terrorist organizations' media activities. The Department of Defense (DoD) released a Directive-Type Memo (DTM) in February 2010 describing the department's new social media strategy, identifying Internet-based capabilities such as social networking platforms as critical to operations.[49]

Social media is also used by US diplomacy for influence and propaganda purposes When James Glassman was undersecretary of state for public diplomacy in 2008, he came up with and formally launched the idea of "Public Diplomacy 2.0." This is what happened at a special event at the New

[48] Maltby, Sarah, and Helen Thornham. "The digital mundane: social media and the military." *Media, Culture & Society* 38, no. 8 (2016): 1153-1168.

[49] Gallacher, John D., Vlad Barash, Philip N. Howard, and John Kelly. "Junk news on military affairs and national security: Social media disinformation campaigns against us military personnel and veterans." *arXiv preprint arXiv:1802.03572* (2018).

America Foundation. Glassman says that Public Diplomacy 2.0 is a new way to communicate that takes advantage of the power of social media. This gives the diplomatic corps a big advantage in terms of economic, scientific, technological, and geostrategic relations, as well as soft power activities that try to fight radicalized ideologies, religious extremism, and political violence. People who use Public Diplomacy 2.0 must make sure that their activities are based on a central strategic plan, coordinated with all diplomatic institutions, and well integrated with the military. During a talk on Public Diplomacy 2.0, Helle Dale said that the U.S. government could use social media as well as radio, TV, libraries, and student exchange programs to reach people all over the world. There are people in the US government who work on public diplomacy and strategic communications who are looking into how new social media could help them win over people in other countries. This is particularly true in the Muslim world, where the current intellectual battle is being waged. At the stroke of a computer key or a mobile phone button, these low-cost gadgets may link hundreds, if not millions, of individuals. People who dislike the United States are already familiar with how to exploit them. [50]

When WikiLeaks released this cablegram in February 2010, it said the US embassy in Jakarta needed more money to use new media and social networking tools in order to support President Obama's trip there in March of that year. This shows how important social media is to the US Department of State. For the US military, public diplomacy was meant to make the US more credible and legitimate, make an adversary less credible and legitimate, get specific audiences to do things that helped the US or the world, and make an adversary not do things that helped the US or the world.

Diplomacy is used by the Kenyan military to obtain and disseminate information. Kenyans may research and comment on current political, economic, and social concerns through blogs, Facebook, emails, and Twitter. During the 2002 and 2007 general elections, for example, most Kenyans learned of the results through mobile phones rather than traditional media. Kenyans may read and comment on subjects that traditional media outlets choose to overlook via blogs and emails on the internet.

As vital as the internet is in getting Kenyan tales out to the world, where individuals have been saved from life-threatening circumstances thanks to an SMS sent through the internet, it can also

[50] Jones, Nigel, and Paul Baines. "Losing control? Social media and military influence." *The RUSI Journal* 158, no. 1 (2013): 72-78.

be perceived as a double-edged sword. According to Mungai, diaspora Kenyans utilized virtual media such as online chat forums and email to actively invite their relatives in Kenya to break up the nation. Even highly educated professors naively participated in these conversations, which included racial intolerance as a significant component.[51]

2.8 Military use of Social Media for Psychological Operations (PsyOps)

Military doctrine contemplates the use of social media's enormous audiences to conduct psychological operations (PsyOps) in the framework of information warfare, with the main goal of influencing big masses' "sentiment," such as emotions, motivations, and objective reasoning. The United States military describes PsyOps as "organized operations to deliver chosen true information and indications to foreign audiences such that their emotions, motivations, objective thinking, and, eventually, the actions of their governments". The military has employed information dissemination in the past to interfere with opponents disclosing factual information or propaganda messages on several times and at various eras. [52]

Secret spies penetrated behind enemy lines, or leaflets were dropped from an aircraft over enemy territory by military intelligence; nowadays, social networks have an edge over these sorts of operations. The phrases "psychological operations" and "psychological warfare" are often interchanged; "psychological warfare" was coined in 1920, while "psychological operations" was coined in 1945. Famous strategists such as Sun Tzu have emphasized the significance of psychological warfare: "One does not need to annihilate one's adversary. "All that is required is to kill his desire to interact." Because a hundred wins in a hundred fights isn't the pinnacle of expertise. The highest greatness is to subjugate the opponent without fighting.[53]

The use of new-generation media and large-diffusion platforms like mobile and social media gives governments a powerful instrument for instantly reaching critical masses. PsyOps is a popular option among the military for diplomatic, military, and economic measures. PsyOps sends information to certain groups of individuals, identified as target audiences, in effort to enhance specific themes that impact the accomplishment of political and military objectives. The target

[51] Ibid

[52] Goldstein, Frank L., and Benjamin F. Findley. *Psychological operations: Principles and case studies*. Air Univ Maxwell AFB AL, 1996.

[53]Bates, Rodger A., and Mara Mooney. "Psychological operations and terrorism: The digital domain." *The Journal of Public and Professional Sociology* 6, no. 1 (2014): 2.

audience was described as "an individual or group selected for psychological operations to persuade or attack" by NATO in a doctrine for psychological operations.

NATO emphasizes the viability of psychological operations in the paper "Allied Joint Doctrine for Psychological Operations AJP3.10.1 (A)." Strategic psychological operations include using psychological operations to erode the will of enemy or potential adversary target audiences, increase the dedication of friendly target audiences, and gain the cooperation and support of uncommitted or indecisive target audiences. Due to the sophisticated state of technology at their disposal, a psychological operation has been thoroughly contextualized in today's military: the Internet, virtual reality, blogs, video games, chat bots, and, of course, social media platforms are all employed by the military for different purposes. The military is spending heavily on psychological operations specialists and placing these technologies to the test in order to persuade individuals to support their cause or alter a nation's attitude.

2.9 Social Media Activism in Kenya

When youth have their space in a state the country is always in peace. Kamau (2013) investigates the role that social networking sites play in influencing political participation and civic engagement among Kenyan urban youth.[54] Kamau notes that social media sites such as Facebook and Twitter have been positioned as important platforms for political participation among the youth, which also have the potential of sparking interest and augmenting youth participation in civic and governance processes among disengaged youth. What positions social networking sites to take up this role is their ease of accessibility and usability, appeal and convenience in participating in political discourses. Says Kamau: “SNSs cannot replace the existing traditional structures of political campaigning and mobilization but on the other hand, campaign strategists and politicians cannot ignore the opportunity provided by SNSs in the mobilization process”.

While acknowledging the importance and role of social networking sites in facilitating political participation, the author, however, cautions that social media activism must be paired with traditional methods of activism to facilitate appreciable participation. According to Kamau, the mobilization of people for any form of activism must primarily be done offline, with social media sites serving a complementary role. Social media, the author concludes, have not got to a level

[54] Kamau, Samuel. "New Media Techologies and Democracy: The influence of Social Networking Sites on Political Attitudes and Behaviour among the Urban Youth in Kenya." PhD diss., 2013.

where they directly impact on political choices among the users.[55] He, however, notes that they are useful in shaping public opinion, as well as mobilising people and resources, and are particularly effective in spreading negative propaganda to damage opponent's credibility. This is facilitated by the fact that social groups tend to believe messages posted by members of the same group.

Online platforms, particularly social media sites, in Kenya have become some of the most dynamic spaces for engaging the political establishment on social, economic and political issues. Debates on topics such as young unemployment, the environment, reproductive health rights, and sexual assault are increasingly being heard, despite the fact that they have traditionally had difficulties entering onto the public priority list.

On Twitter, the hashtags #StandwithLiz and #JusticeforLiz (about a young girl from Western Kenya who was gang-raped by four men) trended for several days, according to Mwaura, as Kenyans rallied to support a petition started by activist Nebila Abdulmelik urging the Inspector-General of Police to re-open the case, which had previously been closed. On October 31, 2013, the online campaign was accompanied by a rally in Nairobi, when demonstrators submitted a petition signed by over 1.2 million people. As a consequence of the widespread public outcry, police personnel who (mis)handled the case were penalized, and the Director of Public Prosecutions ordered an investigation into the event, which resulted in the arrest and conviction of one suspect.

#KOT Kenyans on Twitter involves a gallery of middle-class Kenyans' who highlight social problems that range from racism at up-market eateries to rants about the constant traffic jams in Nairobi. While no noticeable change has been forthcoming from the government, government officials often join in debates about social ills. I Paid a Bribe (http://ipaidabribe.or.ke/) is an initiative of Kenyan anti-corruption activists fighting corruption in Kenya using the new technologies to crowd source corruption experiences. I Paid a Bribe is sponsored by the Wamani Trust of Kenya to bring IPAB to East and Central Africa, with its key objective being to provide a platform for people to expose public officials who extort bribes from Kenyans.[56]

"Occupy Parliament" is one of the more recent activist movements that was created to challenge the conventional, "accepted" norms that have given birth to social inequity and injustice,

[55] Ibid p. 290

[56] Jones, Nigel, and Paul Baines. "Losing control? Social media and military influence." *The RUSI Journal* 158, no. 1 (2013): 72-78.

oppression and intolerance. The movement turned to social networking sites – Occupy 26 Parliament on Facebook and #OccupyParliament on Twitter to mobilize Kenyans to protest against a plan by Members of Parliament to award themselves hefty salary increments and allowances. This culminated into a protest that lasted several hours outside Parliament buildings, a demonstration of the power of social media sites in garnering numbers for civil causes. Bunge la Wananchi is another notable platform for agitating for change.

