UNIVERSITY OF NAIROBI

SOCIAL MEDIA AND NATIONAL SECURITY THREATS: A CASE STUDY OF KENYA

BY

JULIUS KIPKORIR KIMUTAI

R50/68426/2011

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE DEGREE OF MASTER OF ARTS IN INTERNATIONAL STUDIES, INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES, UNIVERSITY OF NAIROBI

2014

DECLARATION

This research project is my original work and has not been presented to any other university.

JULIUS KIPKORIR KIMUTAI

R50/68426/2011

Signature……. Date……

Supervisor

This research project has been submitted for examination with my approval as the University of Nairobi supervisor.

Name.....

Signature……. Date……

DEDICATION

I dedicate this work to all members of my family

ACKNOWLEDGEMENT

I would like to thank Dr. Patrick Maluki, my supervisor for his wise counsel, incisive insight resulting to an immense contribution for this study. And all my family members for their help; in particular my wife Rose who offered me enormous support and guidance. Not to mention all my fellow colleagues for cheering me up and being supportive.

And to God, who has provided for, guided, and sustained me during this period of my training and academic work.

May the Almighty God bless you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Social Media are connection and mass communication tools, characterized by a global diffusion and an ever-growing level of use, considering their handiness and flexibility, as well as their extreme cheapness. Social media platforms has far reaching social and security implications for the people of Kenya, their government and its national security agencies such as the military and the police. In order to protect Kenya's freedom, security and prosperity, it is only fair that some serious studies be done about how the Government can harness online social networking tools and in equal measure monitor them in the event it threatens national security. The purpose of this study is to analyze social media and national security threats in Kenya. Specific objectives were to examine: the threats of social media technology to Kenya's national security; the use of social media by the military in preventing, limiting or removing threats to national security; and the current state of Kenya's national security and how social media makes it worse. The study adopted survey research method. The target population was all members of the military working in Nairobi units and a sample size of 50 members of the military working in Nairobi units. The study used proportional stratified sampling method. From the findings, it was found that social media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members. It found that terrorist groups take advantage of Social Media to communicate with cyber-crime groups and to coordinate along with them fund-raising activities carried out in part or completely on the Internet. The study found that social media are also used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, at throwing civil population into a panic. Criminal organizations are threats on drug smuggling, human trafficking and money-laundering. It found that community criminal organizations like Mombasa Republican Council (MRC), '*Mungiki*' and '*Sungusungu'* use social media as a tool to recruit, communicate, Spread propaganda and radicalization to a great extent. On the other hand the military use social media for military operations, communicating process of operation, boost morale of soldiers, clarify on propaganda messages sent by enemies and dispelling rumors, for updating civilians on progress of military operation, for public relations and operations such as "operation Linda Kenya". It found that the military uses social media as Open-Source Intelligence (OSINT) to analyze social media threats as was the case in Westgate attack, Nairobi. The study found that the Kenyan Military uses social media as tool for Diplomacy in gathering and Disseminating Information. Through blogs, Facebook, emails and Twitter, Kenyans can source and comment on topical political, economic as well as social issues. The study found that the security in Kenya is average and Kenya is still grappling in the dark as the monster of hatred spreads. It found that social media has contributed towards cattle rustling, poaching, terrorism attacks, tribal clashes, information warfare and hate speech. The study concluded that terrorist groups take advantage of Social Media to communicate with cyber-crime groups and to coordinate along with them fund-raising activities carried out in part or completely on the Internet. It concludes that social media are also used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, throwing civil population into a panic. It concludes that counter propaganda is used by the military to counter social media threats. And that the best news management comes from the military since they have a range of options for communicating their standpoint. The study recommends that Kenya needs to develop a comprehensive and adaptive national government policy framework that identifies roles, responsibilities, and resources across the government in order to detect, defend and pre-empt social media threats to the nation.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The spread of social media, driven by internet boom and mobile technology is changing the way society operates.[1] For the past couple of decades, the two main screens have been the Television screen and the computer screen. These days a host of smaller screens have joined the line-up; the screen on a cell phone, Ipod or Ipad.[2] The emergence of the small screen has encouraged the emergence of new trends; mass media have become increasingly mobile. The emergence and use of wireless laptops and cell phones are the current trend that has taken the world by storm, best known as "social media". These simply are online communications that use special techniques that involve participation, conversation, sharing, collaboration, and linkage.[3]

Today, social media tools have become a staple in the everyday lives of many people becoming one of the main methods of social connection and interaction around the world, whether between individuals, or with businesses and governments. The growth of Web 2.0, its expanding global reach and potential new technologies to further its use and adoption argue that today's social networking is a change in the form of human communication that cannot be ignored. Online social networks have impacted every field of human endeavor from education to health care and many more. National security is no exception. Due to globalization, focus has now shifted to assessing the effects of non-state actors. The advancement in social media has increased the ability of non-state actors including terrorists, criminals, protestors, hate mongers and rioters to

[1]Ungerer C., (2012). *Social media and national security*, ASPI Strategic Policy Form, 27 February 2012, p1.
[2]Chadwish, Andrew (2006). *Internet Politics: States, Citizens and New Communication Technologies*. NY: Oxford University Press, 2006.p.11.
[3] Ibid

impact national and international security. Power is constantly shifting and diluting from states to groups and individuals.

