ROLE OF SOCIAL MEDIA ON SECURITY MANAGEMENT: A CASE OF THE KENYA NATIONAL POLICE SERVICE KILIMANI AND DAGORETTI POLICE DIVISIONS

JERUSHA NOORETET LOONKOSHO

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTERS DEGREE OF GOVERNANCE, PEACE AND SECURITY IN THE DEPARTMENT OF GOVERNANCE PEACE AND SECURITY STUDIES SCHOOL OF HUMANITIES AND SOCIAL SCIENCES OF AFRICA NAZARENE UNIVERSITY.

JUNE 2022

DECLARATION

I declare that this thesis is my original work and that it has not been presented in any other university for academic credit.

Signature……Date…22nd June 2022…

Name of Student: Jerusha Nooretet Loonkosho

Student No: 19S01DMGP009

SUPERVISORS' DECLARATION

This thesis is submitted for examination with our approval as the University Supervisors.

Signature……...Date…22nd June 2022…

Name of Supervisor: Dr. David Muthondeki

Signature……..Date…22nd June 2022…

Name of the Supervisor: Dr. Dennis N. Wamalwa

DEDICATION

I dedicate this thesis to the almighty who has been my pillar and source of strength without him I wouldn't have made it, Glory to his name and to my boys Amani and Tajeu

ACKNOWLEDGEMENTS

A special thanks to My Supervisors Dr. David Muthondeki and Dr. Dennis Wamalwa for their countless hours of reflecting, reading, encouraging, and most of all patience throughout the entire process. Their willingness to provide feedback made the completion of this research an enjoyable experience. I would like to acknowledge and thank African Nazarene university for allowing me to conduct my research and providing any assistance requested. Special thanks go to the H.O.D Dr. Emily Okuto for her continued support throughout this project. I would like to thank the lecturers that assisted me with course work being the preliminaries to this thesis proposal. I also make special acknowledgement to my family, to my parents and sister Diana You have always encouraged me that no matter what I will do it, your prayers and love have kept me going even when I was ready to give up, to you have been my motivation and the reason I have always wanted to work hard and excel. Last but not least to my friends especially Timothy your help has been tremendous may God richly bless you.

ABSTRACT

There are many aspects that have given rise to the usage of social media in Kenya today such as smart phones and internet connectivity. The availability of cheap digital mobile devices, wide coverage of internet connectivity by various network providers and variety of digital content are some of the main reasons for increased social media usage. Social media platforms have been used to fuel and quench violence or riots in different ways. Therefore, the National Police Service and other security agencies must monitor the social media platforms and analyse their dynamics so as not to be caught unaware in case of offensive usage of social media by criminals and terrorists. The purpose of this study was to assess the role of social media on security management in Kenya. The objectives of this study were to analyse the use and effectiveness of using social media in Security Management, to evaluate security challenges posed by Social Media technologies in Security Management, to investigate the policies that guide NPS in using social media for Security Management. The study employed collective approach theory and social responsibility theory. The study employed descriptive research design where 188 police officers formed sample size in police stations within Kilimani and Dagoretti Police Divisions through proportionate sampling. The empirical data was collected by use of questionnaires while secondary data was gathered from existing literature both print and non-print. Professional advice was sought on data collection instrument to ensure their validity while Cronbach alpha score was used ensure reliability. Quantitative data was analysed using the SPSS output for descriptive statistics while qualitative data was analysed thematically as per study objectives. The study established that Social Media was greatly used in information dissemination, creating public awareness, crime reporting and intelligence gathering. Lack of digital infrastructure and training were the main challenges encountered by police officers as far as SM was concerned. Existing policies were not well understood and insufficient in convictions of SM offenders. The study recommended additional funding NPS to aid in acquisition of advance digital technologies to boost already existing infrastructure. The study also recommended in-house training of officers on dynamics of social media, tools and on policies.

TABLE OF CONTENTS

DEDICATION ..... **iii**

ACKNOWLEDGEMENTS ..... **iv**

ABSTRACT ..... **v**

LIST OF TABLES ..... **ix**

LIST OF FIGURES ..... **x**

OPERATIONALIZATION OF TERMS ..... **xi**

ABBREVIATION/ ACRONYMS ..... **xii**

CHAPTER ONE **1**

INTRODUCTION AND BACKGROUND OF THE STUDY **1**

1.1 Introduction 1

1.2 Background of the Study 1

1.3 Statement of the Problem 7

1.4 Purpose of the Study **8**

1.5 Specific objectives 8

1.6 Research questions 8

1.7 Justification of the study 8

1.8 Scope of the Study 9

1.9 Delimitations of the Study 9

1.10 Limitations of the Study 10

1.11 Assumption of the study **10**

1.12 Theoretical Review 10

1.12.1 Collective Security Approach Theory 11

1.12.2 Social Responsibility Theory (SRT) 11

1.13 Conceptual Framework 13

CHAPTER TWO **15**

LITERATURE REVIEW **15**

2.1 Introduction 15

2.2 Effectiveness of Social Media on Security Management 15

2.3 Challenges of Social Media on Security Management 19

2.4 Policies that guide NPS in using Social Media on Security Management 27
2.5 Summary of Literature Review and Research gaps 31
CHAPTER THREE **33**
RESEARCH METHODOLOGY **33**
3.1 Introduction 33
3.2 Research Design 33
3.3 Research site 33
3.4 Target population 33
3.5 Sample and Sampling Technique 34
3.6 Instrument 35
3.7 Piloting Study 36
3.7.1 Validity of the Research Instruments 36
3.7.2 Reliability of the Research Findings 37
3.8 Data Collection Procedure 37
3.9 Data Analysis and Presentation 37
3.10 Ethical Considerations 38
CHAPTER FOUR **39**
DATA ANALYSIS AND FINDINGS **39**
4.1 Introduction **39**
4.2 Response Rate **39**
4.3 Demographic Information of the Respondents **40**
4.3.1 Gender 40
4.3.2 Police Division 40
4.3.3 Numbers of years in service 41
4.3.4 Social media Platform for personal use 42
4.4 Presentation of Research Analysis and Findings **43**
4.4.1 Effectiveness of using Social Media in Security Management **43**
4.4.1.1 National Police Service on Social Media 43
4.4.1.2 Social media platforms used by NPS 43
4.4.1.3 Social Media for work related purpose at NPS 44
4.4.1.4 Police unit responsible for monitoring use of Social Media 45
4.4.1.5 Effectiveness of Social Media in various constituents 46
4.4.2 Challenges in Use of Social Media on Security Management **49**
4.4.2.1 Challenges in Use of Social Media 49

4.4.2.2 Challenges orchestrated through use of social media 51
4.4.3 Policies pertaining use of social media on security management **53**
4.4.3.1 SM policies Availability in NPS 53
4.4.3.2 Statements on Policies 54
4.4. Influence of social media on security management **57**
4.4.1 Level of insecurity attributed to offensive use of social media 57
4.4.2 Statements on Influence of SM is security management 58
CHAPTER FIVE **61**
DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS **61**
5.1 Introduction **61**
5.2 DISCUSSIONS OF THE STUDY FINDINGS **61**
5.2.1 Effective use of Social Media in National Security Management 61
5.2.2 Security challenges posed by Social Media on National Security Management 62
5.2.3 Policies that guide NPS in using social media on Security Management 64
5.3 Summary of Main Findings **65**
5.4 Conclusions **66**
5.5 Recommendations **67**
5.6 Areas of Further Research **67**
REFERENCES **68**
APPENDICES **72**
APPENDIX I: INTRODUCTION LETTER **72**
APPENDIX II: CONFIDENTIALITY AGREEMENT **73**
APPENDIX III: QUESTIONNAIRE **74**
APPENDIX IV: RESEARCH PERMIT NACOSTI **81**
APPENDIX V: UNIVERSITY RESEARCH LETTER **82**

LIST OF TABLES

Table 3.1 Target population....34
Table 3.2 Sample Size....35
Table 4.1 Response Rate....39
Table 4.2 Gender....40
Table 4.3 Police Division....40
Table 4.4 Years served NPS....41
Table 4.5 Social Media tools do you use for personal interactions....42
Table 4.6 Social Media on Security Management....43
Table 4.7 Social media platforms used by NPS....43
Table 4.8 Who is allowed to use Social Media for work related purpose at NPS....44
Table 4.9 integrated police unit for monitoring SM....45
Table 4.10 effectiveness of Social Media....46
Table 4.11 Challenges in Use of SM....49
Table 4.12 Challenges orchestrated by SM....52
Table 4.13 Policies guiding in use of SM....54
Table 4.14 Statements on Policies....55
Table 4.15 Level of insecurity attributed to SM....57
Table 4.16 Influence of SM is security management....58

LIST OF FIGURES

Figure 1.1 Conceptual Framework……..15

OPERATIONALIZATION OF TERMS

Security Management: This study defines security management as structures and mechanism put in place to ensure national security

Social Media: This study defines SM as a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0 and that allow the creation and exchange of User Generated Content.

Social Interactions: They are defined as the communication among users through social media and for the purpose of this study this definition will be used

Social Network Sites: These are web-based services that allow individuals to construct a public or semi-public profile within a bounded system; articulate a list of other users with whom they share a connection, and view and traverse their list of links and those made by others within the system.

Social Media Use: This is the frequency of a user's contribution, retrieval, and exploration of content within a social media site and the meaning thereof will be used in this study.

Social Media Engagement: This is the process of gaining traffic or attention in social media network sites as follows, likes tweets, tags and shares. This study will adopt this definition.

Social Media Measurement: As far as this study is concerned, SMM means the way of computing popularity of a brand or company by extracting information from social media channels, such as blogs, wikis, news sites, micro-blogs such as Twitter, social networking sites, video/photo sharing websites, forums, message boards and user-generated content from time to time

ABBREVIATION/ ACRONYMS

ALPR: Automatic License Plate Readers

BWC: Body Worn Camera

CSAT: Collective Security Approach Theory

ICT: Information Communications Technology

IT: Information Technology

NACOSTI: National Commission for Science, Technology and Innovation

NPS: National Police Service

SM: Social Media

SPSS: Statistical Package for Social Sciences

SRT: Social Responsibility Theory

STI: Science & Technology and Innovations

CHAPTER ONE

INTRODUCTION AND BACKGROUND OF THE STUDY

1.1 Introduction

This chapter looked into the background of the study, statement of the problem, the objectives and significance of the study; scope, limitations and de-limitations of the study, and conclude the chapter with conceptual framework.

1.2 Background of the Study

Mobile technology and internet proliferation has changed the current interactions and communications in the society. The growth and development of Web 2.0 has given birth to development of new technologies that has greatly influenced the interactions globally through wireless networks. It's without a doubt that social media use has been adopted by organizations of diverse type and size and individuals both for good and evil agendas. Ngige, Badekale, and Hamman (2016), argued that social media have been used to fight global terrorism and in the same manner it has been used by criminals and terrorist to plan and execute atrocities.

Invention of Web 2.0 gave birth to advanced technological knowledge which has powered social media platforms in the 21st century. Human communications and interactions in our modern times have been redefined by the advancement of digital technologies bringing new skills and knowledge. According to Trottier and Fuchs (2014) social media can be said to be internet based services which allows an individual to connect with others, know their thoughts and how they are faring on as well as their connections. The 21st century greatest technological invention and innovation is social media by the virtue of revolutionising information access, bringing people closer, enabled sharing of skill and knowledge. Sajithra and Patil (2013) further regarded Social Media as online centred applications put up on the Web 2.0 platform ideal for creating and sharing contents from individual users. They further described Web 2.0 as a platform which enables people to create content and permit the constant dissemination of

information changes by others (Sajithra and Patil, 2013). This study regards social media as applications on Web 2.0 platform which links people through information, knowledge and other informatics dissemination.

There are various diverse kind of SM networking sites, for example Tiktok, Facebook, Twitter, WhatsApp, Google Plus, Yahoo Messenger, Instagram, and Wikipedia among many other platforms. These social media tools have impacted social, economic, cultural and political aspects of humanity in such that, events are held virtually with larger audiences. The adverse side of social media applications tools is that, they have also been the channel to promote and spread rumours, propaganda and fake news (Nsudu &Onwe, 2017).

Globally, 4.48 billion people equivalent to 57% of total global population were using social media in 2020, (Kemp, 2021). The number of social media users in North Africa was 45% of the total population in 2020 while South African countries it was 41% (Kemp, 2021). According to PEW research centre (2020) seven out of ten Americans engaged the use of social media with young people being the early adopters. According to CAK (2019), there were 45.7 million Kenyans who had subscribed to internet services. SIMELAB (2018) report on social media consumption in Kenya established that, 88.6% used WhatsApp and 88.5% were subscribed to Facebook. The top motivations behind using these social media platforms were; acquiring information that is news, exploring and knowledge 31%, entertainment and pleasure 28%, and social interactions 24%. Further investigation revealed that, majority of Kenyans used mobile phones to access social media and few especially in rural areas used cyber café. Consumption of social media was high during the night where entertainment, blogging and education contents were mostly consumed, (SIMELAB 2018).

Social media has become the tool for online discussions where politics, social, cultural, economic and even scholarly debates takes centre stage. The power of social media cannot be

underestimated. 66% of Kenyan has engaged SM while its consumers spend an average of three hours daily online, (SIMELAB 2018). Therefore, security organs should find ways to exploit these platforms in security management in this digital era.

Social media is very wide and hard to define because it encompasses tools and applications over a network to allow the connection between two or more individuals and/or entities (Trottier & Fuchs, 2014). They further argued that, social media collects values of individual and societies facilitating cognitive behaviours just like artificial intelligence machines do. Social media is a communication apparatus for it lets new friendship to form and hook up, societies, individuals and corporate connections while existing ones are maintained. According to Cann (2011) social media is web-based applications which permit users to create personal contents for service and other agendas; meaning social media facilities virtual communities allowing discussions and events planning over the internet, for example Facebook live and WhatsApp video calls.

The presence of social media usage poses a security challenge because some use to promote propaganda, fake news, events and other mass dynamics. According to Cann (2011) and Nsudu and Onwe, (2017) social networking platforms are used to empower their users to develop content and communicate. New opportunities for collaboration and interaction between producers and consumers, government and public have been created by these technologies (Barker, 2012). In the business world, businesses and organizations have created social media pages to advertise their products and for general information sharing. The Kenya national police service too has social media pages where issues regarding public safety and security are shared and the public can also report crime through these social media pages.

Missauoi (2015) ascertained the fun and colourfulness social media platforms have accorded users as an alternative communication tool deepening personal relationships and activities.

These activities give the users opportunities to interact by participating, sharing, collaborating, conservations and linking. The use of social media since inception and for the last few years has extensively been used to promote and pursue personal objectives. At the click of a button, an individual can share an idea/opinion, follow, learn, collaborate and interact with others in faster, convenience and efficient manner than it could be done in the past decade. Internet proliferation has enabled social media platforms be readily available for users who have limitless possibilities of interaction over the internet. Social media platforms have enabled users to record videos, messages and share them reaching a wide audience (Nsudu & Onwe, 2017). Gad (2017) noted that, videos circulating online of an event which had occurred often triggered riots or solicit help for the victim.