With a following of more than 15,000 members on Facebook, its mandate, as posted on its page is to "Facilitate sensible and responsible discussions of pressing current issues in the society". Bunge La Mwananchi provides an alternative 'parliament' where members of the public can engage on various issues touching on politics and social responsibility. While Bunge la Mwananchi does not overtly engage in activism or take a stand on issues, it gives the online Kenyan public a chance to provide alternative views to counter what they consider to be a breach of ethical principles, and maladministrative injustices. [57]

In 2006, Ory Okolloh a lawyer-cum-activist co-founded the parliamentary watchdog site Mzalendo (Swahili for patriot), whose objective was to increase accountability in government through tracking Parliamentary (National Assembly) sessions and politicians' speeches (http://info.mzalendo.com/).[58] And in 2007 when Kenya was engulfed in post-election violence following the disputed presidential election, Okolloh helped create Ushahidi (Swahili for witness), a website through which Kenyans would collect and share eyewitness reports of the violence using text messages services and Google Maps (http://www.ushahidi.com/). Okolloh has got a personal blog, Kenyan Pundit, which has been featured on Global Voices Online, a web-based community that defends online rights and freedoms and fights censorship, empowers isolated and marginalized communities with tools, skills and support to voice their plight and challenger marginalisation (http://globalvoicesonline.org/about/). [59]

Global Voices describes their objective thus: "Link to text, photos, podcasts, videos, and other forms of grassroots citizen media that people around the world are talking about and sharing. Help people around the world learn how to use open-source and free tools to express themselves through

[57] Weaver, Alfred C., and Benjamin B. Morrison. "Social networking." *Computer* 41, no. 2 (2008): 97-100.

[58] Okolloh, Ory. "Ushahidi, or 'testimony': Web 2.0 tools for crowdsourcing crisis information." *Participatory learning and action* 59, no. 1 (2009): 65-70.

[59] Mäkinen, Maarit, and Mary Wangu Kuira. "Social media and postelection crisis in Kenya." *The international journal of press/politics* 13, no. 3 (2008): 328-335.

mentoring, tutorials, and publicizing how people can use them safely...” Writing in The Standard, Nyambega Gisesa looks into the rise of online activism in Kenya, and its increasing importance in Kenyan politics. Social media sites, he argues, are the new front in the mobilisation of people for social causes, as evidence by the Occupy Parliament movement.

The blog Wanjiku Revolution Movement that is run by Edwin Kiama – he also runs related accounts on Facebook and Twitter – reaches thousands of Kenyans with whom he engages on various issues such as governance its associated issues such as corruption and inflation (http://edwinkiama.blogspot.com/). Through it, he accords different writers the chance to post various articles on issues they feel need attention. On Twitter, the #WanjikuRevolt has 13,500 followers and 1,300 Likes on Facebook. Another blog that is active in terms of highlighting social ills is Laura Korongo’s. A Kenyan Perspective[60] where she profiles some of Kenya’s renowned figures in a bid to motivate good governance and responsibility.

2.10 Social Media and Economic Development

Insecurities are associated with poverty. Poor developing states have had states of conflicts. Growth in economy and development always leads to peace and raise living standards. The function of social media in promoting economic growth in transitional or emerging nations is critical. A slew of studies suggest that media freedom and economic progress are inextricably linked. Media influences market actors' incentives through increasing competitiveness in a certain industry and affecting commodity demand and supply via advertising. [61]

As per findings of the study, state ownership of social media is linked to negative development outcomes such as increased corruption, poor economic governance, and underdeveloped financial markets. Removing obstacles to foreign social media investors or forbidding concentration of ownership may improve the media's role in economic growth, as well as the function of the media in promoting market development and giving individuals with access to market possibilities.

In terms of economics, social media informs individuals about stock exchange procedures, e-banking, investment program recommendations, company prospects, and new market innovations, among other things. To augment existing financial systems, social media has developed a new

[60] https://laurakorongo.wordpress.com/tag/activism/

[61] Jones, Nory, Richard Borgman, and Ebru Ulusoy. "Impact of social media on small businesses." *Journal of Small Business and Enterprise Development* (2015).

banking system. At the press of a button, one may now pay bills and make purchases via the internet.[62]

In terms of business, social media has become a place where people can share ideas and come up with new things. Products and services can be bought and sold online, which makes it easier for small businesses to start-up and grow. Many Kenyans, like people in other countries, have learned how to start businesses on social media and hire people to work for them. People and businesses have made a lot of money by buying and selling things online. Bank operations like online deposits and transfers have made it easier for people to make and transfer money. It used to be impossible to travel without going to public transport and tourist agencies to make booking and set up other things.

Online businesses like Jumia and OLX are becoming popular places for people to shop. Masoko and OLX, for example, are also popular places for people to shop. Social media has had an impact on a lot of different areas, including e-education, health and agriculture and crime prevention and safety. This is because so much data is shared on social media by people and organizations and institutions.[63]

Commercial marketing has made extensive use of social media. Business and markets contain a variety of strategies for converting practical ideas into objectives. The ways through which businesses strive to educate, convince, provoke, and remind customers about the brands they offer are referred to as marketing communications. Marketing communication allows businesses to communicate with their customers and may also act as a brand's voice. There are several marketing communication strategies available, including all types of promotion, advertising, publicity, public relations, personal selling, and marketing.

Marketers are under pressure to determine whether or not to engage in the new internet communications accessible, as well as to justify the expense of employing classic advertising channels like television or radio. Social media, according to Chei and Long[64] is a critical instrument in the marketing environment. According to his study, 60 percent of planners employ at least 16 web leads every year through social media. He also came to the conclusion that the

[62] Ibid p.90-91

[63] Llorente, Alejandro, Manuel Garcia-Herranz, Manuel Cebrian, and Esteban Moro. "Social media fingerprints of unemployment." *PloS one* 10, no. 5 (2015): e0128692.

[64] Lee, Chei Sian, and Long Ma. "News sharing in social media: The effect of gratifications and prior experience." *Computers in human behavior* 28, no. 2 (2012): 331-339.

majority of financial planners are on Facebook. LinkedIn, which was developed for business professionals, also provides decision-makers with information and chances. Different uses are assigned to social networking sites by businesses. Human resources departments at companies, for example, regularly utilize LinkedIn to find and choose qualified applicants for unfilled positions. Employees of organizations utilize 'glassdoor.com' to submit evaluations and reviews of their workplaces in order to retain service to candidates or companies in the same manner.

The vast potential of social media for location marketing, SEO (search engine optimization), and engagement has been acknowledged by most economic development groups. Many people begin (appropriately and sensibly) with LinkedIn, which is created primarily for business interactions. Many people go on to Twitter, YouTube, Facebook, Instagram, or Flickr from there.

2.10.1 Use of Social Media as an Advertising Tool

News, information, and advertising are being liberated from the limits of conventional print and broadcast distribution methods as a result of a digital revolution in the media. Social media, as well as the platforms that support social networks, are not only new technologies; they are also facilitators of a fundamental marketing strategy change in how businesses and consumers interact. We may include blogs and microblogs (like Twitter and others), videos, review boards, online forums, and other social channels when we talk about social media, also known as consumer-generated media. [65]

Users of social networking sites may utilize them as a unified communications platform, allowing them to connect with others at the same time. Traditional marketing channels are increasingly dissolving or being incorporated into a global network powered by the Internet.

The existing agreement on communications development is based on a common understanding of current market and technology advancements. These developments have paved the way for the growth of internet communication. Companies must begin to consider new methods to convey their services as customer behavior shifts toward being more demanding and impulsive. [66]

As a result, traditional corporate communication is fluctuating away from one-way sales messaging delivered to broad audiences by hierarchical companies with special information possession. This has gradually become visible for today's marketers, as social networkers discuss

[65] Hassan, Shahizan, Siti Zaleha Ahmad Nadzim, and Norshuhada Shiratuddin. "Strategic use of social media for small business based on the AIDA model." *Procedia-Social and Behavioral Sciences* 172 (2015): 262-269.

[66] Dwivedi, Yogesh K., Kawaljeet Kaur Kapoor, and Hsin Chen. "Social media marketing and advertising." *The Marketing Review* 15, no. 3 (2015): 289-309.

consumer brands and participate in business communication. They are urged to be more open, live more impulsively, and have more immediate conceptions of value and trust as customers.