Since Social Media are extremely quickly evolving and are facing a many-sided interaction with geo-economic and socio-cultural elements, it is important to constantly monitor how they develop, analyze how they work, and measure their potentialities. This process aims at making the states not to be caught by surprise in case of a potential offensive use of Social Media by adversaries and at changing such innovative tools into resources of primary importance, to be ready for all the bodies involved in the protection of the national security.

Social media platforms has far reaching social and security implications for the people of Kenya, their government and its national security agencies such as the military and the police. This study's key concerns are on social media and national security threats in Kenya. Advances in the sciences of computers have enabled social media to grow and reach the point where the exchange of information, both for good or evil now occurs on a global scale. For Kenya's national security planners, this information superhighway creates many challenges. In a world of "active global listening, higher premiums are placed on the ability of intelligence agencies to sort the background "chatter" from the more critical and useful information that forms intelligence for security agencies and decision makers.[4] Despite the fact that social media is outside state control and does not discriminate. Nevertheless, the study will demonstrate that their use can lead help state foresee how emerging threats will present themselves in the future and figure out how to counter their effects.

[4]Aday, Sean, Henry Farrell, Marc Lynch, and John Sides, (2010). *Blogs and Bullets: New Media in Contentious Politics*. Peaceworks, no. 65 (2010). P.11.

Since social media constitutes a threat to national security, it is imperative that study be done to determine the negative impact of social media on Kenya's national security. National security is the protection of Kenya's territorial integrity, its people, laws, values and national interests from both external and internal threats of all kinds (Constitution of Kenya, Article 238). This study therefore aims to provide the current state of the situation regarding the nature and use of social media in Kenya and its threats and risks to the military and national security in general.

1.2 Statement of the Problem

Kenya being a member of international community is not immune to forces of social media regarding its use and misuse. The use of social media as a new communication platform introduces serious security and privacy concerns, including new vectors for cyber-attack that the government and the military cannot ignore. Criminal gangs, terrorist organizations, non-state actors with bad intentions and subversive elements including Al-Qaeda and Al-Shabaab, regularly use social media websites to disseminate propaganda with sole intention to reach out, recruit and radicalize their target audience. Individuals use social media to send alarming messages, hate messages and false information to the public regarding state of national security affairs. Most of the social media users remain unanimous and cannot be easily traced by law enforcement agencies and subsequent prosecution. States therefore are faced with tough challenges to track, monitor and contain the use and misuse of social media relative to state security. National security demands a strategy such as e.g. monitoring conversations and content shared on Social Media, arranging effective methods to counter adversaries' propaganda and interferences, improving governmental agencies and institutions' performances, strengthening a state's geopolitical position and its international credibility. However, such initiatives require sophisticated technologies which are very complex, costly by third world countries.

Social media pose major threats and unfavorable consequences for national security. In order to protect Kenya's freedom, security and prosperity, it is only fair that some serious studies be done about how the Government can harness online social networking tools and in equal measure monitor them in the event it threatens national security. Therefore, like addressing any other national security challenge, the military and other security agencies need an understanding of how social media threatens national security. This study therefore will conduct a study about social media and national security threats, with specific reference to Kenya.

1.3 Objectives of the Study

1.3.1 General Objective

The general objective of the study is to analyze social media and national security threats in Kenya.

1.3.1 Specific Objectives

The specific objectives of the study are to:

i. Examine the threats of social media technology to Kenya's national security.
ii. Examine the use of social media by the military in preventing, limiting or removing threats to national security.
iii. Examine the current state of Kenya's national security and how social media makes it worse.

1.4 Research Questions

i. What are the threats of social media technology to Kenya's national security?

ii. How does the use of social media by the military prevent, limit or remove threats of national security?

iii. What is the current state of Kenya's national security and how does social media make it worse?

1.5 Justification of the Study

The value of this study has both academic and policy functions when finalized. Policy functions in that, nations will learn the threats of social media on their security and formulate policies that will regulate the way information is passed via social media. Similarly, it will also inform of counter strategies of the threats posed by social media. This study will enable nations identify the weaknesses and threats of social media and help steer the nation's security in the right direction, towards having a secure nation. There is need therefore to discuss a framework of social media which will help in understanding that social media is used to eradicate threats, same way it's being used as a tool by individuals and groups to instigate threats to people, society and a nation. Preliminary research indicates that there is little study that has been done here in Kenya and even elsewhere in Africa on the impact of social media on the national security. This study will therefore fill the literature gap as the discourse over social media and national security is just beginning and is in its infancy. In view of academics, students and scholars especially those undertaking International Relations and Diplomacy courses, as well as security studies will also benefit from the research as a source of information may be for their tasks in related topics.