In London riots, according to Ghonim (2012) police used social media with the help from the public to quell rioters who had turned to be looters and improve security. The technology of CCTV cameras was used to capture photos of looters and rioters and the images shared on social media platforms helping with apprehension of perpetrators, (Ghonim, 2012). This is in contrast with what happened in Arab uprising where social media was used to fuel riots, in London it was used to quench them. Therefore, social media can be used in management of national security if used comprehensively. Use of web applications has evidently been used by some agencies to curb crime. For example security agencies used Pinterest to recover stolen property, identify looters leading to their arrests and alerting neighbours of a nearby larceny or break-in by pinning photos of criminals caught on camera (Ericksen, 2014).

In Tunisia and Egypt Cuman (2012) did a research study on the role internet and social media plays in transnational relations with precise attention of Arab revolution in these North Africa Arab countries. The study documented the usage and the role of social media networks for instance the Facebook, Twitter, YouTube and weblogs in aiding uprisings in Egypt, Tunisia and Syria. It was established by the study that, the proliferation and use of social media in those

Arab countries facilitated in mobilising mass protesters, opinion shaping to influence change, empowering and boosting morale of protesters. Since then, those Arab regions have are continually facing domestic conflicts giving birth to political instability. It can be observed that, such social unrest have detrimental effect on social, political, cultural and economic dynamics of a nation. The actual cause of Arab spring revolution was not social media but it was the tool that was used, (Ghonim, 2012).

In Kenya, Kimutai (2014) did a study on social media and national security threats targeting its use in military units. The study revealed that, social media was used to spread hate messages, aid in cattle rustling, organize criminal activities, poaching and terrorism. Ndonye (2019) also did a study on the implications of technological advancement on performance of police officers. Her study which focused on railway police unit established that, there was use of digital technologies though not advanced and neither superior to detect and prevent crime. The study focused on police performance and therefore cannot be generalized to include security management. Social media have been found to have been used in planning and facilitating terrorism and other criminal activities across Kenya (Ndonye, 2019).

During electioneering period in Kenya, there are heighted tensions among the citizens. In the 2007/08 post-election conflict, social media was not as available as it is today but phones were used in communication by calling or sending SMS which either fuelled violence or saved lives. However, in 2013 electioneering period, the extreme inflammatory speeches posted online rose from 197 to 321 for the period between February and March same year. The offensive messages were mostly circulated through Facebook, (Umati, 2013). Other general messages which were not offensive but had ulterior motives rose from 122 to 405 of the same period, this was recorded by Umati an online monitoring firm. Makinen and Kuira (2018) observed that, during election period heightened political events arouse hatred among different tribal dialects. They further established that, those social media platform were used to channel prejudices based on

tribes, biased and false information and hate speech. Social media platforms acted as a catalyst to both ethnic based conflicts and mass media communication tool for peace campaigns after elections. Wamungai (2010) found that, SMS were mostly used in post-election violence in 2007/08 where messages sent via mass email were reduced in size to be an SMS. He also established that, messages shared across communication networks then were fed on rumours and misinformation from the press. Increased sending of SMS prompted the government to issue a stern warning to prosecute those found sending hate messages despite having weak legal legislation.

The Constitution of Kenya 2010 gave provisions for the creation of the National Police Service. Further, provisions were made namely; the National Police Service Act 2011 and the National Police Service Commission Act 2011. The National Police Service consists of following in accordance to the above provisions: The Kenya Police Service; The Administrative Police Service; and The Directorate Criminal Investigation.

The National Police Service is under the independent command of the Inspector General, while each arm is headed by deputy inspector general. Since social media platform are used for mass communication, the NPS has embraced their use by opening Facebook and twitter official pages. In additional to social media platforms, the NPS has expanded its communication network by improving broadband of hotline numbers which are 999, 112 and 911 which public can call at any time to report crime or seek help. NPS has towed the line and adopted social media platforms to communicate to the general public official IG's messages which are authentic and official.

According to Communications Authority of Kenya (2020), there was detection of 13.9 million cyber-attack threats between April and June and 34.6 million for the period between January and March all in year 2020. The attacks were in form of malware, botnets, system

vulnerabilities and web application attacks. These cyber-attacks targeted mainly financial institutions with aim to siphon money.

There is therefore need for in-depth study to examine how social media have influence on security management; its effectiveness both negative and positive, challenges faced, threats posed and legal mechanism available to guide and control the use of it before it happen as Chinua Achebe said “things fall apart”.

1.3 Statement of the Problem

The exponential growth in use of social media has given the public great opportunities to interact and share opinions. Information sharing has been the main motivation for using social media platforms, promote peace and advertise business which is good for national growth and development. Social media offers many benefits than threats posed; therefore studies should be carried out on how NPS can get the very best out of social media for both national security and gross domestic growth. However, subversive elements such as terrorist organizations like Al-Qaeda, Boko-haram and Al-Shabaab have used the same social media platforms in disseminating propaganda, recruiting and radicalizing targeted audiences. Other criminal elements and non-state actors with bad motives have used social media to carry out cyber-attacks, with aim of demanding for ransom and spreading propaganda (Nsudu & Onwe, 2017). Since the Social media platforms have been used to fuel and quench violence and riots in different ways, the National Police Service and other security agencies must monitor the social media platforms and analyse their dynamics so as not to be caught unaware in case of offensive usage of social media by criminals and terrorists.

There were studies done on influence of social media with respect to business enterprises (Morgan, 2017; KMPG, 2016), but there was very little information on security management. Ndonye (2019) and Kimutai (2014) in their research studies did not use variables that will be used in this study that is effectiveness and policies guiding. There is very little literature on the

policies governing NPS on the use of social media on security management warranting a study to be conducted to fill this gap. It is against this background that this study sought to fill empirical gap on the influence of social media on security management with special reference to the National Police Service.

1.4 Purpose of the Study

The aim of this study was to assess the role of social media on security management in Kenya with specific reference to National Police Service

1.5 Specific objectives

i. To assess NPS the use and effectiveness in using social media for Security Management in Kilimani and Dagoretti police Divisions.
ii. To examine the policies that guide NPS in using social media on Security Management in Kilimani and Dagoretti police Divisions.
iii. To evaluate Security challenges of Social Media technologies on Security Management in Kilimani and Dagoretti police Divisions.

1.6 Research questions

i. How does NPS find the use of Social Media effective in National Security Management in Kilimani and Dagoretti police Divisions?
ii. What are some of policies that guide NPS in using social media on Security Management in Kilimani and Dagoretti police Divisions?
iii. What are the security challenges posed by Social Media on National Security Management in Kilimani and Dagoretti police Divisions?

1.7 Justification of the study

Justification can be referred to as rationale or significance of the study which aim to convey the relevance and the reason why the research is being conducted. The when completed may

be useful to National security organs in identifying threats posed by social media use and misuse. The findings will inform new strategies in addition to those in place. The findings will help policy makers to identify legislation gaps and loopholes that need to be filled mostly in prosecution of individuals who use social media to undermine national security. To the academicians and scholars, the finding of this study will add to the vast body of knowledge in existing theories.

1.8 Scope of the Study

Scope of the study is the extent and parameters of which the research study will be conducted, how and where. The study was limited in scope to Kenya National Police Service officers based in six police stations in Kilimani and Dagoretti police Divisions. The study focused on investigating the influence of social media on security management in Kenya. The researcher used available secondary data from and primary data which was be collected by use of questionnaires which were distributed to 188 respondents in Kilimani and Dagoretti Police Divisions. The researcher also interviewed two senior police officers in the same police divisions.

1.9 Delimitations of the Study

Delimitation is a confined population area in which a study is conducted (Mugenda & Mugenda, 2012). For the purposes of data collection this research study did not interview entire national police service. The study did not look into other factors in regard to national security which will but will use. For data analysis, the study used filled questionnaires which the respondents filled them honestly and truthfully since of their work culture. The police community is like a closed society and getting desired information and at a faster pace might be difficult.

1.10 Limitations of the Study

Mugenda and Mugenda (2012) defined limitations as the conditions beyond the control of the researcher that may place restrictions on the successful accomplishment of the study and their application to other situations.

The police work culture demand secrecy due to information deemed classified. The researcher informed the respondents of the significance of the study and assured them that the information provided was to be used only for research and academia purposes as guaranteed in confidentiality agreement in appendix v.

The measures put in place by the ministry of health were observed while conducting the research especially on data collection. The measures included, observing physical distance of two meters, washing hands regularly and using hand sanitizers, and wearing a face mask.

1.11 Assumption of the study

The study assumed that, social media can have influence in security management. It also assumed that, effective use of social media can have a positive impact on national security management.

This study assumed that, data will be collected without hindered by COVID-19. The study also assumed that, he respondents will be willing to share information even though police culture entails living in a closed community.

1.12 Theoretical Review

According to Michael (2009), theoretical framework can be regarded as reasoned set of prepositions. These prepositions support and explain a phenomenon based data or evidence derived. This study will be based on two theories namely; Social Responsibility Theory and Collective Security Approach Theory.

1.12.1 Collective Security Approach Theory

Collective Security Approach Theory (CSAT) was first proposed by Immanual Kant (1724-1804) as an alternative to power balance approach theory (Williams, 2010). It was not until World War 1 that the theory grew root and its theoretical foundations used to established United Nations and the League of Nations. One of the proponents of this theory is White (2003) who termed it as National Security Law. National security when managed by some transcendent authority from above in CSA is seen like a side benefit of global security and order.

The basic idea was to relieve nations to provide security by themselves especially poor nations which had the burden of war while stronger ones continued in arm race. The theory will be useful in this research study because, security management is complex and cannot be handled by one nation single handed but calls for collaboration of nations. National security has many players for example, police, administrators, intelligence and security researchers who can embrace collective security approach theory to deter insecurity in various fronts. Under CSAT, countries can have agreements on tackling common security challenges.

Collective Security Approach Theory gives more weight on security organs in nations without addressing the responsibility of citizens as regard to constructive use of available channels of communications and for the case in this study, social media. This theory focuses on policing which can create unhealthy power concentration in police and security actors because citizens must be accountable for information they create, share and distribute on social media platforms without being policed thus creating need for another theory that targets citizens' responsibilities on the use of social media.

1.12.2 Social Responsibility Theory (SRT)

The Hutchins Commission on Freedom of the Press projected the social responsibility theory and it was introduced in 1947. In SRT the media should serve the public freely from government interference in order to fulfil their mandate. In theory, there would be no need for government to regulating the media and its participation in dispersing reports and information

to the public when the producers of contents prove to be responsible. The theory also proposes that, public must be digital literate.

The guidelines that the media is obligated to follow in serving the public are defined in Social responsibility theory. There are various precepts claiming that the media can regulate itself by adhering to them, they are: preserving freedom in a democratic society is an obligations media to fulfil; self-regulation is a must for media; professionalism and objectivity in the highest standards should be maintained by the media, as well as truth and accuracy; diversity of the cultures presented by the media should be well reflected; lastly the community is in the right to anticipate that media acts professionally.

The reporters and media producers are not the only one social responsibility fall upon. Consumers too have the responsibility of becoming knowledgeable of the media while maintaining realistic expectations from media. In the social responsibility theory, government regulating and intervening in media's work should not be heard to the public if the stated media accountability and responsibilities happen.

Shuchman and Wilkes (2017) in explaining what it meant by press being accountable to the society and that, the media services should be geared towards the improvement of the society. They analysed the effectiveness of communication between medical scientists and health news reporters, their analysis ascertained that, when journalists failed to be precise and identify crucial interests on stories follow-up the covering of imperative health issues had adverse consequences in regard to civic knowledge.

The existence of code of ethics is the basis of self-regulation in media. The impact of actual ethical values in media firms is generally questionable, by the fact that, some quota of media practioners are not in full awareness of the content they create, and the other reason is that, there is no proper structure safeguarding against violation of code of ethics. Media can control these types of preventive procedures while participating in its duty toward the public as the

first step in self-regulation. However, applying appropriate laws in the media to enforce social responsibility has remained a controversial debate.

These two theories complement each other as Collective Security Approach focuses more on security actors in security management while Social Responsibility Theory focuses on citizen's responsibility in content creation and dissemination thus targeting the use of social media

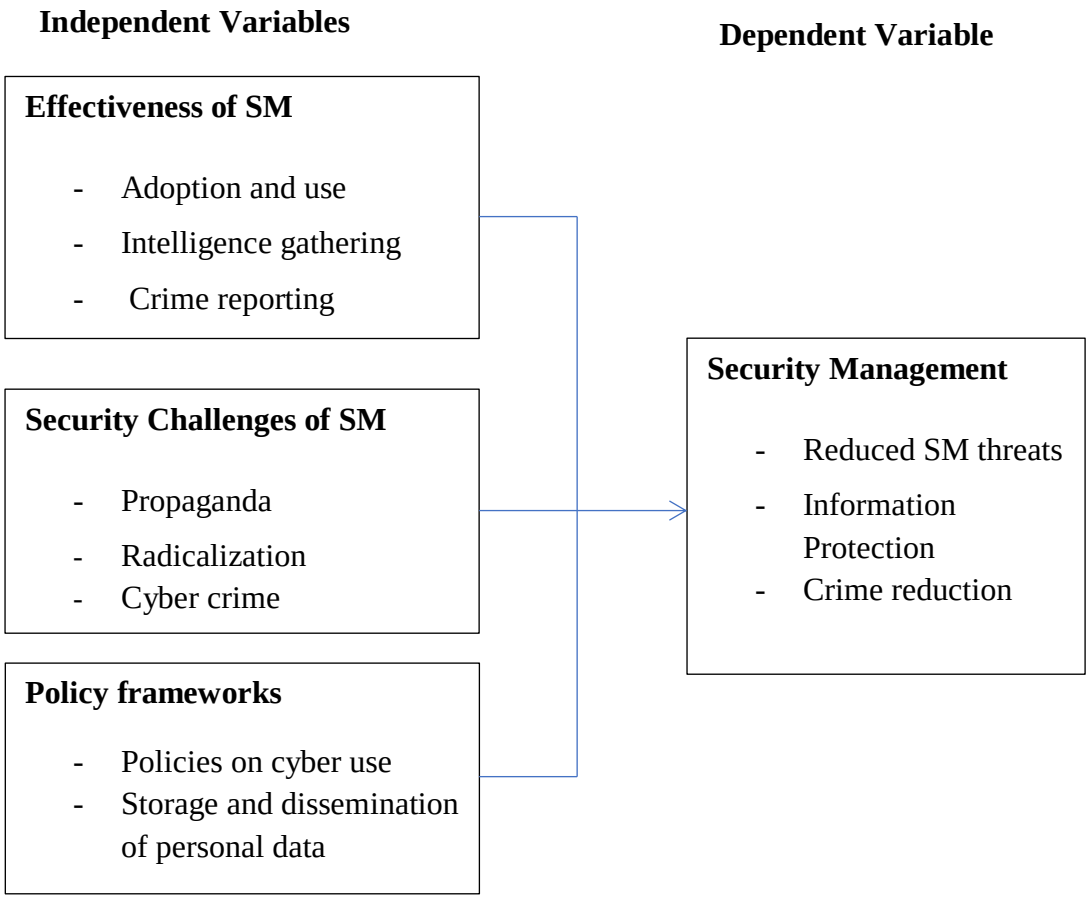
1.13 Conceptual Framework

The first independent variable in this study was the effectiveness of digital technologies by law enforcers. It entails the adoption and usage of social media tools like Facebook, YouTube, etc. and surveillance of digital platforms to enable detection for timely response. These social media tools have characteristics that enable sharing of information in form of videos, photos blogs which can be used in security response. Social media can be used to gather intelligence, report crime and clarify propaganda. The second variable is analysing social media challenges posed to national security. Identification of channels used and the targeted groups for example financial institutions, government institutions by criminal operatives is paramount in crime prevention. The form of threat posed may be different for example banks and financial institutions experience systems attack to siphon money while government institutions are targeted for siphoning of sensitive information. The last variable in this study will be legal frameworks that govern social media usage. Good laws governing the social media usage should be legislated to avoid criminals getting off the hook with a slap on the hand. The advancement of technologies pose a challenge to a police service that has been using 'brick and mortar' in fight against crime. The NPS should be well funded to help in acquisition of modern digital technologies that there will be timely detection and prevention of cyber-crime. This will be enabled by formulation of substantial policies and laws regarding use and dissemination of digital content, training police officers to deal with electronic crimes and the dynamics of social media and acquiring recent tools, while providing training in all levels of

forensic modus operandi and in using advanced digital technologies. The said measures will influence the security management on digital front hence early detection of crimes, reduced electronic crime rates and have a positive impact on the ability of officers to respond appropriately

Figure 1.1: conceptual Framework

Conceptual framework demonstrating independent and dependent variables used in this study



Source: Researcher 2021

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter focused on the scholarly works done by others on the influence of social media in security matters. The chapter presented a theoretical and empirical review on the variables of this study.