As a result, a new, critical source of data on customers comes directly from them. This information is based on real customer views and comments shared on social media. Because the majority of present and future consumers are online, they use social or user-generated media. They're talking about their favorite brands and items, as well as their least favorite brands and things. They have the ability to influence and impact the firm and its product sales. Winning businesses are devising strategies and techniques for listening to, learning from, analyzing, comprehending, and engaging with this powerful new channel.

CHAPTER THREE

THE NEGATIVE EFFECTS OF SOCIAL MEDIA ON NATIONAL SECURITY

3.0 Introduction

Social media platforms are web-based services that allow users to establish profiles inside a limited system and communicate with other users all over the world. Social networking is the process of forming connections amongst individuals who have shared interests and aims. Recently, social media platforms like as Facebook, Twitter, YouTube, LinkedIn, Skype, jabook, Lagbook, and others have cemented their places in the hearts of many users throughout the globe, prompting hackers and other bad actors to exploit them to further their harmful goals. [67]

Recent incidents throughout the globe have shown that the use of social media, like other conventional media, may jeopardize a country's security.[68] It is worth emphasizing that the security of any given country is critical to the preservation of peace and harmony. Countries all around the globe have recently faced a slew of security issues, one of which has been fueled by the abuse of social media platforms. It is important to note that social media networks do not constitute a security risk in and of themselves; rather, it is the users of these platforms that pose a security risk via their anti-social activities. This is especially true when there is a lack of government control, less incentives to inform and educate users about information security, a lack of understanding about online privacy, and a lack of understanding about how abuse of these platforms may jeopardize national security.

This means that, although social media offers significant advantages for both individuals and nations, it may also contribute to instability, as well as other well-known security problems. People's use of social media platforms, for example, may result in violence and conflict as a result of repeated messages of hate and propaganda. As a result, arguments about the usage of various social networking sites should focus on the larger issue of national security and information flows.[69] Numerous examples have been documented in which criminals used social networking

[67] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

[68] Chukwuere, Joshua Ebere, and Chijioke Francis Onyebukwa. "The Impacts of Social Media on National Security: A View from the Northern and South-Eastern Region of Nigeria." *International Review of Management and Marketing* 8, no. 5 (2018): 50.

[69] Hadžić, Faruk. "The influence of social media on threats to identity, stability and national security; institutional inefficiency and vulnerability of B&H." *SCHOLARLY JOURNAL FOR PROTECTION, SECURITY, DEFENSE, EDUCATION AND TRAINING ISSUES YEAR XXIV, NO: 45-46, 2020* (2020): 67.

sites to disseminate harmful cryptograms in order to compromise users' systems or obtain access to personal information such as location, contact information, and professional ties. Facebook is the most susceptible social media network to cybercrime, according to a poll done by Sophos in 2009. Cyber thieves exploit this site and other social media platforms to disrupt security by spreading malware, third-party apps, social engineering assaults, and identity theft, among other things.

3.1 Threats of Social Media to National Security

National security in many nations has lagged as the internet and social media continue to expand and change, particularly in most third-world countries. Experts and politicians in national security must now adjust fast to evolving dangers or risk severe national security breaches. Recent occurrences throughout the globe have shown that social media may be used to undermine national security. Social media may be used to expand common space, but it can also be used to destabilize it. Social media may be readily used to disseminate propaganda, biased speech, and information that incites violence. Any discussion of the function of social media must thus include a discussion of the relationship between information flows and a state's stability. It is amply evident that unconstrained social media could present security risks to nations. Non-state actors such as terrorist groups and unscrupulous individuals are now using social media to export hate messages. Groups like Boko Haram in the western African region are using Facebook and other platforms as conduits to recruit fighters and increase their support base. In addition to using these platforms for recruitment purposes, these groups and individuals are effectively using this medium for propaganda activities to create panic.[70]

The social media platform is also used to conduct criminal activities. This website is used by criminal organizations to communicate information and organize unlawful actions. Child pornography, phishing, drug smuggling, computer virus propagation, human trafficking, financial fraud, and the transfer of documents from industrial espionage are only a few of the illicit acts. In addition to these illegal acts, the uncontrolled and unlawful dissemination of private and sensitive information through social media platforms such as print, audio, and video has become ubiquitous. These acts can compromise national security. An example is the WikiLeaks saga. This platform provides the public with national security-related information without considering the possible

[70] Sayler, Kelly M., and Laurie A. Harris. *Deep fakes and national security*. Congressional Research SVC Washington United States, 2020.

negative consequences. Social media is also essential to social movements or groups seeking nondemocratic changes. Protests against former Egyptian President Hosni Mubarak occurred in January 2011. Tunisia's revolution affected the demonstrations in certain ways. The protests sparked other rallies around the Middle East, including in Libya, Syria, and elsewhere. This wave of anti-government protests crossed national lines and spread like wildfire. Several analyses concluded that the use of social technologies, ranging from Facebook pages to cell phone cameras, aided in the organization and documentation of actions related to the Arab Spring uprisings. During the Arab Spring, the movement's leaders took use of social media's unconstrained nature and tools to organize and stir the public.

Though social media has the potential to threaten national security, it also can strengthen national security. Governments are utilizing social media as a warning or trend indicator tool, for example. The government can detect the earliest beginnings of any unfriendly or possibly harmful action with this surveillance technique. Governments might try to forecast occurrences that could have a detrimental effect on national security by collecting and analyzing signals.

3.2 Social Media and Terrorism

Terrorist cells and organizations have discovered that social media is one of the most effective instruments for facilitating their activities.[71] With the extensive use of contemporary information and communication technology, cyber terrorism has arisen as a significant threat to national security throughout the globe. Terrorists are increasingly using social media networks as a realistic means of disrupting people, organizations, and national peace. Terrorists have mostly used social media networks, notably Facebook, YouTube, and Twitter, to propagate their ideology and gain followers throughout the globe, due to the cheap cost, simplicity, and widespread coverage of these platforms.[72]

The organizations are presently using social media to plan and organize attacks, to communicate with other linked terrorist cells and criminal groups, to broadcast false information and propaganda, and to create hatred that may harm the public mood. Terrorist groups today have their websites, which they use to propagate their beliefs and propaganda, as well as numerous social media platforms via which they connect to promote their causes. The use of social media

[71] Hossain, Md Sazzad. "Social media and terrorism: Threats and challenges to the modern era." *South Asian Survey* 22, no. 2 (2015): 136-155.

[72] Sayler, Kelly M., and Laurie A. Harris. *Deep fakes and national security*. Congressional Research SVC Washington United States, 2020.

chat platforms like Skype, which includes both audio and video capabilities, has grown more popular among terrorist groups. The rebels may connect and communicate with one other and with supporters from all over the globe via chat rooms and e-forums. This also allows them to recruit new members and exchange information with security services with little or no fear of being identified.[73]

Terrorists are heavily employing social media platforms for radicalization, recruiting, and training recruits throughout the world in the current period, which is defined by internet connection and extensive use of social media networks. Individuals are influenced to participate in collective activities via social media platforms.[74] They make it easier for people to make friends and form bonds, which influence their behavior and attitudes over time. Vulnerable people may be forced to join jihadist organizations as a consequence of the extensive dissemination of extremist ideology and materials. In addition to the aforementioned uses of social media by insurgents, these organizations use social media to cooperate with other criminal gangs and to seek funds from diverse supporters throughout the globe. With the progress of technology, the use of social media has greatly eased the relationship between terrorist organizations and organized crime, as well as the development of new offensive tools.[75]

Islamic-jihadist groups are now the terrorist cells and organizations that make extensive use of social media platforms. Because most of these organizations have a net-like decentralized structure, they may use social media networks like Facebook and Twitter to efficiently connect all of their associated organizations and coordinate their leadership throughout the globe. Al-Qaida, for example, uses social media to coordinate its leaders, recruit and train its recruits, gain support from across the globe, seek funds, broadcast their successful operations via photographs and videos, disseminate a list of their martyrs, and spread their ideas. ISIS and al-Shabaab, for example, use social media not just for recruitment and training, but to also advocate their ideologies, highlight their successful operations, and inspire fear in people. [76]

[73] Mayfield, Antony. "What is social media." (2008).

[74] Dean, Geoff, and Peter Bell. "The dark side of social media: review of online terrorism." *Pakistan Journal of Criminology* 3, no. 4 (2012): 191-210.

[75] Gunawan, Budi, and Barito Mulyo Ratmono. "Social Media, Cyberhoaxes and National Security: Threats and Protection in Indonesian Cyberspace." *Int. J. Netw. Secur.* 22, no. 1 (2020): 93-101.