1.6 Literature Review

An emergence of social media as a tool utilized by social organizations and an increasing set of security concerns does exist. However, these two ideas rarely converge in an academic setting, let alone that their convergence is not defined thoroughly. Social Media are connection and mass communication tools, characterized by a global diffusion and an ever growing level of use, considering their handiness and flexibility, as well as their extreme cheapness.[5] Using these media can cause several negative effects for national security and unfavorable consequences for a state's strategic interests. Nevertheless, their use can also lead to remarkable opportunities for a country in order to reach its strategic relevant goals, foresee how threats will work in the future and figure out how to counter their effects.[6]

Since Social Media platforms such as Facebook and twitter are extremely quickly evolving and are facing a many-sided interaction with geo-economics and socio-cultural elements, it is important to continuously monitor how they develop, analyses how they work, and measure their potentialities whether contributing positively or negatively to well being of state and citizens.[7] This process aims at making the states passively able to monitor, report and neutralize potential offensive use of Social Media by enemies and instead diverting such innovative tools into resources of primary importance, to be ready for all the bodies involved in the protection of the national security.

[5]Hasni A, 'Hacker group Anonymous claims attacking Greek official websites' As seen in The News Tribe, 9 October 2012, viewed on 29 November 2012.
[6] Ibid
[7]Sydney Morning Herald, 'Every Click They'll Be Watching' 12 July 2012, viewed 29 November 2012.

In a study about the role of internet and social media in international relations with particular focus of Arab revolution of 2011, Cuman (2011)[8], a documented analysis was conducted on the extent to which social networks such as the FaceBook, Twitter, youtube and weblogs played in facilitating uprisings in Egypt, Tunisia and Syria. The study found that the usage and growth of social media in the Arab region played a great role in mass mobilization of protestors, empowerment, shaping of opinions and influencing change. To date such Arab countries has witnessed constant conflicts and political instability, coupled with widespread social unrest affecting negatively on broader sets of economic, social, and political factors.[9] Social media therefore become a tool rather than the actual cause of the revolution. However, apart from the Arab uprising, there exists other examples of people using social media effectively as forms of threats to violence and secure communities exist. For example, during the London riots, the police and the public at large used the social media to fight against rioters and improve security. The London police scanned through the CCTV images to find the pictures of rioters.[10] Therefore, in an effort to understanding social media and national security, a number of studies has been documented especial on social dynamics of unrest and movements, driving on a directed ideological end.

To explain this, Social movement framework provides a context to the impact social media on national security. This can be contextualized in form of protest or political revolt against a regime. According to Herbert[11] Social movements can be viewed as collective enterprises to establish a new order of life. They have their inception in the condition of unrest, and derive their

[8]Cuman K., (2012). The Role of Internet and Social Media in International Relations. Arab revolution of 2011
[9] Davies, Catriona. "Yemen's Tribes 'Put Differences Aside' to Protest for Change." CNN World.
[10]Ghonim, W. (2012) *Revolution 2.0*: *The Power of the People is Greater Than the People in Power*. Houghton Mifflin Harcourt, Boston.
[11]ibid p. 30

motive power on one hand from dissatisfaction with the current form of life, and on the other hand, from wishes and hopes for a new scheme or system of living. Social movements have been occurring for centuries, and they have most often been connected with socio-political and economic changes. More often than not when changing the order of one's life it's good to look at the government and political straggles. Political struggle can take three different forms which are protest, collective action, and contention.[12] Protests are generally an expression of popular consciousness that are manifested in street politics; collective action occurs when a population has a shared interest and coordinates action on behalf of that interest; contention involves "claim-making," in which a party demands certain actions that would affect multiple parties' interests. Social movement theory often posits that communities with dense network ties are more likely to experience collective action than those with sparser ties. On the individual level, those recruited to participate in social movements are likely to possess more social ties to those already in the movement. Strong social ties or dense social ties in networks often facilitate an initial request to participate in a social movement and then smooth the way to participation by lessening the uncertainty of mobilization.