2.2 Effectiveness of Social Media on Security Management

According to Moon (2010), national security is often threatened by disasters that demand security organs such as police, military and disaster units to act quickly in order to save lives. Moon observed that, in catastrophic occurrences like the earthquake in Haiti, Japan tsunami, the Katrina hurricane and Californian wildfires, members of the society and general public were kept engaged and active by peer of the realm communicating, using cell phones, SM, blogs, wikis and web fora, and SMS applications. The same communication methods were used during the Britain riots, Arab uprising and Norwegian island massacre and many others.

Hodge (2010) observed that, social media and mobile technologies have greatly enabled engagement of citizens in information dissemination. In case of disasters or crime, the citizens are enabled to give first-hand information as eye witnesses; the information shared is often critical and accurate. Alert messages have been sent through social media platforms aiding in timely evacuation and rescue operations. According to Gad (2017), search missions, publication of related information, collection of donations in form of goods and services and asking for volunteers have been enabled through social media platforms. Social media technologies have connected more people establishing mechanism to collaborate; created informal networks and communities without boundaries not forgetting their primary purpose of being communication tools. Emphasising strongly on instant information dissemination, mobile and online tools have considerably enhanced the public and the victims' ability to get help from different sources and disaster response units. The messages they send mostly enables

enriched situational cognizance among the Public Protection and Disaster Relief (PPDR). The dissemination of assortment of information and data enables the public protection and disaster relief agencies make informed decisions on crisis management, (Trottier & Fuchs, 2014).

In 2013, Montrose Police department reported on its pages a case of missing teenager. Within hours there were over ten thousand responses posting the missing teenager elucidating the influence information shared on social media to multitudes (Woody, 2013). Social media, especially Facebook has been incorporated as an investigative tool, with photos of crime scene and criminals shared online which in turns help in the arrest, documenting evidence from scene and the witnesses (Gad 2017).

During English riots, the London police used social media with help of public to quell rioters who had turned to be looters and improve security. The use of CCTV cameras was used to capture photos of looters and rioters and the images shared on social media platform helping with arrest of perpetrators, (Ghonim, 2012). Thus, use of social media greatly assisted in quenching riots and apprehending looters.

In Kenya Nakuru County, chief Kariuki widely referred to as the "Africa twitting chief" of Lanet Umoja location in Nakuru North Sub-County. Mr. Kariuki used twitter for his administration work which made him to receive global accolades due to using twitter to manage security in his location. By using twitter, it helped to recover stolen domestic animals in his area and other properties, report crime timely, find missing child and public announcements.

As the country was being ravaged by Covid-19, the DCI and Child Protection Unit were pursuing "online criminal racket" that was luring school going children through social media by promising movie casting roles. According to Kimani (2020), when the report of missing girls came to light when parents complained about missing girls in Nairobi Komarock area. Parents took to social media pleading with members of public who may have privy information

about them to report while urging DCI to investigate. No sooner than the issue were published online, the teenagers were traced in their hide outs. The effectiveness of social media in investigations was evident by tracing the missing girls and it concurs with Gad (2017) who stated that; social media is a powerful tool for investigations.

For decades security management and technologies have been interconnected, since the dawn of the telecommunications, automobiles, and radio communication. Technological advancement propagated through mobile technologies, audio visual technologies, advanced analytics, highly powered computing among other technologies have advanced at an accelerated pace. Many security agencies are employing these technologies to enhance outcomes and increase efficiency, while being faced with shrinking income and ever-increasing inquiry of law enforcers' tactics and outcomes by the public (Kambuti, 2013).

Over the years, policing and security management have been moulded by technological advancements. In the advent of the twentieth century, development of mechanical methods in crime prevention and security management assisted in administration of security in that radio communications, vehicles, and computers supported dispatch frameworks. According to Mullen (1996), deoxyribonucleic corrosive testing innovations, video surveillance, tag pursuers, and incorporation of digital advancement have essentially impacted on security management and policing in the recent decades.

Smyth (2011) noted that, security organs are overwhelmed in keeping themselves abreast in adoption and use of new technologies. The steady growth of numerous technologies has barraged law enforcers with a consistent stream of creative technological tools, whose intention is to enhance the fight against crime. There are several types of digital technologies that have been used in security management such as drones, body cameras, cell phone tracking software, GIS among others.

GIS has been used as a computerized crime mapping software to aid in recovery of stolen vehicles, pin mapping crime hotspot over space and time. According to Chamard (2006) security agencies uses GIS in mapping, visualizing, and spatial analysis of crime patterns in geographical area for duration of time. It has also helped trace the paths of crime by exhibiting the spaces between happenings within an occurrence. Security actors through GIS can document clusters of crime cases by types for instance, crime hot spots and territories. In addition Markovic, Bueermann, & Smith (2016) GIS has enabled security organs to determine numbers of security officers deployed and allocated in certain areas or community as a result of graphic crime contents displayed and generated. Although some security agencies have been using crime mapping predominantly to produce graphic exhibitions of criminal activities in given area, others conduct intricate approaches of spatial scrutiny to comprehend the connection between crime categories or instances and select features both physically and in social situation. Techniques in spatial analysis can also diverge extensively depending on geographic policing strategy which an agency adopts whether proactive or reactive.

According to Reaves (2015) it was not until 2015 when Body Worn Cameras received amplified public attention due to prominent incidents involving police incidents, like those that happened in Ferguson, Missouri; North Charleston, South Carolina; New York City; and Cincinnati, Ohio. Latest estimates propose that about third of resident police divisions uses BWCs, even though these figures are predicted to increase significantly in the future (Reaves, 2015). However, it is imperative to note that there are assorted opinions from the ground about the possible effect of BWCs on relationship in the community (Hermann & Weiner, 2014).

Automatic License Plate Readers (ALPR) are high-speed cameras paired with character recognition software that can read and document thousands of license plates per minute while also recording the date, time, and location of every scan (Litten, 2015). ALPRs can be moveable for example being mounted on police cars or stationary for example fixed on physical

objects like an overpass. The information gotten is then compared with existing hot list of license plates compiled by agencies and pertinent matches used to direct signals to police officers on patrol. According to Reaves, (2015) LPR technology has recently courted controversy in recent times for the reason that license plate data collected by the ALPRs is retained by law enforcers and can even be merged into regional information sharing systems. Accordingly, the American Civil Liberties Union raised alarm connected to citizens' rights to privacy and the need for firm regulating LPR technology (Litten, 2015). In Kenya LPRs are mounted on all outlets of the capital and major highways.

The use and adoption of information and communications technology has brought new normal of how people interact, work, learn, and live. Over the time the law enforcement organs has continually upgraded their technologies and gears to match up new crime patterns that are super digital sophisticated. In a study conducted by Kambuti (2013) on the prevalence of technological use by Kenya police service in crime prevention, the study established that, KPS did not have latest technologies advancement in crime prevention. The study found out that, KPS hardly used digital technologies to enable strategic use of information to prevent crime. The mainly used communication equipment in crime prevention was personal mobile phones and walkie-talkies (Kambuti, 2013).

2.3 Challenges of Social Media on Security Management

Challenges orchestrated by use of social media use takes two forms; one the challenge on national security and the other is challenge on part of security organs ability to control offensive use of SM platforms.

There are many concerns on the social media usage in security management. Though SM enables free exchange of information, security organs cannot freely exchange the some information with public since their environment is controlled. The information shared by officers operating NPS social media platforms cannot bypass organizational control of

information exchange since police environment deals with information which is considered as highly sensitive.

Few attempts have been made in order to systematically address the social media usage by law enforcement officers even with its widespread usage. In USA, LexisNexis (2014) did a survey of law enforcement officials investigating the extent to which police personnel used social media for various policing activities. The study established that, 34% of the respondents stated to have used social media to alert the public of emergencies, crimes, and criminal suspects, while 29% used SM to solicit crime suspects tips from members the community. 30% of the study participants used social media to encourage positive relationships with the community, and about half of the sample monitored social media for criminal activity. The majority of social media sites that were frequently used were Facebook (93%), YouTube (67%), and Twitter (50%); (LexisNexis, 2014). The study covered effectiveness of social media in security management but did delve into challenges and policies governing its use in security management.

According to Walsh and O'Connor (2018), security officers face unprecedented attacks when their personal information is retrieved from social media sources and is shared online with aim of profiling and harassing them. The officers are confronted with dangers while on duty or off duty especially when they are a target of criminal gangs who keep surveillance by obtaining crucial information about them and their families from social media platforms.

Many governments across the globe institutions lacks technological sophistication capacity and are ill equipped to fight cybercrimes and other evils associated with social media. Xinxin (2018) observed that, though China had sophisticated cyber laws, cyber control abilities and dedicated social media police enforcement unit, the law enforcement resources were not

sufficient to keep up with the pace of growing numbers of social media users and amount of content that is being generated and distributed.

The NPS has endeavoured that police officers are equipped with skills on modern technologies. Recruits entering Kenya Police College accesses computer and they are instructed on the essentials of personal computer technology. KPS too have similarly procured Personal Computers for some police stations, armoured vehicles, and weaponry to extinguish and repel crime. In spite of all these accomplishments, the capability of controlling all digital related crimes has not yet been attained, (Kambuti, 2013). The Police Officers are continuously confronted by the advancing and increasingly sophisticated forms of emerging technologies. In this digital era, police stations keep occurrence books in hard copies whereas digital copies are cost effective and can be used at any place any time and very conveniently.

Policing has been interesting and exciting topic to research about. It is and has been public occupation that requires total commitment. According to Walters (2012), things has drastically changed since 2003 with invention of the social media platforms which has made security organs struggle to maintain their public image. Inception of smart phones made matters worse for security actors as anybody with the phone which has video recording capabilities can take photos and record videos to share whenever they chose to. He further adds that, shared contents which are viewed by billions of people globally, brings a lot of trouble to law enforcers. This is mainly because, content shared is not filtered to fit all audiences thus wrong information shared can caused irreversible damage (Walter, 2012).

Many countries have attempted to regulate use of social media due to the illicit contents being shared. In some extreme instances governments orders total ban on internet to deal with problematic contents being shared or to avoid mass mobilization especially during election cycle and public unrest triggered mostly by a tragic event. In Uganda in the recent concluded

elections 2021, the government ordered total shutdown on all social media platforms lasting five days arguing it was preventing mass mobilization and spread of fake news during election. However the critics and opposition argued that, the government ordered shutdown of social media to cover up election fraud and prevent sharing of evidence on the social media (Ragg & Wellington, 2021).

The trend of total internet blackout has been witnessed globally especially in countries whose regimes are dictatorial or when there are military coups. For example, a report released by West (2021) on the internet blockade globally, cited governments justifying it by alluding public unrest and destruction of nation's heritage by activists using social media to call for mass protests. In Myanmar, the military junta ordered internet shutdown arguing that, opponents were using social media to destabilise the country but mob resulted to using traditional methods of protesting like hitting pots.

In 2020, Ethiopian government ordered internet shutdown following public unrest over murder of a popular local singer from Ormo tribe (West, 2021). While government says they shutdown use of social media on security grounds, opponents always say it is censorship and abuse of democratic rights. According to Giles and Mwai (2021), in Africa there were 25 documented cases of limited or total internet shutdown in 2019 in comparison with 20 and 12 in 2018 and 2017 respectively.

Justice was sometimes delayed all denied as Kambuti (2013) established in her study on the prevalence of technological use by Kenya police service in crime prevention. She found that dispensation of justice sometimes was delayed because basic items such as occurrence books went missing because they were kept in hard copies. The same is true because when documents are kept in hard copies there is likelihood of pages being torn, illegible hand writing; the

document is also available in one place and can be used by one user at a time as opposed to when documents are kept in soft copies where they can be retrieved anywhere and easily.

In Kenya, Olaka (2017) conducted a study on the knowledge and practices on utilization of social media for Security Management in Kitui West Sub County. The study established that security personnel did not have enabling infrastructures to effectively use social media in security management. The study cited lack of internet and digital communication devices which fundamentally ought to be available in using social media on security management. The officers were at times forced to respond to false alarms since there were no sophisticated tools to help interpret the kind of response needed.

The national security actors are bombarded with numerous and emerging crime trends. Traditionally, use of guns and physical presence of police officers was regarded as having tight security. However, with emergent of digital technologies crime can be committed remotely leaving no foot prints to follow or finger prints to dust for forensic analysis. The study looks into some security challenges resulting from abuse of social media platforms.

Propaganda propagated through social media is a security challenge to national security and as Lasswell (1927) defines propaganda as the handling of collective attitudes by the manipulation of important symbols. From the period of French revolution to current events literature is in abundance of how public opinion has systematically been altered. Lately, prior to the Rwandan genocide in 1994 the infamous the Radio Libre des Mille Collines and the Balkan wars have been the most influential of these studies. Ethnic and political conflicts were found to be constructed by propaganda as it had ways to incite for violence (Hallin, 2004). The propaganda model was advocated by Hermon and Chomsky (2010). In this model the principal machineries of propaganda in the capitalist democracies is the media, which carry out the power relations of the existing state of affairs and undemocratic forces. Klaehn (2002) in critical review of

propaganda model, he observed intensification of propaganda due to the twenty four hours news cycle.

Makinen and Kuira (2018) observed that, during election period heightened political events arouse hatred among different tribal dialects. They further established that, those social media platform were used to channel prejudices based on tribes, biased and false information and hate speech. Social media platforms acted as a catalyst to both ethnic based conflicts and mass media communication tool for peace campaigns after elections. In addition to this, Portland communications (2018) alluded that, the 2017 general elections in Kenya were influenced by fake news, ethnic incitement messages all propagated and spread through social media platforms. This also concurs with SIMELAB (2018) report that, social media platforms are often fed will troll of fake news, propaganda, hate speech in order to interfere with online debates especially political to influence elections and damage the reputation of individuals.