[76] Gunawan, Budi, and Barito Mulyo Ratmono. "Social Media, Cyberhoaxes and National Security: Threats and Protection in Indonesian Cyberspace." *Int. J. Netw. Secur.* 22, no. 1 (2020): 93-101.

Jihadist organisations also make extensive use of social media channels to instill fear and terror among the general people. When natural disasters happen, such as floods or earthquakes, some terrorist groups and organized crime groups use social media to spread false information. This is done in an effort to confuse the public and put people at risk. They also utilize internet platforms to propagate pornographic material, virtual identity theft, phishing, and malware, as well as to coordinate the arms trade and narcotics trafficking, encourage human trafficking, and money laundering. All of this jeopardizes and exacerbates the impacted nation's security.[77]

To far, the Islamic-jihadist terrorist organizations have made the most extensive use of social media for their aims. AlQaeda often posts photos and videos of fruitful terrorist attacks on Facebook and YouTube to recruit and rise the number of people who support jihad, especially in the West. They also post martyr lists and biographies of people who died, as well as preaching or ideological literature. A person's behavior and willingness to take part in collective action can be changed by social media because of their socializing and recruiting functions, as well as because they enable social contact and the creation of social bonds, which can bring about changes in behavioral patterns over time, as well.[78] When people change their attitudes, they might start to follow the community's most common beliefs. Social media and the Internet in general make it easier for extremist ideas and information to spread, which can make people more likely to join. This can happen without the help of anyone else.

3.3 Social Media and Spread of Propaganda

Propaganda is a kind of communication that is intentionally deceptive and prejudiced in order to promote or advocate a certain point of view.[79] Propaganda is a kind of persuasion that uses the media, particularly social media platforms, to spread single-sided information.[80] One of the significant developing concerns, according to the World Economic Forum's Global Risks report, is the fast dissemination of deceptive and false information through social media networks. Unlike in the past, when communication and information sharing were accomplished via conventional

[77] Mayfield, Antony. "What is social media." (2008).

[78] Bowman-Grieve, L., & Conway, M. (2012). Exploring the form and function of dissident Irish Republican online discourses. Media, War & Conflict, 5(1), 71-85.

[79] Farkas, Johan, Jannick Schou, and Christina Neumayer. "Cloaked Facebook pages: Exploring fake Islamist propaganda in social media." *New Media & Society* 20, no. 5 (2018): 1850-1867.

[80] Phadke, Shruti, Jonathan Lloyd, James Hawdon, Mattia Samory, and Tanushree Mitra. "Framing hate with hate frames: Designing the codebook." In *Companion of the 2018 ACM conference on computer supported cooperative work and social computing*, pp. 201-204. 2018.

media, the widespread use of the internet has revolutionized the art of information dissemination, which propagandists have exploited. The internet is a vast sea of information that, unlike conventional media, is almost impossible to control and manage. Terror groups, crime syndicates, and people who don't want to be good people are taking advantage of the ease and wide reach of social networks to propagandize, and this has become one of the biggest threats to national security around the world because of strict social media regulations.

Islamist groups also use social media to try to make effective terror acts public and scare the public, so they can make the public more afraid of them. Because news and content can go viral on social media, this type of propaganda has the power to significantly outshine the media effect that traditional information and communication methods already have. This could lead to even more dangerous consequences than terrorist attacks, like transmitting news of a terrorist attack on communication platform infrastructure and services used by the stock market, which could cause panic. For example, al Qaeda has a well-thought-out plan for using social media platforms to spread propaganda to its adherents all over the globe in order to urge people to engage in criminal activity. This isn't all that the group does. They also use social media to make people afraid by posting news stories, gruesome pictures of beheadings, and other heinous acts. The Islamic State of Iraq and Syria (ISIS) streamed live on social media to show how they cut off a man's hand as an example of what they did.

US Congressional Research Service thought that some groups, mostly terrorist groups, could use social media to spread false information during or soon after a disaster like an earthquake, flood or nuclear reactor accident. This would make the damage seem worse, confuse people, and slow down emergency response and response times. In a study by the US Army, they say that social media could be used as a way for malware to get into computers or other mobile devices like smartphones and tablets. They may use social media platforms like Twitter and Facebook to spread their message and build their networks, but they can also hide harmful software in links and programs that could damage someone's computer.[81]

3.4 Social Media and Information Leaking

Social media has completely changed the way individuals receive and exchange information, resulting in a democratized communication infrastructure unlike any other. However, the strong

[81] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

invention has brought with it several major security dangers for both people and corporations. Among other things, social media is a major unprotected way for data to leak, encourages people to overshare private information, gives hackers information that helps them break into organizations, and allows people to spread false narratives in the context of misleading information or impersonation, among other things. [82]

Staff members have been alleged of spilling personal and private information through online social networking (OSN) in high-profile cases that have been talked about in the news. For example, an Israeli military officer posted the location and time of a planned raid on Facebook, which led to the whole thing being called off. Same thing happened in the UK 16 times. Ministry of Defense staff leaked British military secret info to the public through Facebook and Twitter. In the United States, a congressman who also serves on the House Intelligence Committee revealed that he had made a secret trip to Iraq by using his cell phone to "tweet" his arrival in Baghdad. He then revealed his location and the party's agenda every few hours. The enemies will undoubtedly benefit from the information that is revealed. The organizations, on the other hand, will lose out because of this.[83]

Irresponsible use of social media has a negative effect on businesses, placing their networks and systems at risk of malware, potentially resulting in copyright and defamation litigation, loss of productivity, and negatively harming their reputation and future income.[84] Cybercriminals have recently targeted OSN, not just to steal data, but also to leverage their storage and bandwidth for botnet command-and-control purposes. To make matters worse, Facebook profiles are now accessible for download via pirate sites, exposing the information of over 170 million users worldwide.[85] Another instance of social media platforms being used to breach security happened in the United Kingdom, when personnel from the Ministry of Defense released the country's security secrets to the general public through Twitter and Facebook. Four Indian senior navy

[82] Xiao, Fangjun, and Bernard Wong-On-Wing. "Employee Sensitivity to the Risk of Whistleblowing via Social Media: The Role of Social Media Strategy and Policy." *Journal of Business Ethics* (2021): 1-24.

[83] Mount, Matthew, and Marian Garcia Martinez. "Social media: A tool for open innovation." *California management review* 56, no. 4 (2014): 124-143.

[84] Bertot, John C., Paul T. Jaeger, and Justin M. Grimes. "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies." *Government information quarterly* 27, no. 3 (2010): 264-271.

[85] Bertot, John C., Paul T. Jaeger, and Justin M. Grimes. "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies." *Government information quarterly* 27, no. 3 (2010): 264-271.

personnel were charged of revealing sensitive information concerning the location of warships, weaponry, and patrolling routines in a similar case in India.

Furthermore, today's thieves are more interested in obtaining information and determining the worth of an enterprise than in infamously knocking down networks. Some of them are hired by other people to carry out very complicated attacks on workers of the companies they want to steal important information from. Public sources like online social media are used to get as much information about the important people as possible before they use spear-phishing and social engineering to get their passwords so they can get valuable information. Though cyber espionage and advanced persistent threats (APT) are not new, they are becoming more common because of social media, which makes them more dangerous.[86]

3.5 Social Media and Social Engineering

Social engineering is the skill of persuading individuals to give up their personal information, which may range from passwords to financial information. It's natural to believe that something like this would never happen to us or our company, or that we're immune to being duped, yet in 2016, 60 percent of people in the workplace were victims of social engineering. Individuals may be easily duped into giving out personal information, completing a legitimate-looking transfer, or even handing over access to their computer when they are targeted. Social engineering is used by criminals since it is much simpler to influence people into trusting them than attempting to break into their program.[87]

There are two ways that social engineering on social networks may function. First, there are cyber-attacks carried out on legitimate social media accounts. Second, there's the issue of information published on social media being utilized against a person or another in a different context. Social engineering efforts are most often carried out through email, but they may also take place over the phone (known as "voice phishing," or "vishing"), SMS (smishing), and messaging applications like WhatsApp.

These put an individual's or an organization's information security at risk. It's worth emphasizing that maintaining information security is critical, especially since failing to do so might result in a significant security breach that can harm the company or the person impacted. This is especially

[86] Culnan, Mary J., Patrick J. McHugh, and Jesus I. Zubillaga. "How large US companies can use Twitter and other social media to gain business value." *MIS Quarterly Executive* 9, no. 4 (2010).

[87] Tayouri, David. "The human factor in the social media security–combining education and technology to reduce social engineering risks and damages." *Procedia Manufacturing* 3 (2015): 1096-1100.

true today when the fear of terrorism looms large in the backdrop. Social engineering may take many forms. In certain cases, the criminal approaches the victim directly and attempts to get personal information over the phone or via social media sites. In other circumstances, the attackers approach a third party for sensitive information, such as executive assistants, office managers, or IT personnel. This strategy is used by criminals to get personal information such as birthdates. In certain circumstances, cyber thieves use this technique with others to attack and penetrate businesses and collect data. This puts the country's security at risk. Social engineering has been used by criminals for a long time to abuse human behavior and circumvent complicated and secure structures. According to a poll of the security industry, social engineering is one of the most popular hacking techniques.