Although the strength of social ties strongly influences recruitment on the individual level, weak social ties can be effective in communicating and spreading the message of a social movement across diffuse networks hence an effective network structure would have dense networks of weak ties to outside entities in addition to strong interpersonal ties within those groups.[13] Since participants in social movements are often recruited through preexisting social ties, additional context is necessary to better determine the nature of individuals' interpersonal social ties to the

[12] Tilly C.,.(2011). Describing, Measuring, and Explaining Struggle. Qualitative Sociology 31, no. 1 (2011): 2
[13]McAdam D., Sidney T. and Charles T. (2008). Methods for Measuring Mechanisms of Contention. Qualitative Sociology 31, no. 4 (2008): 310.

movement. Such context illuminates whether it is the presence of a tie to the movement, the number of ties, or the strength of the tie that matters most. It is good to emphasize the importance of considering the manner in which social ties can both lead to increased and decreased activism. Individuals' large variety of relationships are all crucial elements of the context surrounding why those who had social ties to the movement chose to participate, and what the effect of ties to parents, peers, and others had on the decision.[14] In general, pre-existing organizational affiliation has been found to be a critical structural factor linked to participation in social movements, as membership in organizations facilitates the formation of increased interpersonal ties, and thus individuals belonging to certain groups are more frequently targeted for recruitment by movement organizers over unaffiliated individuals.

If certain mechanisms are proven to operate in similar ways across diverse settings, they are more likely to be important causal factors in the trajectory of social movements in general. Mechanisms such as bargaining and boundary deactivation, which is the diminishment of boundaries between local communities and national political networks, can help fuel an upward shift in scale as the process of bargaining between government officials and movement leaders can foster new ties and mutual understanding.[15]

Another key mechanism in the formation of social movements is the nature of the conversations in which individuals engage during coalition formation. The use of compartmentalizing mechanisms as a means by which organizers foster connections to a broader range of identities[16]. This is easily accomplished by focusing on a narrow scope of identities shared by many, such as

[14]McAdam D. and Ronnelle P., (1993).Specifying the Relationship between Social Ties and Activism. American Journal of Sociology 99, no. 3 (1993): 642.
[15]Ibid.,pp. 311-312.
[16] Ibid

that of a youth and by limiting the proposed timeframe of the coalition in order to alleviate concerns that participants are entering a constraining long-term agreement. "Conflation mechanisms" are used in a similar manner to establish a broad base of support through focusing on the "lowest common denominator" by playing up common identities while downplaying differences.

Social networking link individuals together as part of a voluntary group[17]. People join groups because they share common attributes, interests, activities, or causes. Within the group, they exchange information and opinions. As the group grows, it develops into a network and a social movement. A social network is a complex system. When systems become complex, their behavior cannot be easily predicted by traditional methods of analysis (i.e. breaking a system down into its component parts and analyzing the elements in detail).[18] As physicist Philip Anderson observed, aggregations of anything from atoms to people exhibit complex behavior that cannot be predicted by observing the component parts. Anderson noted that chemistry isn't just applied physics, that is, "you cannot understand all the properties of water from studying its constituent atoms in isolation"[19]. Likewise, social networking is more than simply the sum of the attitudes or activities of its members. The system's complexity creates outcomes that are different than the sum of the group. Furthermore, outcomes can be dramatically different from those that might emerge from a more rigid system, such as a government bureaucracy. That is because they are usually "nonlinear," often described as "disorganized" systems. Unlike

[17] E. Barsky and M. Purdon, "Introducing Web 2.0: Social Networking and Social Bookmarking for Health Librarians," Journal of Canadian Health Librarian Association, Vol. 27 (2006), p. 65)

[18] L. A. N. Amaral and J. M. Ottino, "Complex Networks: Augmenting the Framework for the Study of Complex Systems,"*The European Physical Journal* (May 14, 2004), pp. 147–162,

[19] Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin Books, 2008), p. 28.

hierarchical organizations, the outputs of a social network are less predictable and controllable. They are subjected to fewer rules and controls.

In social media and national security, movements/groups and social media have interacting systems which is the conversation that happens between parties.[20]This emphasizes the inter-reliance on account of all parties, but also the different needs and approaches by social movements and media organizations. Looking at this description from the contemporary perspective, there has been growth in the interaction of social media and movements/groups. As stated prior, new media has changed this relationship to an unparalleled place in modern history with the technology and tools available, such as Facebook, twitter and you tube. In relation to the social network, social media has greatly expanded the capacity and speed for establishing networks of people. More and more social networking applications are being developed for cell phones. Other new and different social networking is likely to emerge in the future as nanotechnology and new materials are developed that could greatly reduce the weight, cost, and power requirements for information sharing technologies.[21]

Melissa Lerner highlights the negative effects attributed to social media use by some social movement/groups theorists. Such includes increased access to online information by the public, combined with the often unregulated ability to publish a wide variety of information that can actually lead to an oversupply of confusing, inaccurate and distracting information.[22] In addition, the replacement of real-world, face-to-face communication decreases solidarity and consensus-building that is critical to social movements. Lerner argues that the combination of web-based

[20]Gamson, W.A., Wolfsfeld, G. (1993). Movements and Media as Interacting Systems. *Annals ofthe American Academy of Political and Social Science: Citizens, Protest, and Democracy*. 528, pp.