The revolutionary power of social media was seen during the Middle East upheavals where it was used to rally protesters. The advantage the organizers had over security organs and the governments is that, they possessed superior communication methods i.e. social media platforms as opposed to security organs that relied on old-style means of communication. Ranko and Haase (2018) on their report on Jordan and the Jihadist threat they documented great magnitude of internet and social media plays in intercontinental relations with precise attention recruitments and fund mobilization. The study documented the usage and the role of social media networks for instance the Facebook, Twitter, YouTube and weblogs in aiding jihadist activities even across the borders with Syrian refugees being ripe target for recruitment. Their study established proliferation and social media usage in those Arab countries facilitated in mobilising mass protesters, opinion shaping to influence change, empowering and boosting morale of protesters. Since then, those Arab regions have are continually facing domestic conflicts giving birth to political instability. It can be observed that, such social unrest have

detrimental effect on social, political, cultural and economic dynamics of a nation. The actual cause of Arab spring revolution was not social media but it was the tool that was used, (Ghonim, 2012).

Weng (2010) noted that, the online platforms have been embraced by groups whose intention is to spread hate messages such as anti-Semites, homophobes, racists. This confirm earlier notion that social media have greatly helped illegal groups to reach out to masses. Long forgotten groups such as Nazis, KKK, skinhead, Identity church among many other have resurfaced and are now active thanks to social media platforms.

In Nigeria, security challenges according to Ani and Onyebukwa (2016) shoot from a plethora of national issues that are either ethnically tied, regard religion or socio-political and/ or culturally faceted. The Boko Haram Islamists, the militia from the oil-rich Niger Delta, the repeated clamour for secession in the south-eastern part of Nigeria are some of militia groups using social media to spread fear among the common citizens. The characteristics of social media platform being cheap, easily accessibility and ability to reach masses are some of the reasons why private and public organizations, individuals of all ages and across social divide use them not exempting terror network (Ngige, Badekale, & Hamman, 2016).

In Kenya illegal groups that have been criminalized such as mungiki, sungusungu, Al-Shabaab, cattle rustlers, and urban criminal networks are technologically savvy joining other global bigots (Kenya Police Service, 2014; Kimutai, 2014). Social media platforms have changed communications dynamics of 21st century and require security organs to be abreast not to be caught flat footed.

The rise in digital transactions has given rise to digital crimes. Das and Nayak (2013), defined cyber-crime as criminal activity that uses computer as tool or a target in criminal transactions. This happens through cyber-attack which is an intrusion of computerised systems and networks

by unauthorized person. Global computer networks have enabled communications and business transaction via online means, where goods and services are sourced and financial transactions done virtually. According to Communications Authority of Kenya (2020), there was detection of 13.9 million cyber-attack threats between April and June and 34.6 million for the period between January and March all in year 2020. The attacks were in form of malware, botnets, system vulnerabilities and web application attacks. Availability of internet provides access to information and services virtually breaking physical and distance barriers, makes it fertile ground for cyber criminals.

According to Morgan (2017), over six trillion dollars are been spent annually on cyber-crime globally by businesses. Cyber-crimes include, cyber-attacks commonly known as hacking, bullying, stalking and surveillance. In agreement with Collective Security Approach Theory, CAK (2019) stated that, there was no single institution that had the capacity to effectively handle cyber threats single handily. The commission called for collective approach between government and private entities to handle the challenge of cyber-crimes. In Uses and Gratification Theory, business use social media and other digital technologies to gratify their needs that is, market their products and other business transactions; in the same manner, criminals uses social media and digital technologies with evil motives.

The report released by Kenya digital security report 2014 indicated that Kenya losses an estimated 2 billion shillings per year through cyber-crime. The revelations emanating from the report gives a persuasive purpose for a study to be conducted on how security actors are formulating on with emerging innovations and technologies to restraint cyber-crime (Kenya cyber security report, 2014). In a report released by KMGP (2016), 93% of cyber-attack on small and medium enterprises had very severe impact on business and out of this cyber breach 60% of businesses closed down within six months after their reputation were damaged or their money in bank accounts stolen.

These call for NPS to acquire advanced digital forensic technologies to assist in investigation, arrest and prosecution of cyber attackers. The punishment should be severe to act as deterrent to others. According to Communications Authority (2020), there was detection of 13.9 million cyber-attack threats between April and June and 34.6 million for the period between January and March all in year 2020 in Kenya. The attacks were in form of malware, botnets, system vulnerabilities and web application attacks.

2.4 Policies that guide NPS in using Social Media on Security Management

Traditionally business organizations had many human resources policies detailing the code of conduct of staff engagements on behalf of the company. Currently, businesses are hurrying to have such policy on the use of social media in representing their entities. Hitt, (2015) observed that, organisations have embraced social media networks to help to accelerate spread of information through the use of platform such as Facebook, Instagram, WhatsApp, Twitter and LinkedIn. Information shared may include private and personal information which may jeopardize individual security and damage company reputation. Therefore, there should be rules and policies governing the use of social media as public communication tool

Technology use in security management has never been void of controversy. The government of the People's Republic of China in 2009 added to its criminal law crimes committed by use of computer. In the computer law, the government tightened the process of registering domain names and banned individuals from getting domains unless they are registered and licensed business (Kshetri, 2015). The offenders on the other hand are to serve custodial sentence of up to seven years in prison for cybercrime. In 2011, the computer law was amended requiring internet users to register using their real names targeting bloggers and social media content developers (Kshetri, 2017). Despite china having sophisticated cyber laws, cyber control ability and dedicated social media police enforcement unit, the law enforcing agents resources are not sufficient to keep up with the pace of growing numbers of social media users (Xinxin, 2018).

In the African region, Lesotho enacted legislation requiring social media users with more than one hundred followers to register with the local communications authority as internet broadcasters. Critics argued that this will interfere with freedom of expression and association. Their neighbouring country Botswana had in 2012 banned military officer from using Facebook, Twitter and other social media platforms citing security reasons with military bosses stressing out that the directive was meant to safeguard them and prevent leakage of classified information. On the hand, soldiers complained that they used social media to connect with friends and family and banning them from accessing these platforms made them feel isolated (Bowmans, 2014).

In Tanzania, the government enacted Electronic and Postal Communication (Online Content) Regulation 2020, banning the use of social media in publishing information that can be deemed to ridicule, harm or damage the prestige and reputation of the republic or defame other individuals, United Republic of Tanzania (2020). Critics argued that, the new regulations are a threat to freedom of speech and expression and that they are in clear violation to international standards.

In Kenya, research study conducted by (Munyua, 2011) established that, there were no specific legal provisions for crimes such as identity theft, cyber stalking, chat room abuse and impersonation in Kenya. Two years down the line, Kenya communications (Amendments) Act 2013 failed to address cyber-crimes committed against the person. However, later on Kenya was not been left out in regulating the use of computer and internet. In 2018 the government enacted the Computer Misuse and Cybercrimes Act (Computer Misuse and Cybercrimes Act No 5 2018, sections 22-23) which make it criminal to publish false reports and communicating in a manner deemed offensive by the recipient. This was in response to social media platforms becoming often used as means of spreading false broadcast and hate speech.

A research study conducted by United States International University Africa based in Nairobi Kenya coded SIMELAB (2018), highlighted that in 2016 alone at least sixty political bloggers were detained and indicted for publishing false information that was likely to cause public alarm. Though charges were dropped or court set them free due to lack of proper legislation in spite of provisions of section 9, with enactment of Computer Misuse and Cybercrimes Act 2018. By the time of writing this report there were no convictions of offender under the new Act in Kenya.

Social media raises concerns on security management due to integrity of information generated and shared online. Personal or organization data and confidential information is jeopardizing when information is leaked maliciously or accidentally and phishing by attackers through malwares. Therefore, there should be adequate legislation and tough laws to deter such actions.

The National Police Service was created through provisions of the 2010 Kenyan Constitution, the National Police Service Act 2011 and the National Police Service Commission Act 2011. In accordance with the provisions, the National Police Service consists of The Kenya Police Service, The Administrative Police Service and The Directorate Criminal Investigation. The Acts provide for powers, functions, procedures and jurisdiction guiding NPS in their responsibilities.

NPS is commanded independently by the Inspector General (IG), while each arm is headed by Deputy Inspector General (DIG). Since social media platform are used for mass communication, the NPS has embraced their use by opening Facebook and twitter official pages. In additional to social media platforms and official website, the NPS has expanded its communication network by improving broadband of hotline numbers which are 999, 112 and 911 which public can call at any time to report crime or seek help. National police service and other security organs are not just ordinary organizations; it is the body that is tasked with

maintain law and order, safety of citizens and their properties. In this era of digital age, big data and artificial intelligence where messages are conveyed at speed through social media platforms security managers should be extra vigilant on what is posted, shared or commented on their social media platforms.

In Kenya, Data Protection Act 2018 legislation was enacted by parliament to establish the Office of the Data Protection Commissioner to regulate the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes. The legislation elaborates measures in ensuring public data, personal information with regard to storage, retrieval and dissemination is well secured.

On Dec of 2018, a court of law ordered the Inspector General (IG) and Director of Criminal Investigation (DCI) to stop publishing photos of suspects on their social media platform mostly twitter and Facebook, (Daily Nation, Dec 10, 2018). The court argued that, sharing of photos of suspects may cause mistrial. However, DCI responded by quoting the NPS Act of 2011 that gave Power to take photographs, fingerprints and forensic evidence. CAP 84 subsection 55 *(1)*

> A magistrate or a police officer, and any other person appointed to give certificates under subsection (2) of section 142 of the Criminal Procedure Code (Cap. 75), may take, or cause to be taken in his presence, for the purposes of record and identification, the measurements, photographs, footprints and casts thereof, palm-prints, finger-prints and other forensic evidence of any person in lawful custody or who is subject to police supervision.

Communication Authority of Kenya and NPS are the only constitutional organs empowered to enforce and implement the legislations enacted to govern use of social media and other channels used in communications.

2.5 Summary of Literature Review and Research gaps

The literature reviewed presented variety of scholarly works on how social media has been used globally, regionally and locally shaping how content is created and disseminated. The literature established that, in USA social media has been used to alert the public of emergencies, crimes, and criminal suspects, and solicit crime suspects tip from members the community. It also found that social media was used to encourage positive relationships with the community, and monitoring for criminal activity (LexisNexis, 2014). The study also observed that, though there were many challenges, social media was used to clarify information, gather intelligence and report crime (Kimutai, 2014). The literature review has covered other nations' policies and laws regarding using social media and found that, although China has sophisticated cyber laws and social media police but is overwhelmed by multitude of content generated (Xinxin, 2018).

The research studies cited in the literature review have tried to bring out the effects of social media on security matters. However, they did not indicate the influence of social media on security management with specific reference to NPS. This therefore created a knowledge gap on the link between these variables with a specific reference to NPS. Kimutai (2014) study on social media and national security threats focused on military unit in Nairobi thus cannot be used in NPS setting due to their differences in operations. His study used social responsibility theory only which due to its relevancy has been also been used in this study. However, application of the theory is different and this study added collective security approach theory to complement SRT. Nsudu, I. and Onwe, E.C. (2017) did a study in Nigeria on Social media and security challenges in Nigeria: The way forward. Their study found that, Social media was the tool used for planning, spreading propaganda, mobilizing and fundraising but it did not address the challenges faced by security actors hence the need to look at challenges faced by security players in respect to social media. Kshetri, N. (2017) did a research study on Cyber-victimization and cyber security in China. The results found that, though China had

sophisticated cyber laws and social media police it was still overwhelmed by multitude of content generated and disseminated. However, this study focused on China only, creating the need to look at regions.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This section discussed the research the methodology used in this study. The features included are the research design, target population, sample size and sampling procedure, validity of research instruments, reliability of the research findings, and data collection procedures, data analysis techniques.

3.2 Research Design

Cooper and Schindler (2011), defined research design as a meticulous plan to guide a research study to obtain answers to the research questions conceived in its objectives. The study employed descriptive research design which is a popular and common methodology in business, social sciences and management research and is most frequently used to answer who, what, where, how much and how many questions, (Saunders, Lewis & Thornhill, 2009). The descriptive survey method is perceived as authoritative by people in general and is both comparatively easy to explain and to understand a phenomenon.

3.3 Research site

The research study site was Kilimani police division and Dagoretti police division. Kilimani police division serve residents of Kilimani, Kileleshwa, Upper hill and some parts of Kibera. On the other hand, Dagoretti police division serve parts of Karen, Satellite, Waithaka, Mutuini and Kawangware. The rationale for the research site was because it covered high class estate (kilimani, Kileleshwa), low class estate (Kibera) and rural area setting (Mutuini & Waithaka) thus creating cosmopolitan population.

3.4 Target population

This study defines the term population as a complete set of individuals. Accessibility of the target population is a must for the purposes of conclusive research. According to Kothari (2004)

30% of the reachable population is enough for descriptive studies. The target population of this study were NPS personnel based across police stations within Kilimani and Dagoretti police Divisions. The respondents were officer commanding police station, their deputies and officers under their command in the police stations within these two police divisions. The researcher interviewed two senior police officers in the same divisions.

Table 3.1 Target population

Police Division	**Police station**	**Population**	**Percentage**
Kilimani	Jamhuri	38	6.08
	Kibera	42	6.42
	Capitol Hill	97	15.52
	Kilimani	200	32
Dagoretti	Riruta	48	7.68
	Waithaka	52	8.32
	Mutuini	30	4.8
	Dagoretti	118	18.88
Total		**625**	**100**

Source: Each police station information desk

3.5 Sample and Sampling Technique

Ingule and Gatumu, (2011) defined sample as a frame of smaller number of cases drawn from the total population. Robson (2012) highlighted the importance of sampling as that; it saves on expenses and time that could have been used in studying the entire population. The researcher used proportionate sampling for **s**ample size on the population of police officers in police stations within Kilimani and Dagoretti police Divisions.

The researcher adopted a systematic random sampling to pick police stations in the police divisions and the same method to pick study respondents. Nassiuma (2000) formula was used to calculate sample size. $n = \frac{N}{1+N(e)^2}$

Where:

n= sample size

N = Population

C = confidence level of 95%

e= error margin of 0.05%

Therefore sample size was 244

Table 3.2 Sample Size

Station	Population	Sample ratio	Sample
Kilimani	**200**	$\frac{n}{625} * 244$	**78**
Capitol Hill	**97**		**38**
Jamhuri	**38**		**15**
Kibera	**42**		**16**
Riruta	**48**		**19**
Dagoretti	**118**		**46**
Waithaka	**52**		**20**
Mutuini	**30**		**12**
Total	**625**		**244**

Source: Researcher 2021

3.6 Instrument

Open-ended and close-ended questionnaires were used to collect primary data and important information from the population. The researcher interviewed two senior police officers in the

same police divisions. Secondary data was collected from books, journals, and literature review by other scholars. According to Mugenda and Mugenda (2012), a self-administered questionnaire is the only way to elicit self-report on people's opinion, attitudes, beliefs and values.

3.7 Piloting Study

According to Isaac (2012), a sample size of not less than 8% of the population is adequate for pilot study and the study itself. The researcher developed the questionnaire as per study objectives. The researcher then administered 20 questionnaires to officers at Nairobi Central Police station to test the reliability and validity of the questionnaire; this was informed by the fact that, the respondents are the same and likelihood to get the same response due to similarity in the nature of their work. It aided in fine tuning the questionnaire by ensuring data collected will be free from ambiguity and errors and that, the data was to be relied for the purposes of this research. The sample was picked randomly and covered all ranks.