Cyber thieves and invaders are modernizing the numerous methods by which they may obtain entrance to important resources, such as company information systems and personal information, which they can use for nefarious objectives and personal gain. Cybercriminals have lately taken advantage of people's thirst for news and social relevance to socially pressure them into disclosing secret material.[88] All of this jeopardizes the safety of people and the country as a whole. There have been several recorded incidents of social engineering resulting in catastrophic losses. For example, rising incidences of cybercrime, especially social engineering, cost companies in the United States $266 million in 2002. According to the results of research done by the San Francisco-based Computer Security Institute (CSI) and the San Francisco FBI, almost 90% of 273 participants discovered some kind of security violation in 2002 using social engineering.[89]

3.6 Social Media and Financial Fraud

Social media platforms are utilized for electronic financial fraud and hacking. Malware is used by cyber thieves to steal key banking credentials and transmit money. Hackers also employ ransomware to encrypt user accounts and then demand payment. Carberb, a Facebook-targeted virus that is concealed in PDF and Excel files and activates once opened, harvests crucial credentials for social networking sites and emails, is an excellent example of this.

[88] Oehri, Caroline, and Stephanie Teufel. "Social media security culture." In *2012 Information Security for South Africa*, pp. 1-5. IEEE, 2012.

[89] Wilcox, Heidi, Maumita Bhattacharya, and Rafiqul Islam. "Social engineering through social media: an investigation on enterprise security." In *International Conference on Applications and Techniques in Information Security*, pp. 243-255. Springer, Berlin, Heidelberg, 2014.

This malware not only steals personal information from users, but it also keeps their accounts hostage and demands a ransom. Ramnit is another virus that is mostly propagated via Facebook.[90] This virus is especially dangerous to businesses since it collects Facebook login information and allows the culprit to carry out different remote control operations. Spy Eye Trojan is another spyware that is used to commit financial crimes in the same way as Carberb is. Using stolen credentials, this malware has the capacity to obtain access to victims' bank accounts. This Trojan is not only able to take money out of an account, but this also covers the transfers from the account owner. It stops the account holder from getting balances. Instead, it substitutes the fraud cases with the account owner's transaction records, so the account owner only learns about the forgery only when a bank fails to permit transactions or sends the account holder a printed statement with all of the transactions.

17-year-old hackers and their friends broke into Twitter's network on July 15, 2020, and they took over lots of high Twitter accounts that they didn't own before. After a public hack, they took one high-profile account after another and tweeted that they were going to "double your bitcoin." The world watched for hours as they did this. There were a lot of people who had Twitter accounts that were hacked by the hackers. They also hacked into the Twitter accounts of a lot of businesses and politicians, like Barack Obama, Kim Kardashian West, Jeff Bezos, and Elon Musk. Twitter doesn't seem to be able to stop the breach for a long time, though.[91]

They took about $118,000 in bitcoin from the company. There are over 330 million people who use Facebook every month and over 186 million people who use it every day. This episode, on the other hand, showed how vulnerable this social media network is to hackers. Twitter is very important to how we communicate and share information. In the United States, more than half of all people get their news from social media "often" or "sometimes."

When hackers broke into Twitter's network and got access to internal tools that let them take over any Twitter account, it was very surprising.[92] Twitter is a $37 billion publicly traded technology company, so this was very unusual. Hackers also used more typical scam artist tactics, like pretending to be from Twitter's IT department and making phone calls to look like they were from

[90] Dong, Wei, Shaoyi Liao, and Zhongju Zhang. "Leveraging financial social media data for corporate fraud detection." *Journal of Management Information Systems* 35, no. 2 (2018): 461-487.

[91] Astutik, Danik, Iman Harymawan, and Mohammad Nasih. "The effectiveness of social media and press release transparency to detect indications of financial fraud." *Editorial Board* 1507 (2018).

[92] Zhang, Wei, Yi Li, and Pengfei Wang. "Can social media help deter financial fraud?." *Available at SSRN 3746118* (2020).

Twitter's IT department. The Hackers were able to get so much access to Twitter by using this simple method, which shows Twitter's cyber security flaws and could have huge consequences. There were no high-tech or complicated tools like malware, exploits, or backdoors used in the Twitter Hack.

Financial institutions in Kenya and throughout the globe are presently experiencing massive financial losses each year as a result of internet technology.[93] Banks and other financial organizations are now more exposed to phishing, identity theft, card skimming, viruses and Trojans, spyware and adware, social engineering, website cloning, and cyberstalking as a result of new technology. The Kenyan central bank's anti-fraud arm, for example, stated in 2011 that electronic financial fraud cost the country's financial industry about Kshs. 1 billion. This kind of fraud grew so frequent that, in 2011, over a dozen large institutions, both commercial and public, were hacked, including the Communication Commission of Kenya (CCK). All of them posed serious concerns to national security.[94]

3.7 Social Media and Cyber Laundering

The increased usage of the internet and social media platforms has also resulted in an increase in cyber-laundering incidents. This happens when cybercriminals use internet platforms to turn illegal financial transactions into untraceable cash. In this case, cyber thieves use money mules rather than direct means to transfer monies to their accounts. Money mules are those hired by cybercriminals to accept money that has been obtained illegally and then fraudulently channeled to the fraudsters.[95]

Malware Distribution through Social Media Because of their ease of use and wide reach, social media sites have become attractive targets for malicious assaults. People on social media exchange a lot of apparently benign information, which hackers and cybercriminals like to collect and use in their phishing and spear-phishing campaigns. On the other hand, cyber thieves are constantly improving their abilities to follow social network users and infect them with malware.[96] Because social media networks like Facebook and Twitter have such a big audience, fraudsters may infect

[93] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

[94] Kimutai, Julius K. "Social media and national security threats: A case study of Kenya." PhD diss., University of Nairobi, 2014.

[95] Wronka, Christoph. "“Cyber-laundering”: the change of money laundering in the digital age." *Journal of Money Laundering Control* (2021).

[96] Ibid p. 67

a vast number of people. As the globe grows more interconnected via the internet and other communication technologies, data security breaches have grown more common in recent years. Regardless, the danger of malware and viruses did not acquire momentum until the internet's widespread usage, which provided hackers and cyber criminals with an arena to test and hone their talents. As a consequence, there have been a rise in the number of examples of cyber criminals hacking websites, stealing data, or perpetrating fraud. All of these breaches in the organization's security have had an impact on the general public and national security.

Because of the increasing use of the internet and social media platforms in the current day, there have been countless incidents of malware assaults. Cyber thieves are now using social networking platforms to transmit computer viruses and malware, using specific tactics to obtain illegal access to other users' accounts and infect them. Hackers generate malware for a variety of reasons, one of which is to damage the government or for personal gain. Some of these assaults are designed to hurt the systems on which they are placed, while others are designed to seize control of the systems on which they are installed in order to target third parties. Others are designed to assist the perpetrators in stealing data from the particular system. All of attacks, especially those aimed against government entities, pose a major danger to the state's security.[97]

In 2005, a MySpace customer built a warm that allowed him to add a million contacts to his contact list, which was one of the most notable examples of social network security being hacked by malware assaults. This worm sent out a script to users who were looking for exploitable flaws so they could carry out nefarious activities including infecting cookies with malware and initiating SSL connections, among other things. A similar incident happened in 2006, when a worm was built and transmitted via the accounts of MySpace users, with catastrophic consequences. The spyware generated in this case infected every person that visited a certain profile. In 2007, Facebook was the target of yet another social media virus campaign. In this case, a guy pretended to be a teenager in order to entice youngsters and exchange harmful images with them in Illinois (USA). However, this individual was apprehended, and Facebook was heavily chastised for failing to safeguard minors. [98]

[97] Mikhaylov, Alexander, and Richard Frank. "Cards, money and two hacking forums: An analysis of online money laundering schemes." In *2016 European intelligence and security informatics conference (EISIC)*, pp. 80-83. IEEE, 2016.

[98] Meleshevich, Kirill, and Bret Schafer. "Online Information Laundering: The Role of Social Media." *Alliance for Securing Democracy, January* 9 (2018).

In December 2007, a Canadian porn company broke into the accounts of more than 200,000 customers. They were able to get information like user names, passwords, and email addresses. Social media users' information security was in a very bad way because of this. In another case, Russian agents used LinkedIn phishing to distribute malware to a number of various government agencies in the United States. The Russians used a bogus Harvard email account in this effort to try to disseminate malware to American government agencies and non-profit groups. The attackers generated a PDF document titled "Why American Elections Are Flawed." and injected malware into it in this assault that happened shortly after the US general elections. People were enticed to open the email using a false Harvard email address, which disseminated the virus.