[21] James Jay Carafano and Andrew Gudgel, "Nanotechnology and National Security: Small Changes, Big Impact," Heritage Foundation *Backgrounder* No. 2071, September 21, 2007.

[22] Lerner M., (2010). Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt.*Journal of Muslim Minority Affairs* 30 no. 4 (2010): 557.

organizing and social movements, in which members participate both online and in the real world, can be very effective. Also, in a politically repressive climate, cyberspace can facilitate alternate avenues for expression that reduce some of the risks of public activism and can also provide otherwise unavailable information to encourage dissident sentiments or anti-government action. Although social network are being used politically, socially and in attempts to drive their grievances, these movements/groups are not originated by the technology, they are simply used to this end. Technology itself is neutral and can be used in innumerable ways. (Bijker et al. 1987) like all technology; mediums of social networks are not just tools, but also social constructs. They are used to create meaning, but their meaning is also socially constructed. (Castells 2007, 249) Even ICTs are created with the interests of one group against the interests of another. Technology and society are created together and are mutually constitutive. (Tenhunen 2008, 529) Technologies, therefore, are just an extension of societal norms and divide people into haves and have-nots as any other factor in society. Technology itself can therefore not be a cause of insecurity, but only a tool facilitating it.

1.6.1 Kenya's National Security and How Social Media Makes It Worse

Insecurity whether from within and without, combined with concerns over terrorist movements across Kenya's porous border with Somalia and along its coastline, and piracy off the coast have led Kenya to take an increasingly active role in regional security. Threats from within such as emergence of criminal gangs, Poaching, banditry, cattle rustling, and high urban crime, as well as periodic outbreaks of communal violence, place competing domestic demands on Kenya's national security resources. Kenya has repeatedly been a target of international terrorist attacks, and the concentration of potential international and domestic targets in Nairobi remains a serious concern for Kenyan security systems. The September 2013 siege at the Westgate Mall in

Nairobi, a popular shopping destination for tourists, expatriates, and the Kenyan elite, is the most recent successful high profile terrorist attack in the country since the Al Qaeda attacks in 1998 Nairobi Bomb blast and kikambala in Mombasa in 2002. Since then to date there have been numerous small-scale attacks on civilian and state targets in recent years, many of which are attributed to Al Shabaab or its sympathizers. Following such, Kenya invoked its constitutional right and invaded Somalia in 2011 and since then has increased military operations in Somalia to date.

Another concern follows the terrorist incidences posed by militants groups such as Alshaabab. Kenya is now home to over half a million Somali refugees, many of whom live in crowded Dadaab, Africa's largest refugee complex. The influxes of refugees come along with militant groups and illegal arms reaching other parts of the country. Somali migrants have concentrated in the Nairobi suburb of Eastleigh and other parts of the country. Kenya also has a significant population of ethnic Somalis who were born in Kenya, some whose families have been in Kenya for generations. Al Shabaab has drawn recruits from ethnic Somalis and other Muslim communities in Kenya. Many Kenyan Muslims distrust the government and view its counterterrorism efforts as discriminatory. The government faced opposition for years in its efforts to pass anti-terrorism legislation, due to concerns over civil liberties; a law was finally passed in October 2012[23]. The rendition to Uganda by Kenyan security services of Kenyan citizens suspected in the Kampala bombings has been challenged in the courts, as many were reportedly carried out without due process. Security officials have experienced wide range of challenges in dealing with the complexity and nature of terrorist activities in Kenya. Such rising insecurity, coupled with a series of kidnappings along the Kenya-Somali border, led in the

[23] The Guardian (UK), (2012). Kenyan Muslims Fear the Worst Over Proposals to Boost Police Powers.

Kenyan military incursion into Somalia. However, with an increased security attention countrywide presence of real security threats are still very ripe, by the availability of improvised explosive devices (IEDs), hand grenades and other small arms. Some human rights groups allege that Kenyan security forces have committed abuses against Somali Kenyans and refugees as part of indiscriminate reprisals for suspected Al Shabaab attacks in Kenya[24]. Reports suggest Somalis, particularly in Eastleigh, are increasingly subject to security scrutiny viewed as discriminatory and amounting to harassment. However, the militants has gone ahead to recruit not only Somalis of Kenyan origin, but other tribes especially young job seeking population, and involvement with local criminal groups such as MRC. Kenyan police, military, and civilians have been increasingly targeted in multiple grenade and IED attacks since the time terrorism acts began in kenya. In the wake of increasing terrorism incidents, technology (social media and other forms) has a role in facilitation of terrorist's social and political discourse.