3.7.1 Validity of the Research Instruments

The degree by which the sample of tested items denotes the content the test is designed to measure is what is referred to as validity. Content validity which was employed in this study was a measure of the degree to which data collected using a particular instrument represented a specific domain or content of a particular concept. According to Mugenda and Mugenda (2012) the best procedure in assessing the content validity of a measure is to use a professional or expert in a particular field to comment on the suitability of questions and the structure of the questionnaire. The researcher sought professional advice from ANU supervisors and independent security consultants. This helped to improve the content validity of the data that will be collected.

3.7.2 Reliability of the Research Findings

Reliability refers to the consistency of measurement and is assessed using the test retest reliability method of research instruments. Reliability is increased by including many similar items on a measure, by testing a diverse sample of individuals and by using uniform testing procedures. The researcher computed a Cronbach alpha score of the instrument used to obtain the primary data. Cronbach alpha ranges between 0-1. Scores between 0-0.6 indicate that the instrument has a low reliability while scores of 0.7 and above indicate that the instrument has a high level of internal consistency and reliability (Cooper & Schindler, 2013).

3.8 Data Collection Procedure

The researcher obtained a letter from NACOSTI authorising the study and thereafter sought Kilimani and Dagoretti OCPD's permission to conduct the study in their respective police division. The researcher then distributed the questionnaires using drop and pick method in order to give study respondents ample time to fill in the questionnaires in their free time. Questionnaires are the most favoured on the ground according to Mugenda & Mugenda (2012) because they are easy to administer and they are time saving. The researcher gave out a total of two hundred and forty four questionnaires to selected respondents. In addition, the researcher also interviewed two senior police officers one from each police division of the study area. The research dropped and left questionnaires with police officers at respective police stations and picked them later at agreed date not exceeding two weeks. E-books and e-journals together with print were used to retrieve secondary information

3.9 Data Analysis and Presentation

McDaniel and Gates (2004) described the objective of data analysis as to translate and make inferences huge amount of collected data. The collected data was both qualitative and quantitative. Data cleaning was done on filled questionnaires before processing them to ensure completeness and consistence. Descriptive statistical tool (SPSS version 21) was used to aid

in interpretation and drawing conclusion. Data analysis was done using descriptive statistics that is percentages, mean and standard deviation which presented using tables, bar charts to give a clear picture of the research findings. Qualitative data from open-ended questions and interview was analysed thematically according to research objectives and their views and opinions represented findings and discussions.

3.10 Ethical Considerations

Ethics is defined as norms for conduct that distinguishes between acceptable and unacceptable behaviour (Sproul, 2015). Ethics is what is good for an individual, the society and also moral values**.**

After receiving green light from the University and NACOSTI, the researcher sought each individual consent from study respondents and disclosed the purpose of study as purely academic and that their responses was to be treated with utter confidentiality and their identity was not be disclosed that is, their privacy will be respected and that, the responses provided will not be used against them whatsoever. Respondents were not required to indicate their names thus upholding anonymity. The research was voluntary therefore; questionnaires were distributed to respondents who were willing to participate. Filled in questionnaires were burned immediately when the data was coded in computer which had password therefore denying unauthorised access. The research stuck to study objectives to avoid biasness or diverting. Intellectual property rights were respected by acknowledging and giving credit to cited sources.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

In this chapter, the researcher addresses analysis of the primary data collected from the questionnaire. The analysis will consist of the research objectives and demographical data of the respondents.

4.2 Response Rate

A total of 244 questionnaires were distributed to the police officers in Kilimani and Dagoretti police division. However, the response rate was not 100% because 56 questionnaires were not fit for data analysis; 50 questionnaires were blank while 6 were ineligible or half-filled therefore could not be incorporated in analyzing the data. Nevertheless, the overwhelming willingness of the respondents to participate ensured high response rate. The response is represented in the table 4.3

Table 4.1 Response Rate

	Frequency	Percentages
Returned	188	77.02
Not returned	56	22.09
Total	244	100

As indicated in the Table 4.1 above, duly filled and received questionnaires for analysis were for 82.1%. Mugenda and Mugenda (2012) indicated that, a response rate of 50% is considered adequate , 60% is good and 70% and above is excellent for a study. In this study the response rate of 77.02 % was reliable and that the analysis could be done.

4.3 Demographic Information of the Respondents

The respondents demographic information was gender, number of years served in NPS, Police division and social media platforms for personal use.

4.3.1 Gender

The gender of the respondents is as shown in the table 4.4 below

Table 3.2 Gender

Gender	Frequency	Percentage
Male	123	65.43
Female	65	34.57
Total	188	100

Table 4.2 shows that 65.43% of the respondents were male while 34.57% were female. The gender distribution was fair for the study to give different viewpoints and perceptions.

4.3.2 Police Division

The research sought to find out the police division of the respondents and the findings are indicated in the table below

Table 4.3 Police Division

Police Division		Frequency	Percentage
	Kilimani	114	60.64
	Dagoretti	74	39.36
	Total	188	100.0

Kilimani police division had the highest rate of respondents 114 (60.64%) while Dagoretti Police division had 74 (39.36%). This is attributed to the fact that, former has high number of police officers than later.

4.3.3 Numbers of years in service

The study wanted to find out the number of years respondents had been in police service. Response is tabulated below

Table 4.4 Years served NPS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1	13	6.9	6.9	6.9
	1-5	26	13.8	13.8	20.7
	6-10	40	21.3	21.3	42.0
	11-15	43	22.9	22.9	64.9
	16-20	37	19.7	19.7	84.6
	more than 21	29	15.4	15.4	100.0
	Total	188	100.0	100.0	

Table 4.4 shows that 43 (22.9%) of the respondents had been in the police service between 11-15 years followed closely by those in service between 6-10 years 40 (21.3%). Those in service between 16-20 Years accounted for 19.7% (37) and 1-5 years were 26 (13.8%). Police officers who had served NPS less than a year were 13 (6.9%). Police officers who had been in service for more than 21 years were 29 (15.4%). The number of years was needful since the police officers had sufficient experience and information provided could be relied upon in the study.

4.3.4 Social media Platform for personal use

The table 4.5 below shows the social media platforms that were used by the respondents for their personal interactions.

Table 4.5 Social Media tools do you use for personal interactions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Facebook	93	49.5	49.5	49.5
	Tiktok	15	8.0	8.0	57.4
	Twitter	52	27.7	27.7	85.1
	LinkedIn	10	5.3	5.3	90.4
	YouTube	18	9.6	9.6	100.0
	Total	188	100.0	100.0	

Table 4.5 shows that, the majority of the respondents 93 (49.5%) had subscribed to Facebook, followed closely by those who had twitter account 52 (27.7%). YouTube had 18 (9.6%), Tiktok 15 (8.0%) and LinkedIn 10 (5.3%). The researcher sought to find out whether the respondents used social media for personal interactions because by being conversant with SM they could give credible information for the study. Social media facilitates formation of new friendship and hook up, societies, individuals and corporate connections while existing ones are maintained. The formation of social networking help in information flow and security alerts can be shared. It was worthy to note that significant number of the respondents added WhatsApp as a social media tool commonly used for personal engagements.

4.4 Presentation of Research Analysis and Findings

4.4.1 Effectiveness of using Social Media in Security Management

The researcher sought to analyse NPS effectiveness in using social media for Security Management in Kilimani and Dagoretti police Divisions. To find out SM effectiveness, the study further sought to find out the adoption and use of SM, whether social media was used for intelligence gathering and crime reporting.

4.4.1.1 National Police Service on Social Media

The respondents were asked whether NPS used social media on security management. The response is as shown in the table 4.6 below

Table 4.6 Social Media on Security Management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	188	100.0	100.0	100.0

The response as shown in the table above was a resounding positive in that all the respondents affirmed that NPS used social media as a communication tool.

4.4.1.2 Social media platforms used by NPS

The study further sought to find out the social media platforms used for communications by the NPS.

Table 4.7 Social media platforms used by NPS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Facebook	95	50.5	50.5	50.5
	Twitter	80	42.6	42.6	93.1
	YouTube	13	6.9	6.9	100.0
	Total	188	100.0	100.0	

Table 4.7 clearly indicated that, NPS had Facebook, twitter account and YouTube for social media communications with response rate of 95 (50.5%); 80 (42.6%) and 13 (6.9%) respectively.

4.4.1.3 Social Media for work related purpose at NPS

In handling and running the social media platforms, the study asked the respondents to indicated who was allowed to use Social Media for work related purpose at NPS

Table 4.8 Who is allowed to use Social Media for work related purpose at NPS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Senior officers	57	30.3	30.3	30.3
	Designated by the IG	131	69.7	89.7	100.0
	Total	188	100.0	100.0	

Results from the table above indicated that, there are delegated police officers designated by the IG to run NPS social media platforms, 131 (69.7%) affirmed it while senior police officers had 57 (30.3%). The statement had a mean of 2.69 and std. dev. of 0.461.

One respondent indicated that, even when senior police officers posted anything on their personal social media platforms it could be perceived to be official communication by the members of the public.

4.4.1.4 Police unit responsible for monitoring use of Social Media

The study sought to find out whether there was a dedicated integrated police unit responsible for monitoring use of Social Media. The response is as shown in table 4.9

Table 4.9 integrated police unit for monitoring Social Media

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	70	37.2	37.2	37.2
	No	93	49.5	49.5	86.7
	Don't Know	25	13.3	13.3	100.0
	Total	188	100.0	100.0	

The questions generated mixed views with majority 93 (49.5%) of the respondents saying there wasn't a dedicated integrated police unit responsible for monitoring use of Social Media. Those who indicated there was a dedicated integrated police unit responsible for monitoring use of Social Media were 70 (37.2%) while 25 (16.3%) didn't know altogether. The statement mean was 1.67 and the std. dev. of 0.671.

Respondents interviewed were of the view that, DCI and National Intelligence Service had the capacity to monitor the use of social media but if they do so are not in public domain due to legal and constitutional barriers. However, there were criminal elements whose social media platform can be flagged for security reasons.

4.4.1.5 Effectiveness of Social Media in various constituents

The research sought to examine the effectiveness of social media platforms in Creating Public Awareness, Intelligence gathering, Crime Prevention, Counter Propaganda, Administration and Apprehending criminals. The results are as shown in table 4.10 below

Table 4.10 effectiveness of Social Media

Statement	Very Great Extent	Great Extent	Moderate	Low Extent	Not at all	Mean	Std. Dev.
Creating Public Awareness	94 (50.0)	86 (45.7)	8 (4.3)	0	0	1.54	.579
Intelligence gathering	41 (21.8)	143 (76.1)	4 (2.1)	0	0	1.80	.449
Crime Prevention	53 (28.2)	68 (36.7)	0	52 (27.7)	15 (8.0)	3.15	.926
Counter Propaganda	65 (34.6)	123 (65.4)	0	0	0	1.65	.476
Administration	0	0	34 (18.1)	50 (26.6)	104 (55.3)	4.37	.773
Apprehending criminals	69 (36.7)	101 (53.7)	11 (5.9)	7 (3.7)	0	1.76	.722

The result from the table above shows that, the respondents were of the view that NPS social media platforms were used to create public awareness. The SM was effective in creating public awareness to very great extent 94 (50%) followed closely by great extent 86 (45.7%) while those of the opinion that SM created public awareness moderately were 8 (4.3%). The statement had a mean of 1.54 and std. dev. (.579). This implies that NPS social media platforms were very effective in creating public awareness or issuing alerts and official police

communication to the members of the public. According Trottier and Fuchs (2014), dissemination of assortment of information and data enables the public protection whereby members of the public make informed decision especially in times of disaster and on crisis management.

On intelligence gathering, majority of the respondents were of the view that, NPS social media platforms were effective to great extent in gathering intelligence 143 (76.1%) and 41 (21.8%) were of the same opinion to the very great extent while 4 (2.1%) regarded it as moderate. The statement had a mean of 1.80 and std. dev. (.449). These findings are in agreement with Gad (2017) who found that, social media, especially Facebook had been incorporated as an investigative tool, with photos of crime scene and criminals shared online which in turns help in the arrest, documenting evidence from scene and the witnesses.

The statement on the effectiveness of SM in preventing crime and criminal activities drew mixed reactions as it had a mean of 3.15 and std. dev. (.926). Majority of the respondents were of the view that, the effectiveness of SM in preventing crime was to great extent 68 (36.2%) followed by the opinion it was effective to very great extent 53 (28.2%). Nevertheless, 52 (27.7%) were of the view that, NPS social media platforms were effective to low extent in crime prevention while 15 (8.0) held the opinion it was not effective at all as far as crime prevention was concerned. The mixed responses can be attributed to as some respondents said; mostly police react from public SM posts especially when gone viral. In the emergent of digital technologies, crime can be committed remotely leaving no foot prints to follow or finger prints to dust for forensic analysis. Nevertheless, with continue investment in sophisticated digital tools, security organs are sealing this gap and intercepting crime before it occurs. This finding concurs with Kambuti (2013) on the prevalence of technological use by Kenya police service

in crime prevention that, they hardly used digital technologies to enable strategic use of information to prevent crime. One respondent said

> The service is not adequately funded to enable in acquisition of gadgets, software and regular training on emerging criminal trends that will be necessary in crime prevention.

On the effectiveness of SM in countering propaganda, majority of the respondents were of the view that, NPS social media platforms were effective to great extent 123 (65.4%) and very great extent 65 (34.6. The statement mean was 1.65 and std. dev. (.476). The response implies that, SM was effective in countering propaganda and rumour mongering. Official communication gave clarity and corrected misinformation. This is in line with Kimutai (2014) who found that, official SM accounts were very useful for countering propaganda by providing relevant information therefore stopping spread of fake news.

The respondents were further asked whether NPS social media account were used for administration and to which extent. Majority of the respondents were of the contrary opinion that SM was not used at all in administration, 104 (55.3%) while 50 (26.6%) responded it was used but to low extent. However, 34 (18.1%) of the respondents said it was used moderately given example whereby all officers on leave are ordered back to work in crisis times like electioneering period. The statement had a mean of 4.37 and std. dev. (.773). This agrees with one respondent reply

> You cannot administer through social media

However, general information regarding officers like calling those on leave back to work is issued through mass media of which SM is one of the communication channels.

The effectiveness of SM in apprehending criminals to very great extent 69 (36.7%) and to the majority, effectiveness was to great extent 101 (53.7%). Further 11 (5.9%) and 7 (3.7%) of the respondents viewed the effectiveness of SM in apprehending criminal moderately and to low extent respectively. The mean of the statement was 1.76 and std. dev. (.722). An example of the effectiveness of SM in apprehending law offenders was given of the lady who was accosted and harassed by motorcycle riders commonly known as bodaboda on Prof. Wangari Mathai road. Many examples were shared especially where photos are shared online by NPS and the members of the public help in alerting law agents on the criminal elements and their hideouts.