This shows that cybercriminals may easily exploit and change the precise domain names of firms that aren't secured by email authentication. Another malware attack targeted Japan's parliament. The Japanese parliament was the target of a Trojan assault that originated in China. When one of the members of the Japanese parliament opened an email attachment, the computers and servers in the lower house were infected with viruses. The cyber attackers who carried out this act were subsequently discovered to have gained access to important passwords and other data on the affected systems. Taiwan is another nation that has lately been hit by malware assaults, with the majority of the attacks coming from China. Several hacking efforts have been made, with the primary goal of obtaining crucial and sensitive government data and information. In the majority of these instances, cyber thieves utilized Taiwan as a test bed for honing their cyber espionage abilities.

China has also been the target of a number of cyber-attacks. A strong malware assault, thought to have originated from highly experienced offenders, took down the internet services in one of the most significant cyber-attacks of 2013. This was the most serious cybercrime that the nation has ever seen. Another nation that has been subjected to a succession of malware assaults is the United Kingdom. The UK was one of the nations targeted by the WannaCry ransomware, which was transmitted by a gang of cybercriminals known as the Shadow Brokers, in May 2017. Hundreds of thousands of public utilities and huge enterprises were compromised by the virus utilized in this case. The country's National Health Service hospitals and infrastructure were among the most damaged sectors. Only two months after the Wannacry ransomware attack, another wave of ransomware outbreaks swept the globe. Petya, a more complex virus than Wannacry, was able to infect a huge number of vital government systems and certain organizations. Merck, a US pharmaceutical business, Maersk, a Danish shipping corporation, and Rosnof, Russian oil major, were among the hardest hit.[99]

3.8 Social Media and Revolutionary Activities

The speed with which information spreads through social media platforms is one of the primary reasons why platforms like Facebook and Twitter play such an important role in civil society, even fueling revolutions. Social media platforms were heavily utilized during the Libyan revolution to disseminate information and give coverage of events in the nation. Because the state controlled the conventional media outlets, social media networks became credible sources of information for the revolutionaries' supporters. [100]

YouTube was used a lot during the protests to show people what was going on in the streets. Social media and mobile tools like phones and tablets were important in the revolution because they helped rally more people and make the country less safe.[101] The Arab Spring is another example of how social media platforms were used to aid revolutions. The globe was thrown into disarray by the multitudes, who wanted their voices to be heard, through tweets, YouTube videos, and innumerable entries on Facebook and blogs. In this case, the revolution began in Egypt and expanded throughout Northern Africa and the Middle East in a short period of time.

[99] Wu, Chunying, and Juan Wang. "Analysis of Cyberterrorism and Online Social Media." In *4th International Conference on Modern Management, Education Technology and Social Science (MMETSS 2019). Atlantis Press*. 2019.

[100] Tudoroiu, Theodor. "Social media and revolutionary waves: The case of the Arab spring." *New Political Science* 36, no. 3 (2014): 346-365.

[101] Jones, Marc Owen. "Satire, social media and revolutionary cultural production in the Bahrain uprising: From utopian fiction to political satire." *Communication and the Public* 2, no. 2 (2017): 136-153.

CHAPTER FOUR

THE EFFORTS THAT THE GOVERNMENT OF KENYA HAS PUT IN PLACE TO DEAL WITH THREATS CAUSED BY SOCIAL MEDIA

4.1 Introduction

According to the results of this research, creating information technology and communication technologies has been one of the most important things humans have done for us in the last few hundred years. The rise of social media and the use of digital technology has had a huge impact on the way politics work on a global level because it has allowed people to express themselves in ways that were previously not allowed. Furthermore, it has given people more freedom of expression and made it easier for people to go to school.

As has been noted, despite its multiple advantages, the social media landscape is hampered by a number of issues. As a result, more attempts have been made to limit and control the use of social media platforms. Various governments and social media companies have come up with legal and regulatory initiatives to control and regulate the use of new forms of communication. These initiatives are meant to protect user privacy and intellectual property as well as national security and rackets as well as pornography and hacking.

Based on the results, there are ongoing debates taking place throughout the globe between governments and social media corporations about how to regulate social media platforms to safeguard the security of users, businesses, and the countries in which these sites are utilized. Because social media companies have such a large influence over what is communicated in cyberspace, it is critical that they take accountability for their content by prohibiting the spread of propaganda and false info, as well as any other activity that could be considered a threat to the security of users, businesses, or nations. For example, one of the social media firms, Facebook, openly discourages and prohibits hate speech, as part of its aim to provide chances for individuals to form strong bonds and so bring the globe closer together. To that aim, Facebook has been actively engaged in the removal of hate speech, which includes any material that publicly targets someone on the basis of their tribe or race or country or religious background or sexual orientation. Also on the basis of major deformities and illnesses.

4.2 Government Efforts

According to the results, governments play a critical role in establishing legislation to guarantee that information published on social media platforms corresponds to public decency standards. When objectionable information is discovered to be in violation of state laws, the government should take action to remove it from social media networks. Without such restrictions, the public and social media firms will be unable to take their obligations seriously, risking not only the user's security but also the nation's. The government of Kenya has taken various steps in curbing threats associated with social media. One of the steps taken by the government is the introduction of the cybercrime law.

As observed, the Computer Misuse and Cybercrimes Act was unveiled in May of 2018 in Kenya. This piece of legislation mainly purports to ensure that the use of computer systems for illegal purposes is prevented, and also to protect the confidentiality of users and data. In this act, there is a way to make sure that cybercrimes like unauthorized access to and interruption with computer systems by third parties, the spread of explicit material (especially involving children), cyberbullying, and the publishing of false news or false information are caught, investigated, and prosecuted as quickly and effectively as possible. The act's cybercrimes include very harsh punishments and fines. For example, publishing fraudulent information carries a fine of 5 million Kenyan shillings (USD$50,000) or a 10-year prison sentence. Unauthorized entry and tampering with state-protected computer systems is punishable by a 20-year prison sentence. However, the country’s security efforts have yet to find pace with policy recommendations, resulting in the Kenyan economy losing KSh 21 billion ($210 million) to cybercrime in 2017.

It was noted that Kenya as a country has also set up bodies that help in monitoring various activities taking place in different social media platforms. As an example, the Communications Authority of Kenya (CA), which was set up in 1999 by the Government of Kenya, is the country's regulatory authority for the communications sector. CA is in charge of "facilitating the development of the information and communications sectors," which include "television, electronic commerce, cyber security, multimedia, mobile communications, postal and courier services," among other things (CAK, 2018: para 2). Through the Communication Authority of Kenya, the government has been able to install and invest in quite sophisticated infrastructure and software to closely scrutinize and monitor social media platforms to ensure the country is safe.

As revealed by the findings another department is the ICTA (Information and Communication Technology Authority) under the ministry of ICT and youth affairs. The ICT Authority is in charge of rationalizing and simplifying the administration of all ICT services within the Kenyan government, including enforcing ICT standards and improving electronic communication oversight. The Kenyan government has also established the National Cohesion and Integration Commission to promote peace and combat hate speech, particularly that emerging from social media platforms. The National Cohesion and Integration Commission (NCIC) is a legislative agency created in 2008 by the National Cohesion and Integration Act No.12. A few of its functions include investigating discrimination complaints and recommending corrective actions to the Attorney General, Human Rights Commission, or other authorities if the charges are true. Any matter impacting ethnic and racial relations is also investigated on its initiative or at the request of any organization, office, or individual.

The NCIC and CA also issued guidelines in June 2017 (NCIC and CA 2017), which state, among other things, that political messages must not contain inciting, threatening, or discriminatory language that could lead to violence, hatred, or discrimination based on ethnicity, tribe, race, color, religion, gender, disability, or other factors. The NCIC has been vigorously pursuing hate speech suspects, calling a number of prominent figures and politicians for material on social media that was regarded to be nasty and dangerous to the country's peace, as well as for allegedly engaging in ethnic provocation. This has stifled ethnic provocation in public political discourse, including speeches by politicians and aspirants, as well as official campaign materials. Unfortunately, owing to a lack of expertise, political will, technology, and the capacity to control online hate speech, the NCIC has not been able to properly prosecute anybody for hate speech. Also, “Kenya has no laws in place to prevent crimes that are assisted by social media. “The social media law has not been completely implemented, and it seems that there is still a long way to go," says the author (DCI official, 2018). As a result, it is evident that the government still has a lot of work to do in order to effectively protect national security from dangers that arise on the country's numerous social media platforms.