Social media as a tool used by terrorist groups makes this insecurity scenario worse and more complex in nature and operations. Scholars argue that social media has become a tool for political and social movements to facilitate their operations. Like in Kenya, Al-Shabaab started using social media to recruit youths, communicate and even train them. It started to take advantage of Social Media to communicate with cyber-crime organizations and to coordinate along with them fund-raising activities to help raise money to pay its members and organize attacks on the Kenyan soil. To date the terrorist groups which make the most substantial use of

[24] Human Rights Watch, (2012). Criminal Reprisals: Kenyan Police and Military Abuses against Ethnic Somalis.

Social Media for their own purposes are the Islamic-jihadist[25] who have their operations in the country. For example, Alshabaab use HSM press twitter handle for communication and news.

Similarly, Facebook and YouTube channels are often used by al-Qaeda with the aim of recruiting and increasing the number of sympathizers and jihad-supporters. Social Media are used by Islamist groups for propaganda activities aimed at making Kenyans feel that they have successful terrorist attacks, and, consequently, at throwing Kenyans into a panic. Since spreading news and content on Social Media can be considered "viral", this kind of propaganda is able to considerably overdraw the media effect already produced by traditional means of information and communication and cause consequences even more dangerous than those caused by the terrorist attacks themselves in the country.

Since Al-Shabaab has a "net-like" decentralized structure, Facebook and Twitter is used effectively as platforms to organize and connect the single groups or cells linked to Al-Shabaab, and the leadership. Such social networks advances through connections provided by frameworks of social media technologies. More specifically, Social Media are used to communicate coded messages, to arrange plans for terrorist acts, to manage the training of new terrorists, and provide logistical support and operative assistance like giving advice about how to go through a roadblock, build themselves and handle arms and explosives, find and use cyber weapons, dodge and counter investigation by security agencies. This gives a challenge to Kenya security force when investigating and trying to gate the terrorists coming into the country or even the ones already in the country.

[25] Blitzblau S., (2011), Analisi tecnica delle capacità di NetINT dei gruppi terroristici, Information Warfare Conference 2010, Franco Angeli, Milano.

1.6.2 Social Media and National Security

One of the main area that has threaten national security is occurrences of disasters and that requires quick responses by the military and disaster teams to save on lives. For example, from the Haiti's earthquake to the Japan's tsunami, from the Katrina hurricane to the Californian wildfires, from the Virginia Tech shootings to the Norwegian island massacre, from the upheavals in the Middle East to the English riots, peer-to-peer communications, through mobile phones and social media, text and instant messaging applications, blogs, wikis and web fora, become the designated ways for citizens to be involved and active in society, in crisis events.[26]

Citizens' engagement, strongly enabled by social media and mobile technology, is supporting the dissemination of information, often critical and accurate, into the public sphere, providing eye-witness accounts, sending alert messages, exchanging evacuation and rescue experiences, searching and publishing event-related information, volunteering goods and services, collecting donations. More than mere information distribution tools, these technologies connect people and information, establish collaboration mechanisms, create informal networks and build no-boundary communities. With a strong emphasis on real-time, new mobile and online technologies have significantly improved the affected citizens' and the victims' capability to help each other and themselves, with their messages enabling improved situational awareness amongst Public Protection and Disaster Relief (PPDR) , guaranteed by the gathering of a wide variety of data and information, an activity coined as crisis informatics.[27]

[26] Moon, Kate. Physician's assistant student involved in the Haiti relief effort with an independent medical volunteer group. Personal interview. April 6, 2010.

[27] Hodge, Nathan. "U.S. Diverts Spy Drone from Afghanistan to Haiti." Wired Magazine Online. January 15, 2010.

Indeed, several initiatives, mostly private, leverage the real tributes of citizenship and volunteering towards crisis response efforts, whether on web-based crisis management systems, mobile applications for emergencies, location awareness technology in crises, Rich Site Summary (RSS) feeds, social networking platforms or web citizenship on security. Web-based systems for crisis, such as Ushahidi and Sahana, contribute to the permanent monitoring of the evolution of crisis events, enabling crowd mapping functions, reports tracking on maps and calendar, alert services and the interaction with multiple sources of information (text messages, email, tweets, web forms).[28]

Also in this field, Google's Crisis Response is a free portal service applied in past crises Like Chile, Haiti and Japan to enable donations, alerts and infrastructure status reports, as well as satellite imagery and the Google Person Finder, whereas Open Street Map provides free worldwide geographical data created by a community of volunteers.[29]According to Forrest,[30]web-based systems started off as project-oriented initiatives and since evolved to accommodate the requirements of several other crises. Other projects remain confined to the specifics of determined events, namely the KatrinaHelp Wiki dedicated to the Katrina hurricane or DigiCel's Mission 4636, launched as a free phone number to meet the urgent needs of the Haitian people to provide medical care, food, water, security and shelter through SMS messaging.[31] Even the U.S Department of Homeland Security (DHS) launched the Haiti Social Media Disaster Monitoring Initiative to assist the Haiti response and recovery effort, creating a