4.4.2 Challenges in Use of Social Media on Security Management

4.4.2.1 Challenges in Use of Social Media

The respondents were requested to evaluate the following statements on challenges of Social Media on Security Management and either agree or disagree with them. The statement were formulated in Likert scale whereby 1=Strong Disagree 2= Disagree 3=Neutral 4= Agree 5= Strongly Agree

Table 4.11 Challenges in Use of SM

Statement	Strong Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Std. Dev
Are police officers adequately trained on use of Social Media	94 (50.0)	84 (44.7)	10 (5.3)	0	0	1.55	.596
Is there infrastructure to facilitate use of SM on Security Management e.g. internet, computers	50 (26.6)	109 (58.0)	14 (7.4)	15 (8.0)	0	1.96	.813
There are tools to filter and monitor social media use in Kenya	0	120 (63.8)	44 (23.4)	24 (12.8)	0	2.48	.712
There is laid down mechanism to aid police officers in tackling social media offenses	0	95 (50.5)	47 (25.0)	46 (24.5)	0	2.73	.828

The research sought to find out the challenges faced by police officers in the use of social media. The respondents were asked whether the police officers were adequately trained on the use of Social Media; majority strongly disagreed 94 (50%) followed closely with those who disagreed 84 (44.7%) while 10 (5.3 %) of the respondents were neutral. The statement had a mean of 1.55 and std. dev. (.596). Arnoff (2007) stated that, where training was absent, incompetence, inefficiencies and ineffectiveness abound. He further noted that, training improved technical competences and that training was found to be invaluable to staff in various governments.

On whether there was infrastructure to facilitate use of SM on Security Management for example internet, computers and open source intelligence software; 50 (26.6%) of the respondents strongly disagreed, 109 (58%) disagreed while 14 (7.4%) were neutral. However, 15 (8.0%) agreed that NPS had had infrastructure to facilitated the use of SM in security management. The mean was 1.96 and std. dev. (.813). This agrees with Ndonye (2019) on the implications of technological advancement on policing noted that, though there was use of digital technologies they were not advanced and neither superior to detect and prevent crime. In addition, the findings also concur with Olaka (2017) who cited lack of internet and digital communication devices which fundamentally ought to be available in using social media on security management.

The respondents were asked to state if there were tools to filter and monitor social media. Majority of the respondents disagreed 120 (63.8%), 44 (23.4%) were neutral while 24 (12.8%) agreed. The statement mean was 2.48 and std. dev. (.712). This implies that, NPS did not have technological sophistication capacity to respond to all offenses associated with social media. In agreement to the findings, Xinxin (2018) observed that, even though sophisticated cyber control abilities and dedicated social media police enforcement unit are put in place, the law

enforcement resources are not sufficient to keep up with the pace of growing numbers of social media users and amount of content that is being generated and distributed. In additional Walter (2012) further noted that, shared contents are viewed by billions of people globally, bringing a lot of trouble to law enforcers because content shared is not filtered to fit all audiences thus wrong information shared can caused irreversible damage.

On the statement whether NPS had laid down mechanism to aid police officers in tackling social media offenses 95 (50.5%) of the respondents disagreed followed closely with those who agreed 47 (25.0%) while 46 (24.5%) were neutral. The statement had a mean of 2.73 and std. dev. (.828). The margin with between the respondents who agreed and disagreed necessitated the researcher to redirect the question to senior police officer, who was of the views that, police officers are trained to handle all crimes, old and those to come. The mechanism in place to tackle crime using traditional methods is still effective to handle digital crimes because what changes is the arena.

4.4.2.2 Challenges orchestrated through use of social media

With emergent of digital technologies security actors are bombarded with numerous and emerging crime trends. Therefore, the researcher sought to find out challenges orchestrated through use of social media as reported to security organs.

Table 4.12 Challenges orchestrated by SM

Statement	Very Great Extent	Great Extent	Moderate	Low Extent	Not at all	Mean	Std. Dev.
Cyber crime	0	132 (70.2)	34 (18.1)	22 (11.7)	0	2.41	.692
Radicalization	16 (8.5)	143 (76.1)	29 (15.4)	0	0	2.07	.485
Hate speech/ propaganda	77 (41.0)	107 (56.9)	4 (2.1)	0	0	1.61	.530
Fundraising for criminal activities	0	83 (44.1)	69 (36.7)	36 (19.1)	0	2.70	.757

On the some of the security challenges resulting from abuse of social media platforms, the results are as follows. On Cybercrime majority of the respondents 132 (70.2%) indicated it was to great extent, 34 (18.1%) indicated it was moderate while 22 (11.7%) indicated it was to low extent. The statement mean was 2.41 and std. dev. (.692). The finding denotes that, cybercrime is a challenge that police officers dealt with regularly. One of the respondents narrated how a lady was duped through Facebook into buying ghost furniture. The offender had posted photos online looking for prospective buyers but after receiving down payments he did not deliver. The officers on the case found that, the photos posted belonged to some legitimate business whose owner didn't have any relation with the offender.

On extent to which SM was used in radicalization 16 (8.5%) indicated it was to very great extent, 143 (76.1%) who were majority indicated it was used to great extent while 29 (15.4%)

indicated it was moderately used. The mean of the statement was 2.07 and std. dev. (.485). The study findings agree with Ghonim (2012) who found SM has been used as a tool for recruitment, fundraising and mobilization of criminal groups, opinion shaping to influence change, empowering and boosting morale of the targeted groups.

Majority of the respondents 107 (56.9%) indicated hate speech and propaganda were to great extent orchestrated through SM and 77 (41%) indicated it was to very great extent while 4 (2.1%) were moderate. The statement mean was 1.61 and std. dev. (.530). The findings concur with SIMELAB (2018) report that, social media platforms are often fed will troll of fake news, propaganda, hate speech in order to interfere with online debates especially political to influence elections and damage the reputation of individuals. Online platforms have been embraced by groups whose intention is to spread hate messages. Nsudu and Onwe, (2017) also noted that, the adverse side of social media applications tools is that, they have also been the channel to promote and spread rumours, propaganda and fake news.

On the statement whether the respondents were of the view that SM was used in fundraising for criminal activities, 83 (44.1%) indicated it was to great extent while 69 (36.7%) of the respondents indicated it was used moderately. The statement mean was 2.70 and std. dev. (.757). The findings vary in level of extent with Ranko and Haase (2018) who found very great magnitude of internet and social media in intercontinental relations with precise attention recruitments and fund mobilization.

4.4.3 Policies pertaining use of social media on security management

4.4.3.1 SM policies Availability in NPS

The respondents were asked if there were policies guiding police officers in the use of social media on security management. The response is as shown in the table below

Table 4.13 are there Policies that guide NPS in use of Social Media

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	64	34.0	34.0	34.0
	No	94	50.0	50.0	84.0
	Don't know	30	16.0	16.0	100.0
	Total	188	100.0	100.0	

The respondents were asked if they had knowledge of any policies to guide the police officers in the use of social media. Majority of the respondents 94 (50%) indicated that there were no policies while 64 (34%) of the respondents indicated there were policies and 30 (16%) didn't know of existence of such policies.

4.4.3.2 Statements on Policies

The researcher requested the respondents to indicated their level of agreement in the statements below whereby 1=Strong Disagree 2= Disagree 3=Neutral 4= Agree 5= Strongly Agree.

Table 4.14 Statements on Policies

Statement	Strong Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Std. Dev.
Police officers are adequately trained on how to prosecute offensive use of Social Media by citizens	0	94 (50%)	9 (4.8)	85 (45.2)	0	2.95	.977
Are there sufficient laws and policies to control the use of social media in Kenya	0	156 (83.0)	23 (12.2)	9 (4.8)	0	2.21	.571
There is legal framework guiding NPS on use of social media	0	96 (51.1)	37 (19.7)	55 (29.3)	0	2.78	.871
Government should snoop (eaves drop) private/ individual social media accounts for security reasons	0	38 (20.2)	0	150 (79.8)	0	3.59	.805
The rate of conviction for social media offenders is high in Kenya	1 (0.5%)	186 (98.9%)	1 (0.5%)	0	0	2.00	.103

Source: primary data 2022

The study asked the respondent whether the police officers were adequately trained on prosecution of offensive use of Social Media by citizens. Majority of the respondents disagreed 94 (50%) followed closely by those who agreed 85 (45.2%) while 9 (4.8%) were neutral. The statement mean was 2.95 and std. dev. (.977). One respondent indicated

> We are trained but challenged with which digital content to include or exclude in the case presentation

However, majority indicated that, the responsibility of prosecution in in the domain of ODPP and their work is investigation and preparation of charge sheets.

On the statement whether there were sufficient laws and policies to control the use of social media in Kenya, majority of the respondents disagreed 156 (83%), 23 (12.2%) were neutral, while 9 (4.8%) agreed. The statement mean was 2.21 and std. dev. (.517). The finding denoted that, the respondents felt the existing laws governing the abuse of SM were insufficient or weak altogether. Majority of the respondents were not conversant with the Computer Misuse and Cybercrimes Act (Computer Misuse and Cybercrimes Act No 5 2018) which criminalises identity theft, cyber stalking, chat room abuse and impersonation.

The study further sought to find out whether there was legal framework guiding NPS on use of social media. 55 (29.3%) of the respondents agreed and 37 (19.7%) were neutral. However, 96 (51.1%) majority of the respondents agreed with the statement. The mean of the statement was 2.78 and std. dev. (.871). The respondents who agreed cited National Police Service Act 2011 and the National Police Service Commission Act 2011 which provides for powers, functions, procedures and jurisdiction guiding NPS in their responsibilities. However, they were not aware of existence of single policy document addressing use of social media.

On whether the Government should snoop (eaves drop) private/ individual social media accounts for security reasons, 38 (20.2%) disagreed but the majority of the respondents 150 (79.8%) agreed. The statement had a mean of 3.59 and std. dev. (.805). One disagreeing respondent stated that:

> It will amount to violating individuals' privacy

However, those in agreement cited it should be done within set parameters and the law enforcement organs should continually upgrade their technologies and gears to match up new crime patterns that are digitally super sophisticated in operation.

The respondents were further asked whether the rate of conviction for social media offenders if it was high in Kenya. Majority of the respondents 186 (98.9%) disagreed while 1(0.5%) each strongly disagreed and neutral. The statement had a mean of 2.00 and std. dev. (.103). The findings concur with SIMELAB (2018), which noted SM offender had their charges dropped or court setting them free due to lack of witness or proper legislation in spite of provisions of section 9, with enactment of Computer Misuse and Cybercrimes Act 2018.

4.4. Influence of social media on security management

The research asked the respondents whether they though if media had any influence in the overall security management by NPS. The response was overwhelming in affirmation whereby they cited videos of crime that had been shared to police aiding in apprehension and prosecution of offenders. In addition, the respondents cited several NPS products that allows for citizen to report crime while still hiding his/her identity, for example "*fichua kwa DCI/polisi*".

4.4.1 Level of insecurity attributed to offensive use of social media

The study further wanted to find out level of insecurity emanating from abuse of SM. The response is as shown in table 4.15

Table 4.15 Level of insecurity attributed to SM

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High	113	60.1	60.1	60.1
	Low	75	39.9	39.9	100.0
	Total	188	100.0	100.0	

Table 4.15 clearly shows that, majority of the respondents 113 (60.1%) indicated that the level of insecurity stemming up from misuse of SM were high while 75 (39.9%) indicated the level was low. The statement had a mean of 2.60 and std. dev. (.491). The information of the level

of insecurity or crimes arising from misuse of SM is obtainable from daily cases reported to police stations and recorded in the Occurrence Book commonly referred to as O.B. One interviewee said

"Misuse of SM is very high especially cases of impersonation and insults." In agreement with the above quote, one officer responded in Swahili, "hii wakati wa siasa tunajionea mengi" meaning during campaign period we get a lot of cases.

The two responses agree with Makinen and Kuira (2018) who observed that, during election period heightened political events arouse hatred among different tribal dialects, fake news, propaganda, hate speech and insults.

4.4.2 Statements on Influence of SM is security management

In your opinion, state the level of extent the following statement will influence security management by NPS through using social media

Table 4.16 Influence of SM is security management

Statement	Very Great Extent	Great Extent	Moderate	Low Extent	Not at all	Mean	Std. Dev.
Regular civic education on positive use of social media	33 (17.6%)	150 (79.8)	5 (2.7)	0	0	1.85	.425
Government should block or shutdown social media sites that are offensive	27 (14.4)	137 (72.9)	24 (12.8)	0	0	1.98	.521
Government should collaborate with social media platform owners like Facebook	0	153 (81.4)	35 (18.6)	0	0	2.18	.390
There should be interception and censorship of offensive posts	0	160 (85.1)	28 (14.9)	0	0	2.14	.354
Apprehension and prosecution of social media offenders	18 (9.6%)	170 (90.4)	0	0	0	1.90	.295

On the level of extent to which social media can influence through regular civic education on positive use of social media, 33 (17.6%) of the respondents indicated to very great extent and the majority 150 (79.8%) were of the opinion it would influence in great extent while 5 (2.7%) indicated it would be moderate. The statement mean was 1.85 and std. dev. (.425). This implies that, NPS social media platforms would be useful to the greater extent in providing information to the general public as was the reply of one respondent,

> Official messages have been sent through social media platforms giving directions to the public concerning diverse issues.

The study asked the respondents whether they thought if Government by blocking or shutting down social media sites that are responsible for offensive SM posts would influence its use. The majority of the respondents 137 (72.9%) were of the opinion it would influence to great extent and 27 (14.4%) to very great extent while 21 (12.8%) of the responded it was moderate. The statement means of 1.98 and std. dev. (.521) implied that if offensive social media sites were blocked or shutdown, it would have a positive impact on security management.

If Government collaborates with social media platform owners like Facebook, majority of the respondents 153 (81.4%) were of the opinion it would influence the use of SM to great extent while 35 (18.6%) indicated it would but moderately. The statement had a mean of 2.18 and std. dev. (.390).

> Collaborating with platform hosts it would help by pulling down sites that are used by criminals was the reply of one interviewee.

He further gave examples where pages of jihadists like ISIS, Al-Qaeda and other terror network have been flagged and pulled down.

On the statement whether offensive SM posts should be intercepted and censored majority of the respondents 160 (85.1%) agreed to great extent while 28 (14.9%) were moderate. The statement mean was 2.14 and std. dev. (.357). One respondent noted that,

> NPS through the DCI can intercept but you get to know what has already been posted, therefore accounts that are perceived to be used by criminal are flagged or shutdown.

On the influence of SM in Apprehension and prosecution of law breakers, 18 (9.6%) agreed to very great extent and the majority of the respondents 170 (90.4%) agreed to great extent. The statement mean was 1.90 while std. dev. (.295). Videos recorded and shared on social media platforms have greatly helped in management of national security during times of disasters, riots and other crime whereby photographs and video circulating online help capture perpetrators or rescue the victims.

CHAPTER FIVE

DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summarized results on the influence of social media in security management with reference to Kilimani and Dagoretti police divisions. In addition, the chapter presents conclusions based on the summarized study results and further makes recommendations based on the conclusions

5.2 DISCUSSIONS OF THE STUDY FINDINGS

5.2.1 Effective use of Social Media in National Security Management

Majority of the respondents had the necessary information required to help achieve the set study objectives for they had worked in the NPS for a considerable long period. The primary data collected and analysed revealed that SM was effective in creating public awareness to very great extent. During national holidays or city marathons, SM comes in handy when roads are closed. Motorists are advised on diversions and time when the roads will be reopened information available on NPS SM platforms. In absence of Social Media, such information was only available through newspaper and news bulletin which could not reach wide audience as SM does. One of the most quoted case study was of the late chief Kariuki of Lanet Umoja location in Nakuru North Sub-Count who by using of twitter helped to recover stolen domestic animals in his area and other properties, report crime timely, find missing child and public announcements. The social media platforms used by NPS were Facebook and twitter.