As revealed by the study, another strategy by the government used to curb and minimize social media threats to national security is close monitoring of various groups formed on social media platforms and the content published and shared on social media platforms. This way, the authorities are able to identify the malicious social media accounts and to suspend them. Before, during, and after the elections, the Ministry of Interior and Coordination of National Government said that it would use crowdsourcing to monitor hate speech and incitement to violence in the country. According to the findings, this is a key milestone in the fight against social media misuse and enhancing the country's security, especially politically, considering the fact that in the recent past social media has been used in politics to create discord which has even resulted to violence. For instance: Many institution's evidence shows that hostile and divisive rhetoric was distributed through social media and digital technologies. Traditional and social media had a key influence in the escalation of violence both during and after the elections, according to the Waki Report on the 2007/08 post-election violence. The use of social media to spread bad ideas has resulted in a lot of bloodshed, which has put the country's security in jeopardy.

Furthermore, open-source intelligence (OSINT) is information gathered from publicly accessible sources. In Kenya, conducting OSINT for counter-terrorism, broader intelligence, and risk mitigation work has turn out to be a difficult and resource-intensive activity for both government and intelligence organizations, as well as the commercial risk management sector. The Kenyan government is engaged in a slew of open-source initiatives. Because criminal organizations, terrorist groups, enemy governments, and other rivals are increasingly using social media, continuous and extensive surveillance of these platforms may be used as a warning mechanism in the event of current or potential risks to national security.

4.3 Conclusion

From the above discussion, it is clear that the government has made various efforts in dealing with the threats emanating from the use of social media in the country. However, the government has a long way to go as the steps already made can be deemed as only baby steps. Since social media is here to stay and is bound to become part of every Kenyan life as various key sectors such as banking and education are embracing it, the government needs to put in even more stringent measures to curb not only the current threats arising from the use of social media but also future threats.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The study's summary is offered in this chapter in accordance with the research aims. The study's inferences and suggestions are also presented in this chapter.

5.2 Summary of the Study Findings

According to the findings, over the years the dominance of social media in Kenya has continued to grow and its presence can no longer be ignored. Over the past several years, the expansion and development of social media in Kenya has been linked to an increase in internet access and speed, as well as an increase in smartphone ownership in both urban and rural areas. The qualities of social media are well-known. Users may quickly connect with one another through social media platforms, which allow them to share various types of material such as videos, photographs, graphics, messages, and sounds, among other things. Social media also aids in the formation and strengthening of numerous networks, including professional, familial, social, cultural, religious, and political ones, as well as the development and definition of social identities.

As observed, Social media can be viewed as a double-edged sword not only in Kenya but the entire globe. This is because the use of social media is not only associated with positive effects but it has also brought about negative effects some of which have become serious security threats. Some of the negative effects associated with the use social media include: terrorism attacks, hacking, leaking of sensitive information, cyberbullying, cyber fraud and money laundering, livestock rustling, poaching, tribal clashes, information warfare and hate speech. Due to the threats arising from the use of social media, governments and the various social media firms have had to come up with various intervention measures and mechanisms in order to uphold the security of the users, the firms and the nations of the various governments involved.

5.3 Conclusions of the Study

Based on the findings the study concludes that social media dominance in Kenya is not only growing but is also becoming an important player in the Kenyan domain as the number of users continues to increase from individuals to firms and corporations and even the state. Despite the various benefits associated with the use of social media it also carries with it a myriad of negative effects that need to be addressed as they underscore the benefits of social media use.

It is clear from the study that a lot has to be done in regard to ensuring and enhancing social media security. More research needs to be done especially by the government on ways to enhance security pertaining to the use of social media. The government, via appropriate authorities, should keep a careful eye on terrorist social media activity and engage in a number of counter-measures. To deal with these threats, government agencies should be in charge of cyber security, which includes making policies, educating the public, and working with other governments and businesses. From the study conducted it is clear that there is still a huge policy gap when it comes to the use of social media in Kenya. More policies and laws regarding the use of social media and the internet need to be enacted by the state in order to enforce security in using the use of social media.

There is a lot of social media use that could be bad for peace, like hate speech, propaganda, or misinformation. Hate speech in society should be dealt with in a way that protects people's freedoms of association, accessibility, and freedom of speech. Although hate speech and the violence threats have a live, regulation of hate speech should not undermine freedom of expression. However, if there is an imminent risk of violence, it may be necessary to restrict information. The government also needs to ensure that these policies are well specified and not vague so as to ensure that there are no loopholes and that the perpetrators do not escape from the hand of the law.

Ignorance is no excuse, hence this study recommends that the government create more awareness among its people on the use of social media and its threats as most people fall victims due to ignorance. The government needs to sensitive people on the importance of being careful of the information that they share on social media sites as the internet never forgets and they always leave behind a digital trail. If not careful the digital trail they leave behind may be used by malicious groups or people to target them. In addition, the government needs to educate residents about the dangers of joining dubious social media sites or organizations with extreme agendas, as well as how to appropriately utilize social media. The public needs to understand that their security especially on social media starts with them.

5.4 Recommendations to the Study

Based on the above findings, the government and social media sites must improve data security and privacy rules. This will prevent leaking of sensitive information and access of this sensitive information by the wrong people.

The Kenyan government also needs to invest in training officers on social media guidance and closing the gap on the number of personnel equipped in dealing with threats emanating from threats in the use of social media. The government must invest both human and financial resources in strategic communication and social media research. To stay up with changing technology and social media trends, the training curriculum must be revised and repeated on a regular basis. In addition, security apparatus is required to build automated methods for gathering and evaluating social media that are adapted to certain work contexts.

According to the study, it is clear that security from the use of social media doesn't start with the government or the social media platforms but the users themselves. Social media users need to be more careful and cautious of the information they share on social media as this makes them targets to various social media security threats such as cyberbullying and fraud. The users need to be alert and be on the forefront in reporting malicious activities in the various social media sites to the government and the respective social media firms in order for the necessary actions to be taken.

Social media companies need to enhance the security of their sites in order to ensure the protection of the users and their data. This is important as it will protect them from malicious groups such as terrorist groups that are targeting unsuspecting users as their victims and perpetrators of their evil deeds. Likewise, these companies need to monitor the information that is being shared on their sites as they are responsible for the data being shared on their sites, and take the necessary actions on users found in violation of their terms and conditions.

The government of Kenya needs to ensure that the policies that are already in place concerning social media and the internet security are fully enforced in order to ensure the perpetrators are fully prosecuted and brought to justice. This will go a long way in discouraging others from engaging in such crimes thus reducing the threats emanating from the use of social media thus enhancing the security of the users and the entire nation as well.

Bibliography

Astutik, Danik, Iman Harymawan, and Mohammad Nasih. "The effectiveness of social media and press release transparency to detect indications of financial fraud." *Editorial Board* 1507 (2018).

Bertot, John C., Paul T. Jaeger, and Justin M. Grimes. "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies." *Government information quarterly* 27, no. 3 (2010): 264-271.

Bimber, Bruce. "Karl Marx and the three faces of technological determinism." *Social studies of science* 20, no. 2 (1990): 333-351.

Bradshaw, Samantha, and Philip N. Howard. "Online Supplement to Working Paper 2018.1 Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." (2018).

Bowman-Grieve, L., & Conway, M. (2012). Exploring the form and function of dissident Irish Republican online discourses. *Media, War & Conflict*, *5*(1), 71-85.

Chen, Yu. "Research on Social Media Network and National Security." In *Informatics and Management Science II*, pp. 593-599. Springer, London, 2013.

Chukwuere, Joshua Ebere, and Chijioke Francis Onyebukwa. "The Impacts of Social Media on National Security: A View from the Northern and South-Eastern Region of Nigeria." *International Review of Management and Marketing* 8, no. 5 (2018): 50.

Culnan, Mary J., Patrick J. McHugh, and Jesus I. Zubillaga. "How large US companies can use Twitter and other social media to gain business value." *MIS Quarterly Executive* 9, no. 4 (2010).

Dean, Geoff, and Peter Bell. "The dark side of social media: review of online terrorism." *Pakistan Journal of Criminology* 3, no. 4 (2012): 191-210.

Dong, Wei, Shaoyi Liao, and Zhongju Zhang. "Leveraging financial social media data for corporate fraud detection." *Journal of Management Information Systems* 35, no. 2 (2018): 461-487.

Gunawan, Budi, and Barito Mulyo Ratmono. "Social Media, Cyberhoaxes and National Security: Threats and Protection in Indonesian Cyberspace." *Int. J. Netw. Secur.* 22, no. 1 (2020): 93-101.

Hadžić, Faruk. "The influence of social media on threats to identity, stability and national security; institutional inefficiency and vulnerability of B&H." *SCHOLARLY JOURNAL FOR PROTECTION, SECURITY, DEFENSE, EDUCATION AND TRAINING ISSUES YEAR XXIV, NO: 45-46, 2020* (2020): 67.

Hossain, Md Sazzad. "Social media and terrorism: Threats and challenges to the modern era." *South Asian Survey* 22, no. 2 (2015): 136-155.