[28]Catone, Josh. "Developers Band Together to Create Apps for Haiti." Mashable. January, 2010.
[29] Ibid
[30] Forrest, Brady. "Technology Saves Lives In Haiti." Forbes. February 1, 2010. Accessed Febrary 4, 2010.
[31] Ibid

situational awareness vehicle able to monitor the publicly available online forums, blogs, and websites and message boards to collect critical information.[32]

Addressing social media tools for crises, it is quite clear that the relevance of mobile applications for affected citizens to contact closed ones and authorities, to send and receive text messages or to access platforms like Ushahidi or Google to know and provide critical up-to-date information.[33] Today, mobile technology supports advanced functions for improved user experience, a benefit exploited by applications published by Federal Emergency Management Agency (FEMA), the North Dakota State University (NDSU), Ushahidi and the Pacific Disaster Centre, providing citizens useful crisis-related information and upholding built-in bi-directional communication.[34] A notable initiative recently undertook by the North Yorkshire Police Authority (NYPA) resulted in the first police mobile app to be launched in the UK, now shortlisted for the Good Communication Awards 2011. The NYPA application offers numerous functions, including news, contact numbers, alerts and online maps and it is well integrated with Facebook, Twitter and YouTube platforms, accessible by different smartphones and tablets.[35]

As Guadin[36] explains, mobile application Gaia Global Positioning System (GPS) has a special version dedicated to the Disaster Relief, interfacing with Open Street Map to retrieve map and satellite information and associated geo-localized data, to provide lat-long coordinates location and guidance to waypoints and along tracks. Indeed, location awareness services are valuable for crisis response efforts, namely search and rescue actions, particularly in what concerns automated location-based services for directed messaging and alerts generation. In this context,

[32] Ibid
[33] Google Crisis Response. National Security and Crisis Response Map. Accessed on 2014.
[34] Albert L. First Informers in the Disaster Zone: The Lessons of Katrina. Washington: The Aspen Institute, 2006.
[35] Guadin, Sharon. "Facebook creates site dedicated to providing crisis info." Computer World. January 15, 2010.
[36] Ibid

governmental approach has been careful and even conservative, considering not only the legal framework involved but also the pertaining ethical considerations.[37] Nonetheless, mobile phones can be located using the equipment's own capabilities like GPS receiver and/or existing communications infrastructure like cellular and WiFi, a functionality widely accessible through the Google Latitude service, by which citizens share their location and visualize it over a map. This application ensures that communication is done in improving the security of a nation while fighting disasters that come as a result of terrorism attacks.

Lindgren and Bandhold[38] stated that Apple followed the example and is now offering the Find My Friends' service allowing users to share their location and the Find my iPad service for users to locate their Apple devices like iPad, iPhone and MacBook something which ensures there is security in a nation since the find my friends application can locate where an individual is in case of a crisis. Additional commercial solutions exist to locate mobile devices in cooperative and non-cooperative modes and to provide automatic alerts especially when a phone enters or exits a zone, when a phone is nearby and when a phone is turned on by means of Short Message Service (SMS) or email.

The cooperative mode enables users to provide their location as explicit content and 'opt-out' at any time, whereas the non-cooperative mode uses the phone's beacons for real-time location, a method that requires legal authorization and data from telecommunication operators, thus being primarily used for law enforcement and security purposes.[39] These features' benefits in crisis response actions are relevant for their life saving potential, provided suitable legislation and

[37] Ibid
[38] Lindgren and Bandhold, Scenario Planning: The Link between Future and Strategy, 164–165.
[39] Peter Schwartz, The Art of the Long View: Planning for the Future in an Uncertain World (New York: Currency Doubleday, 1991), 36.

ethical principles are safeguarded. Initially created to connect those with common relationships or interests, these sites have become ambiguous reference and, as a result, also present in times of crises. During the 2011 Japanese Earthquake, YouTube had extensive video footage of the Haitian and Japanese crises. Notably, these social media platforms successfully attained mobile reach, enabling users to easily post text, messages or videos.[40]

Moreover, citizens prove to be highly promiscuous in launching and contributing to innovative security-related initiatives, such as the portals and websites created by volunteers in the aftermath of major crises to coordinate assistance and help rebuilding efforts, or the 2007 Virginia Tech shooting Wikipedia page composed by 1500 individuals, the wide collection of tweets posted by citizens to assist firefighters and citizens during the 2007 Californian wildfires.[41] However, the presented ICT tools, platforms and services require communications to be accessible to those located within affected areas. And after large crises, it is often the case that communications infrastructures are damaged or destroyed.

These incidents indicate that social media may have a beneficial role in military relief operations. Pillay, van Niekerk, and Maharaj (2010) suggest that military units participating in such activities should incorporate social media platforms into their communication procedures to improve their ability to communicate, coordinate, and share information with other national military and civilian relief workers[42]. However, they suggest that it may be difficult to keep military movements secret due to mobile devices with integrated digital cameras and social media applications. Anyone with such a device could take a photo and upload it onto the social

[40] Ibid

[41] Cragg, Jennifer. "U.S. Military's Medical Role in Haiti Declines." American Forces Press Service. US Department of Defense. Emerging Media, Defense Media Activity. March 5, 2010.