Influence of SM on security management was found to be of great extent in intelligence gathering, counter Propaganda, and apprehending criminals. This concurred with Gad (2017);

Nsudu and Onwe (2017) and Trottier and Fuchs (2014). SM was found to be moderate in crime Prevention and low extent in administration. The social media tools have characteristics that enable sharing of information in form of videos, photos blogs which can be used in security response. Surveillance of digital platforms can also enable detection and timely response. Social media can used to foster positive relationships with the community, and monitoring for criminal activity (LexisNexis, 2014). The online platform for reporting crime or any suspicious activities for example, fichua kwa polisi had helped the officers in intelligence gathering.

The Collective Security Approach Theory used in this study was useful since as the research found out security management is complex and cannot be handled by NPS single handed but calls for collaboration with other security actors. Security management has many players for example, police, administrators, intelligence and security analysts/ consultants who by pooling knowledge and skills together can deter insecurity in various fronts.

5.2.2 Security challenges posed by Social Media on National Security Management

The research found out that there myriad challenges faced by police officers in the use of social media. The study established that police officers were not adequately trained on the use of Social Media. According to Arnoff (2007), where training was absent, incompetence, inefficiencies and ineffectiveness abound. He further noted that, training improved technical competences and that training was found to be invaluable to staff in various governments. Therefore, training is paramount for it entails having technical know-how. Training police officers to deal with electronic crimes, the dynamics of social media and acquiring recent digital forensic tools can go a long way in crime detection and prevention.

It was also established that, there were no sufficient infrastructure to facilitate use of SM on security management like internet, computers and open source intelligence software. Olaka

(2017) also cited lack of internet and digital communication devices which fundamentally ought to be available in using social media on security management in his study on the knowledge and practices on utilization of social media for Security Management in Kitui West Sub County. Ndonye (2019) on the implications of technological advancement on policing noted that, though there was use of digital technologies they were not advanced and neither superior to detect and prevent crime.

Having infrastructure coupled with training, will help NPS in security management. Walter (2012) further noted that, contents shared on SM platforms are viewed by billions of people globally; bringing a lot of trouble to law enforcers because content shared is not filtered to fit all audiences thus wrong information shared can cause irreversible damage. NPS did not have mechanism to filter and tackle social media offenses.

On the other hand, security challenges resulting from abuse of social media platforms, the fake news, hate speech, propaganda, cybercrime and radicalization are the often reported cases committed through SM. SIMELAB (2018) and Ghonim (2012) have categorically stated that, SM has been used as a tool for recruitment, fundraising and mobilization of criminal groups, opinion shaping to influence change, empowering and boosting morale of the targeted groups; and that it was often fed will troll of fake news, propaganda, hate speech in order to interfere with online debates especially political to influence elections and damage the reputation of certain individuals. However, on the issue of fundraising for criminal the study found its extent of use was low contrary to Ranko and Haase (2018) who had indicated that, very great magnitude of social media in intercontinental relations with precise attention recruitments and fund mobilization.

5.2.3 Policies that guide NPS in using social media on Security Management

In response to social media platforms becoming often used as means of spreading false broadcast and hate speech, the government enacted the Computer Misuse and Cybercrimes Act (Computer Misuse and Cybercrimes Act No 5 2018, sections 22-23) which make it criminal to publish false reports and communicating in a manner deemed offensive by the recipient. This was to add to the Kenya communications (Amendments) Act 2013 which had failed to address cyber-crimes committed against the person. The legal provisions were specific to crimes such as identity theft, cyber stalking, chat room abuse and impersonation. In spite of this legislation, apprehended offenders were in most cases set free by the courts of law or had their charges dropped. Most critics of SM laws argue that, the enacted regulations are a threat to freedom of speech and expression and they are in clear violation to privacy.

Concerning policies guiding NPS in social media use or misuse, the study established that there was no policy document regarding use of SM in work related matters. However, there was spread awareness that, personal SM platforms could not be used in an official capacity and vice versa. The police officers are guided by the National Police Service Act 2011 and the National Police Service Commission Act 2011. The said Acts details the powers, functions, procedures and jurisdiction guiding NPS in their responsibilities.

The study established the laws and policies to control the use of social media in Kenya were not sufficient since rate of conviction for social media offenders was near zero. This can be attributed to either as the study found that police officers were not specifically trained to prosecute offensive use of Social Media by citizens or lack of awareness of existing legal framework. Crime can be prevented when security agents get to know such plans. However, offenses are on SM are difficult to intercept or prevent since as the study established Government does not snoop (eaves drop) private/ individual social media accounts for security reasons which can aid in detection and prevention.

The influence of SM in security management is not cramped in Kenya alone, many governments across the Africa and Asia has resulted to block internet access to shutdown social media. This was to avoid mobilization of crowds in riots or dissemination of information deemed to threaten national security. Capacity wise, security agents across the continents lacked technological sophistication capacity and are ill equipped to fight cybercrimes and other evils associated with social media. Globally, China is reported to be advanced in spying on its citizens and having sophisticated cyber laws, cyber control abilities and dedicated social media police enforcement unit, but still the law enforcement could not keep up with the pace of growing numbers of social media users and amount of content that is being generated and distributed, Xinxin (2018).

Social Responsibility Theory advocating for media freedom and citizen responsibility should be championed that the SM content creators can be free from government interference in order to fulfil their mandate. SRT theory states that, there would be no need for government to regulate the media and its participation in dispersing reports and information to the public when the producers of contents prove to be responsible.

5.3 Summary of Main Findings

The study found out that NPS used social media platform as medium of communication. Twitter and Facebook were SM platform used in additional to traditional means of communication. The research also found out that, there are designated police officers responsible for operation of the SM platforms though messages from senior police officers was often received to be official police communication by the members of the public. SM was found to be mostly used in creating public awareness, in intelligence gathering, countering propaganda, and apprehending criminals but very scarcely in administration. The benefits of

social media platforms were sometimes dented by misuse where trolls of fake news, propaganda, hate speech also thrived.

The study also found out that, lack of the infrastructure that is, internet and digital communication devices which fundamentally ought to be available in using social media on security management and the ones available were not sufficient neither sophisticated to detect and prevent SM criminal activities. In addition, police officers were not trained on SM; its use and abuse.

On policy, the study established that, most police officers were not conversant with the Computer Misuse and Cybercrimes Act (Computer Misuse and Cybercrimes Act No 5 2018, sections 22-23) but were well informed on the police powers and functions as enshrined in the National Police Service Act 2011 and the National Police Service Commission Act 2011. The existing laws and policies to control the use of social media in Kenya were not well understood to help in apprehension and prosecution of offensive contents posted on SM.

5.4 Conclusions

The study concludes that, social media have great influence in security management. In addition, the study concludes that, SM though useful for constructive communication and dissemination of information, it was also used by subversive elements maliciously to spread fake news, hate speech, and commit cybercrimes. The study concludes that, NPS did not have technological sophistication capacity to respond to all offenses associated with social media

The study concludes social media tools enabled sharing of information in form of videos, photos blogs which were used in security response and was used to gather intelligence, report crime and clarify propaganda.

5.5 Recommendations

Good laws governing the social media usage should be legislated to avoid criminals getting off the hook with a slap on the hand. This will be enabled by formulation of substantial policies and laws regarding use and dissemination of digital content.

Since the advancement of technologies pose a challenge to a police service that has been using 'brick and mortar' in fight against crime; the study recommends acquisition of recent tools, while providing training in all levels of forensic modus operandi and in using advanced digital technologies. The NPS should be well funded to help in acquisition of modern digital technologies that there will be timely detection and prevention of cyber-crime.

The study recommends regular in house training of police officers to deal with electronic crimes and the dynamics of social media. Training was described by Sababu (2010) as a process aimed at improving mental and physical abilities to better perform a given task. Sila (2014) noted that training brings an employee up to date with the current happenings in the social, political, economic and technological world.

The said measures will influence the security management on digital front hence early detection of crimes, reduced electronic crime rates and have a positive impact on the ability of officers to respond appropriately.

5.6 Areas of Further Research

The study recommends further research in the roles of civilian in security management through the use of social media. In addition more research should be conducted on policies and law that govern the use of social media in private sector.

REFERENCES

Christopher G. and Peter M. (2021). *Africa internet: Where and how are governments blocking it*? Retrieved from https://www.bbc.com/news/world-africa-47734843 on 19th Feb 2021

Communications Authority of Kenya. (2020). *Fourth Quarter Sector Statistics Report for the Financial Year 2019/20* (April-June 2020)

Cooper, D. & Schindler, P. (2011). *Business research methods* (7th ed.). Singapore: Mc Graw-Hill

Cuman K., (2012). *The Role of Internet and Social Media in International Relations: Arab revolution of 2011.*

Das, S., Nayak, T., Dept, A.-P., & University, C. (2013). *Impact of Cyber Crime: Issues and Challenges. International Journal of Engineering Sciences*, 6(2), 142–153.

Ghonim, W. (2012) *Revolution 2.0: The Power of the People is Greater Than the People in Power.* Houghton Mifflin Harcourt, Boston

Gilboa E., (2009). *Media and Conflict Resolution*: A Framework for Analysis, Marquette Law Review: 93(87).

G.O.K. (2020). The Kenya Gazette. *The National Police Service Act*. Vol. CXXII - No. 32. Nairobi: Government printer

Harmon A. and Chomsky M., (2010). *How to Create a Smart Mob: Understanding a Social Network Capital*. Wellesley College

Hodge, N. (2010). "*U.S. Diverts Spy Drone from Afghanistan to Haiti*." Wired Magazine Online. January 15, 2010.

Iraki F. K., (2010). *Cross-media Ownership and the Monopolizing of Public Spaces in Kenya,' in Wa-Mungai, Mbugua and George Gona (eds.), (Re) Membering Kenya: Idenity, Culture and Freedom.* Nairobi: Twaweza Communications.

Kenya Police Service (2014). *Crime statistics report 2013/25*. Nairobi. KPS

Kimani, B. (2020). *Missing School Girls Found after Police Raid*. Retrieved from Kenyan news.co.ke on Feb 20, 2021

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

Klaehn, Jeffrey (2002) ‗A critical Review and Assessment of Herman and Chomsky's Propaganda Model, 'European *Journal of Communication*, 17, pp.147-174.

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Delhi: New Age International.

KPMG. (2016). *Small Business Reputation & the Cyber Risk*. Retrieved January 24, 2021 from KPMG: http://www.kpmg.com/channelislands/en/about/Documents/small-business reputation-and-the-cyber-risk.pdf

Kshetri, N. (2015). *The global cyber-crime industry: economic, institutional and strategic perspectives.* Berlin: Springer.

Kshetri, N. (2017). *Cyber-victimization and cyber security in China*. Communications of the ACM.

Lasswell, H. D. (1927). The Theory of Political Propaganda' *The American Political Science Review*, 21:3, pp. 627-631

Mäkinen M. and Kuira W., (2008). *Social Media and Postelection Crisis in Kenya*, Press/Politics, 13(3).

Moon, K. (2010). *Physician's assistant student involved in the Haiti relief effort with an independent medical volunteer group.* Personal interview. April 6, 2010.

Mugenda, O. & Mugenda, A. (2012). *Research methods*: Quantitative and qualitative approaches. Nairobi: Acts Press.

Munyua, A. (2011). *Social Media as a positive tool for social transformation*. Nairobi: KICTANEX

Nassiuma, D. K. (2000). *Survey sampling: Theory and methods.* . Nairobi: University of Nairobi Press

Ndonye, R., N. (2019). *Implications of Technological Advancement on Performance of Police Officers.* University of Nairobi

Ngige, C.V., Badekale, A.F., Hamman, J.I. (2016), The media and boko haram insurgency in Nigeria: *A content analysis and review. International Journal of Peace and Conflict Studies (IJPCS*), 3(1), 58-65.

Nsudu, I., Onwe, E.C. (2017), Social media and security challenges in Nigeria: The way forward. *World Applied Sciences Journal*, 35(6), 993-999.

Philip M. N. (2001). Social Responsibility and Commercial Broadcast Television: An Assessment of Public Affairs Programming in JMM, *The International Journal on Media Management*. Vol. 3, No. IV, 2001

Portland Communications. (2018). '*The Reality of Fake News in Kenya.'* https://portland-communications.com/pdf/TheReality-of-Fake-News-in-Kenya.pdf accessed 10 Feb 2021

Roach C., (1993). *Information and Culture in War and Peace: Overview, Communication and culture in war and peace*. SAGE Publications: California.

Sajithra, R., and Patil, K. (2013), *Social media–history and components. IOSR Journal of Business and Management* (IOSR-JBM), 7(1), 69-74.

Sändig, J. (2015), *Framing protest and insurgency: Boko haram and MASSOB in Nigeria*. Civil Wars, 17(2), 141-160.

Saunders, M., Lewis P. and Thornhill, A (2009) *Research Methods for Business students*. India: FT Prentice HQ

Sekaran, U. (2007). *Research Methods for Business: A Skill Building Approach.* . (6th. Ed.). New York: John Wiley & Sons, Inc.

Shuchman M. and Wilkes M. S. (1997). Medical Scientist and Health News Reporting: *a case of Miscommunication*. Volume 126 Issue 12, Pages 976-982.

The Associated Press. (2017), "*Boko Haram Leader in New Video Vows to Establish Caliphate. West Africa*: An Associated Press.

The Government of Kenya. (2018). *Computer Misuse and Cybercrimes Act No 5 2018, sections 22-23.* Nairobi: Government printer

Trottier, D., Fuchs, C. (2014*), Theorising Social Media, Politics and the State: An Introduction*. UK: Westminster

Umati (2013): Umati: *Monitoring Online Dangerous Speech*. Nairobi, Kenya.

United Republic of Tanzania (2020). *The Electronic and Postal Communications (Online Content) Regulations, 2020.* Dodoma: Government Printer

Walsh, P. l and O'Connor, C. (2018). *Social media and policing: A review of recent research*. UK: John Wiley

Wa-Mungai, M., (2010). Soft Power, Popular Culture and the 2007 Elections, 'in *Karuti Kanyinga and Duncan Okello (eds.), Tensions and Revisals in Democratic Transitions: The Kenya 2007 General Elections*. Nairobi: Society for International Development.

Weng, J. and Christopher W. J. (2010) '*TwitterRank: Finding Topic Sensitive Influential Twitterers'WSDM* 10, February 2010

West, M. D. (2021). *Shutting down the internet*. US: Brookings

White, N. (Ed.) (2003). *Collective Security Law*. Aldershot, UK: Ashgate.