Jones, Marc Owen. "Satire, social media and revolutionary cultural production in the Bahrain uprising: From utopian fiction to political satire." *Communication and the Public* 2, no. 2 (2017): 136-153.

Kaigwa, Mark. "From cyber café to smartphone: Kenya’s social media lens zooms in on the country and out to the world." *Digital Kenya. An Entrepreneurial Revolution in the Making. London: Palgrave Macmillan* (2017): 187-222.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and national security*. Potomac Books, Inc., 2009.

Marima, Tendai. "Zimbabwe: Social media as a toxic tool or a future bridge to peace." In *Social Media Impacts on Conflict and Democracy*, pp. 205-215. Routledge, 2021.

Mayfield, Antony. "What is social media." (2008).

Meleshevich, Kirill, and Bret Schafer. "Online Information Laundering: The Role of Social Media." *Alliance for Securing Democracy, January* 9 (2018).

Mikhaylov, Alexander, and Richard Frank. "Cards, money and two hacking forums: An analysis of online money laundering schemes." In *2016 European intelligence and security informatics conference (EISIC)*, pp. 80-83. IEEE, 2016.

Mount, Matthew, and Marian Garcia Martinez. "Social media: A tool for open innovation." *California management review* 56, no. 4 (2014): 124-143.

Nerone, John C. *Social responsibility theory*. na, 2002.

Njamuku, Solomon M. "The Impact of Post 9/11 Film and TV Content on the National Security of Weak States: a Case Study of Kenya." PhD diss., University of Nairobi, 2016.

Nmah, Othello N. *Effects of Social Media on National Security*. US Army Command and General Staff College Fort Leavenworth United States, 2019.

Nothias, Toussaint, and David Cheruiyot. "A “hotbed” of digital empowerment? Media criticism in Kenya between playful engagement and co-option." *International Journal of Communication* 13 (2019): 24.

Oehri, Caroline, and Stephanie Teufel. "Social media security culture." In *2012 Information Security for South Africa*, pp. 1-5. IEEE, 2012.

Ogola, George. "Social media as a heteroglossic discursive space and Kenya's emergent alternative/citizen experiment." *African Journalism Studies* 36, no. 4 (2015): 66-81.

Sayler, Kelly M., and Laurie A. Harris. *Deep fakes and national security*. Congressional Research SVC Washington United States, 2020.

Sykora, Martin D., Thomas W. Jackson, Ann OBrien, and Suzanne Elayan. "National security and social media monitoring: A presentation of the emotive and related systems." In *2013 European Intelligence and Security Informatics Conference*, pp. 172-175. IEEE, 2013.

Thompson, Robin. "Radicalization and the use of social media." *Journal of strategic security* 4, no. 4 (2011): 167-190.

Tudoroiu, Theodor. "Social media and revolutionary waves: The case of the Arab spring." *New Political Science* 36, no. 3 (2014): 346-365.

Wambua, Immaculate M. "Impact of Social Media on National Security in Africa: Case Study Kenya." PhD diss., University of Nairobi, 2020.

Wilcox, Heidi, Maumita Bhattacharya, and Rafiqul Islam. "Social engineering through social media: an investigation on enterprise security." In *International Conference on Applications and Techniques in Information Security*, pp. 243-255. Springer, Berlin, Heidelberg, 2014.

Windsor, Duane. "Corporate social responsibility: Three key approaches." *Journal of management studies* 43, no. 1 (2006): 93-114.

Wolfers, Arnold. "" National security" as an ambiguous symbol." *Political science quarterly* 67, no. 4 (1952): 481-502.

Wronka, Christoph. "“Cyber-laundering”: the change of money laundering in the digital age." *Journal of Money Laundering Control* (2021).

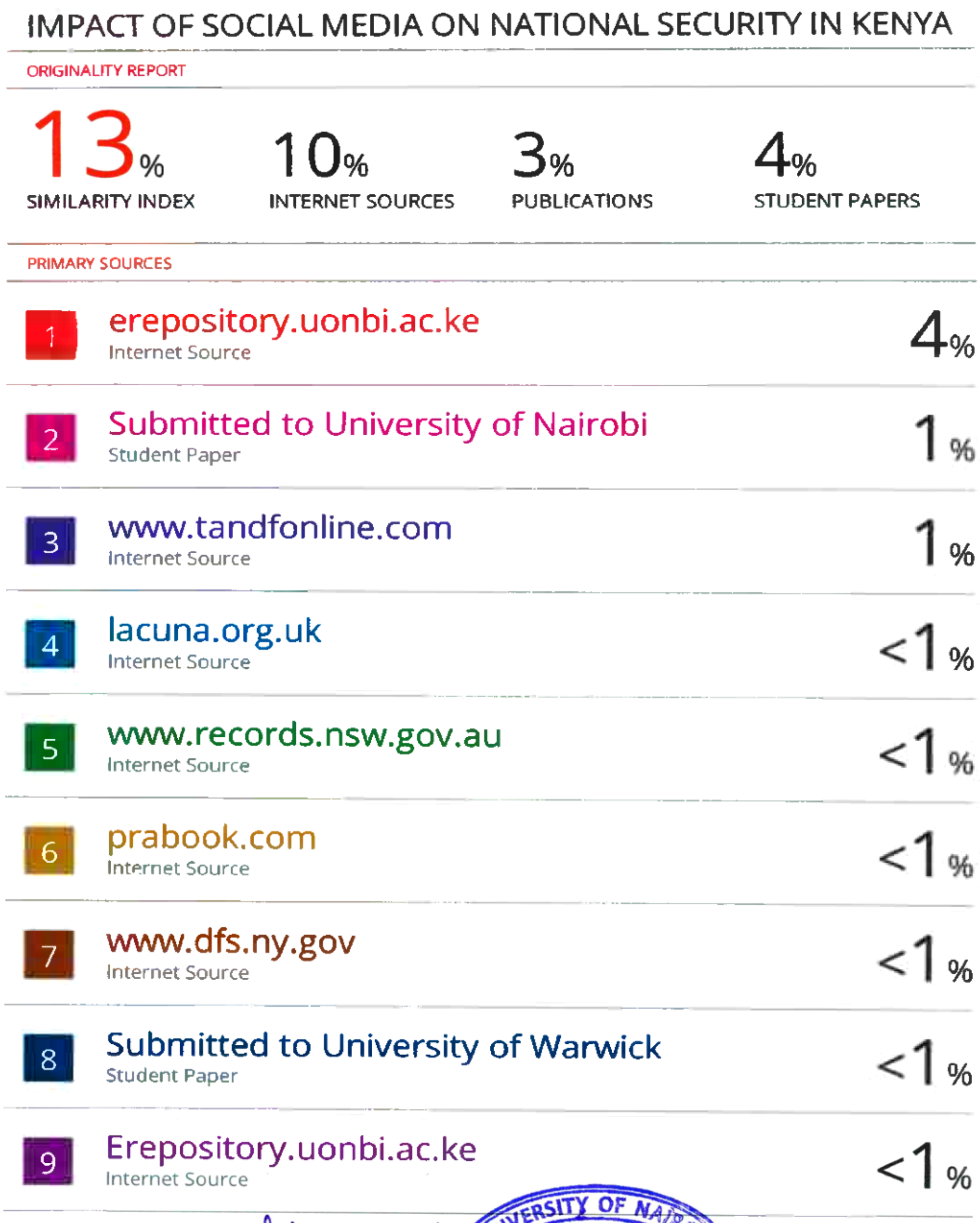
Wu, Chunying, and Juan Wang. "Analysis of Cyberterrorism and Online Social Media." In *4th International Conference on Modern Management, Education Technology and Social Science (MMETSS 2019). Atlantis Press*. 2019.

Xiao, Fangjun, and Bernard Wong-On-Wing. "Employee Sensitivity to the Risk of Whistleblowing via Social Media: The Role of Social Media Strategy and Policy." *Journal of Business Ethics* (2021): 1-24.

Zhang, Wei, Yi Li, and Pengfei Wang. "Can social media help deter financial fraud?." *Available at SSRN 3746118* (2020).

ANNEXES

Annex 1



IMPACT OF SOCIAL MEDIA ON NATIONAL SECURITY IN KENYA

ORIGINALITY REPORT

13%	10%	3%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	erepository.uonbi.ac.ke Internet Source	4%
2	Submitted to University of Nairobi Student Paper	1%
3	www.tandfonline.com Internet Source	1%
4	lacuna.org.uk Internet Source	<1%
5	www.records.nsw.gov.au Internet Source	<1%
6	prabook.com Internet Source	<1%
7	www.dfs.ny.gov Internet Source	<1%
8	Submitted to University of Warwick Student Paper	<1%
9	Erepository.uonbi.ac.ke Internet Source	<1%

UNIVERSITY OF NAIROBI
APPROVED
DATE: 15/9/2022
SIGN:..............
INSTITUTE OF DIPLOMACY INTERNATIONAL STUDIES