Williams, P D (2010), "Explaining and Understanding Security Cooperation in Africa", African Security Review, Vol 19, No 2, pp 97-105

Wolfsfeld G., (2004). *Media and the path to peace, Cambridge, Cambridge University Press. Livingston L., (2006). The Politics of Media Culture and Media Culture Politics, 'in Wa-Mungai, Mbugua and George Gona (eds.), (Re) Membering Kenya: Idenity, Culture and Freedom.* Nairobi: Twaweza Communications

Xinxin, Z. (2018). *China to Further Safeguard Cyber Security*. http://english.peopledaily.com.cn/90882/7704949.html. Accessed 12 Feb 2021

APPENDICES

APPENDIX I: INTRODUCTION LETTER

REF: REQUEST FOR PARTICIPATION IN RESEARCH STUDY

My Name is Jerusha a student at Africa Nazarene University. I am currently undertaking research study on the Influence of Social Media on Security Management a case study of National Police Service as academic requirement for course completion. I kindly request you to spare some time from your busy schedule and fill in the enclosed questionnaire. All the information provided is for academic purpose only and will be treated with utmost confidentiality.

Your timely response is highly appreciated. Thank you in advance

Yours Faithfully,

Jerusha Nooretet

APPENDIX II: CONFIDENTIALITY AGREEMENT

INFLUENCE OF SOCIAL MEDIA ON SECURITY MANAGEMENT IN KENYA: A CASE STUDY OF THE NATIONAL POLICE SERVICE; KILIMANI AND DAGORETTI POLICE DIVISION.

I Jerusha Nooretet Loonkosho, the lead Researcher in the above indicated study

Promise and agree to -

1. Keep all the research information shared with me confidential by not discussing or sharing the research information in any form or format (e.g., disks, tapes, transcripts) with anyone other than the *Researcher(s)*.

2. Keep all research information in any form or format secure while it is in my possession. And After consulting with the *Researcher(s),* erase or destroy all research information in any form or format regarding this research project that is not returnable (e.g., information stored on computer hard drive).
3. Keep all responses deemed sensitive anonymous and confidential
4. Other (specify).

_____	_____	_____
(Print Name)	(Signature)	(Date)

Respondent(s)

_____	_____	_____
(Print Name)	(Signature)	(Date)

APPENDIX III: QUESTIONNAIRE

Please tick in the boxes provided below each question. Write your answer in the space provided. If the space provided is insufficient use the back of the respective page.

Part A: Demographic Background

1. Kindly indicate your gender.

Male ( ) Female [ ]

2. Police Division:

Kilimani ( ) Dagoretti ( )

3. How long have you served in NPS (years)

Less than 1 year ( )

1 – 5 years ( )

6 – 10 Years ( )

11 – 15 years ( )

16 – 20 years ( )

Above 21 Years ( )

4. What Social Media tools do you use for personal interactions? Tick all that apply.

Twitter ( ) Facebook ( ) Tiktok ( )

LinkedIn ( ) YouTube, ( ) Skype ( ) Flickr ( )

Other (please specify)…….

Part B: Effectiveness of Social Media use in Security Management

5. Does the National Police Service use Social Media on Security Management

Yes ( ) No ( )

If yes, which social media platforms are used?

a. Twitter ( )

b. Facebook ( )

c. LinkedIn ( )

d. YouTube ( )

e. Other……

6. How effective in your opinion is the use of social media on security management by NPS?

……

……

……..

7. Who is allowed to use Social Media for **work related** purpose at NPS?

All Officers ( )

Only the seniors Police Officers ( )

Officers designated by the IG ( )

8. Is there a dedicated integrated police unit responsible for monitoring use of Social Media?

Yes ( ) No ( )

If yes in 8 above, kindly explain their role

……

……

……..

9. How are the use social media platforms effective in the following statements?

Statement	**Very Great Extent**	**Great Extent**	**Moderate**	**Low Extent**	**Not at all**
Creating Public Awareness					
Intelligence gathering					

Crime Prevention

Counter Propaganda

Administration

Apprehending criminals

Any other use ……..

……

Part C. Challenges in Use of Social Media on Security Management

10. What are the security challenges you face on the use of social media on security management?

……
……
……
……
……

11. Kindly evaluate the following statements on challenges of Social Media on Security Management and either agree or disagree with them.

Where 1=Strong Disagree 2= Disagree 3=Neutral 4= Agree 5= Strongly Agree

Statement	1	2	3	4	5
Are police officers adequately trained on use of Social Media					
Is there infrastructure to facilitate use of SM on Security Management					
There are tools to filter and monitor social media use in Kenya					
There is laid down mechanism to aid police officers in tackling social media offenses					

Any other comment on the above statements
……

……

12. Kindly evaluate the following statements on security challenges of Social Media on Security Management and indicate the level of extent

Statement	Very Great Extent	Great Extent	Moderate	Low Extent	Not at all
Cyber crime					
Radicalization					
Terrorism					
Hate speech/ propaganda					
Fundraising for criminal activities					

Any other security challenge posed by use of social media
……..

Part D: Policies pertaining use of social media on security management

13. Are there policies guiding police officers in the use of social media on security management?

Yes ( ) No ( )

If yes which ones are you aware of?
……
……
…….

14. Kindly read through the statements below and tick according to your level of agreement

Where 1=Strong Disagree 2= Disagree 3=Neutral 4= Agree 5= Strongly Agree

Statement	1	2	3	4	5
Are police officers adequately trained on how to prosecute offensive use of Social Media by citizens					
Are there sufficient laws and policies to control the use of social media in Kenya					
There is legal framework guiding NPS on use of social media					
Government should snoop (eaves drop) private/ individual social media accounts for security reasons					
The rate of conviction for social media offenders is high in Kenya					

Any comment on above statements?
...…….....

15. What can be done to improve existing laws on use of social media on security management ……..

Part E: Influence of social media on security management

16. Does social media have an influence in the overall security management by NPS and to what extent?

……
……
……
…….

17. What is the level of insecurity that can be attributed to offensive use of social media?

Very high ( ) High ( ) Low ( )

18. In your opinion, state the level of extent the following statement will influence security management by NPS through using social media

Statement	**Very Great Extent**	**Great Extent**	**Moderate**	**Low Extent**	**Not at all**
Regular civic education on positive use of social media					
Government should block or shutdown social media sites that are offensive					
Government should collaborate with social media platform owners like Facebook					
There should be interception and censorship of offensive posts					
Apprehension and prosecution of social media offenders					

Any comment on the above statement ……

…….

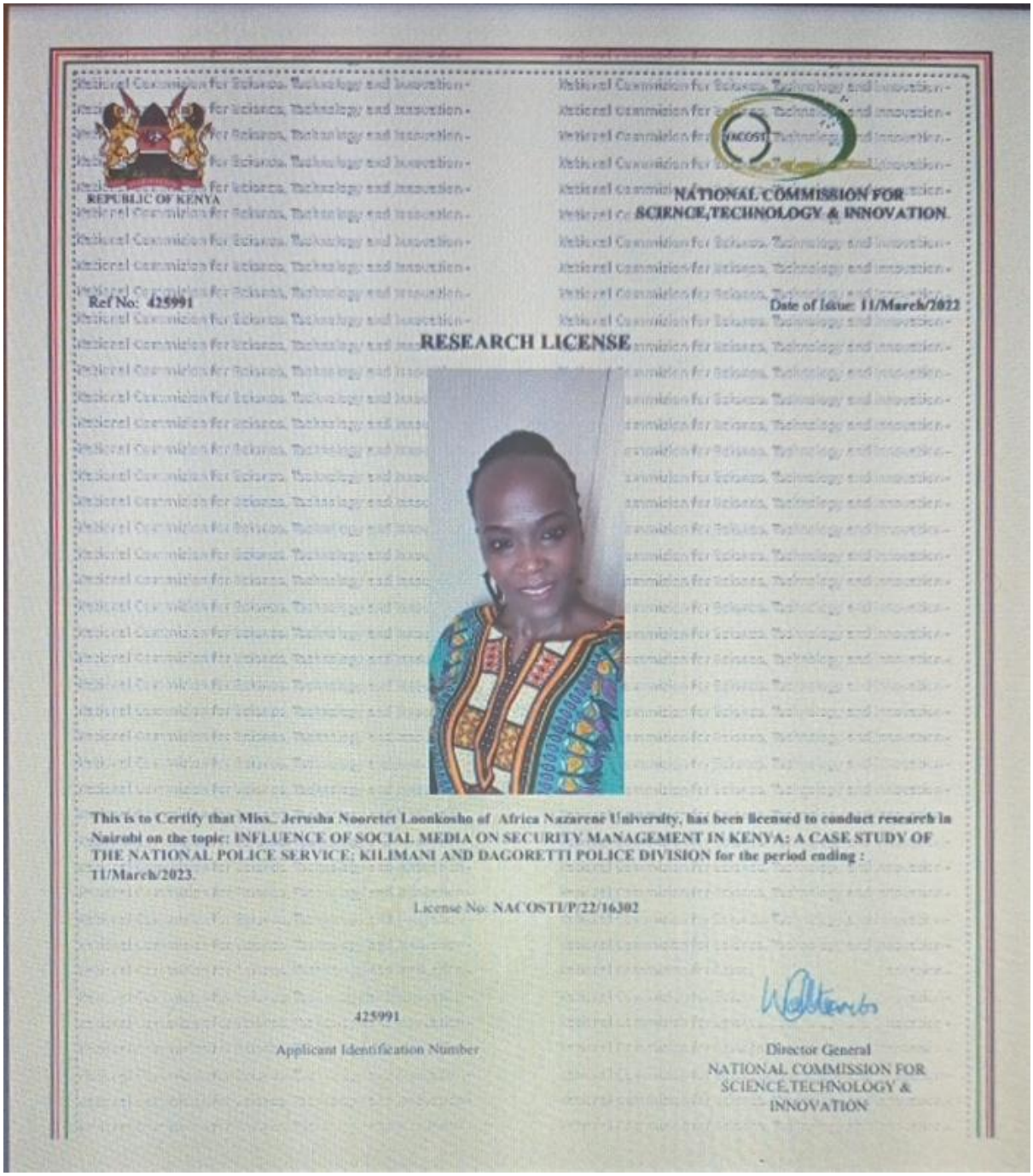
The end, Thank You

APPENDIX IV: INTERVIEW QUESTIONS

Interview Questions

1. In your opinion how effective is the use of social media on security management by NPS?
2. Are there policies guiding police officers in the use of social media on security management?
3. What are the challenges you face on the use of social media on security management
4. What can be done to address the mentioned challenges

APPENDIX IV: RESEARCH PERMIT NACOSTI



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 425991

Date of Issue: 11/March/2022

RESEARCH LICENSE

This is to Certify that Miss. Jerusha Nooretet Loonkosho of Africa Nazarene University, has been licensed to conduct research in Nairobi on the topic: INFLUENCE OF SOCIAL MEDIA ON SECURITY MANAGEMENT IN KENYA: A CASE STUDY OF THE NATIONAL POLICE SERVICE: KILIMANI AND DAGORETTI POLICE DIVISION for the period ending : 11/March/2023.

License No: NACOSTI/P/22/16302

425991

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

APPENDIX V: UNIVERSITY RESEARCH LETTER

AFRICA NAZARENE
UNIVERSITY

3rd March 2022

RE: TO WHOM IT MAY CONCERN

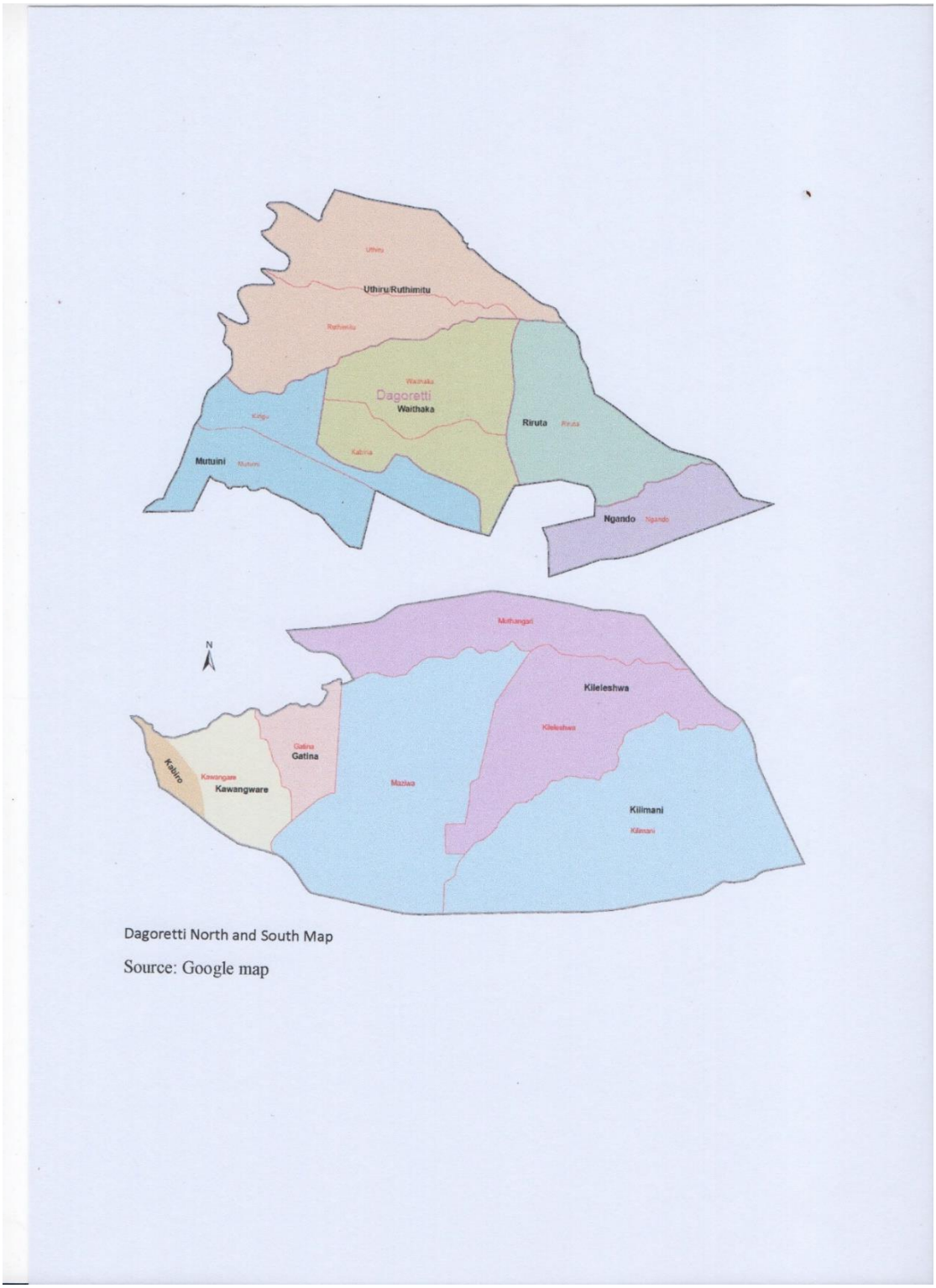
Jerusha Nooretet Loonkosho (**19s01dmgp009**) is a bonafide student at Africa Nazarene University in the School of Humanities and Social Sciences, Governance, Peace and Security Studies department. She has finished her course work and has defended her thesis proposal entitled: - ***"Influence of Social Media on Security Management: A Case Study of the National Police Service Kilimani and Dagoretti Police Division Kenya."***

Any assistance accorded to her to facilitate data collection and finish her thesis is highly welcomed.

Rodney T. Reed.

Prof. Rodney Reed.
DVC, Academic & Student Affairs

APPENDIX VII: SITE MAPS



Dagoretti North and South Map

Source: Google map