[42] Pillay, K., van Niekerk, B., & Maharaj, M. (2010, October 11). Web 2.0 and its implications for the military.

media platform, possibly with geo-location information. Once the photos have been uploaded and the movement becomes common knowledge, others may keep watch and take photos. This could provide intelligence just as satellite photos do. Mobile phone cameras may be able to capture unit insignia, and with geo-location data and multiple uploads, the movements of these units could be traced. Although the military may attempt to control the postings of soldiers, it is more difficult to control what is uploaded by outsiders. A denial-of-service attack against popular social media websites could slow the propagation of such images. However, this would require a coordinated network warfare attack with the physical movement of forces.

Research into how social media can impact national security started with studies of propaganda. Propaganda is the management of collective attitudes by the manipulation of significant symbols.[43] There is an abundance of literature about how public opinion was systematically changed from the French revolution to current events. Of late, the most influential of these works have perhaps been the studies of the Balkan wars and the infamous the Radio Libre des Mille Collines prior to the Rwandan genocide in 1994. These studies have focused on the ways in which propaganda can be used to construct the other and incite for violence in ethno political conflicts.[44] Hermon and Chomsky[45] have advocated the propaganda model. The model argues that media function as central mechanisms of propaganda in the capitalist democracies, which perpetrates the power relations of the status quo and undemocratic forces. According to

[43]Lasswell, Harold D. (1927). The Theory of Political Propaganda' The American Political Science Review, 21:3, pp. 627-631.

[44]Hallin L., (2004) analyzed the media coverage of the conflict and concluded that initially the media was very supportive and only changed its stance on the Vietnam War after the public opinion had turned sour.

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

Klaehn[46]Propaganda is, nevertheless, moving to the background as a topic research, perhaps due to the intensification of the 24-hour news cycle.

The Vietnam War (1955-1975) coincided with the oppositional youth movements and virtually every home acquiring a television set. As a result every American was faced with the tragedy in their living rooms. The socio-structural changes of that time also meant the emergence of a new generation that opposed their parents' values as well as the war. When the United States lost the war, the blame was partially put on social media, whose negative reporting of the war was seen as part of the cause for the retreat from Vietnam.[47] The thought of social media impacting political decision-making through popular opinion was later dubbed the Cable News Network (CNN) effect. As observed by Gilboa[48], the concept was initially suggested by politicians and officials haunted by the Vietnam media myth, the confusion of the post–Cold War era, and the communications revolution. Despite evidence to the contrary, many leaders still believe that critical television coverage caused the American defeat in Vietnam.[49]

The initial studies into the CNN effect saw the implications as quite linear. There was also much difficulty in defining this new concept in a useful universal way.Wolsfeld[50]has observed that the simpler notions about the CNN effect are most likely misguided. Livingston[51] managed to identify three different aspects to the CNN effect, it is an accelerant to decision making, an impediment to the achievement of desired policy goals, and a policy agenda-setting agent.

[46]Klaehn, Jeffrey (2002) ‗A critical Review and Assessment of Herman and Chomsky's Propaganda Model,' European Journal of Communication, 17, pp.147-174.
[47] Roach C., (1993). Information and Culture in War and Peace: Overview, Communication and culture in warand peace, edited by Colleen Roach, SAGE Publications, California.
[48]Gilboa E., (2009) ‗Media and Conflict Resolution: A Framework for Analysis, Marquette Law Review: 93(87).
[49] Ibid
[50]Wolfsfeld G., (2004). Media and the path to peace, Cambridge, Cambridge University Press.
[51]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.

Policymakers have no choice but to redirect their attention to the crisis at hand or risk unpopularity, whether or not such revision is merited by policy consideration.[52]

Social media platforms are also believed to have helped extend the reach of hate groups more broadly. Christopher Wolf [53]has observed that, the online world 'has become a technology embraced by racists, anti-Semites, homophobes and bigots of all kinds to spread their message of hate'. Holocaust deniers, the Identity Church, KKK Members, neo-Nazis and racist skinhead groups are all believed to be particularly active. Anders Breivik,[54] for example, drew much inspiration and impetus from his interactions online, including from the new 'counter-Jihad movement' – an international collection of Islam bloggers, which, according to Hope not Hate, comprise over 200 organizations worldwide.

No research was found that comprehensively measures the amount of hate speech that occurs online. The Simon Wiesenthal Centre's annual Digital Terror and Hate Report from 2012 was based on 15,000 'problematic' websites, social networks, forums, online games and apps. They believe this has seen an increase of around 3,500 problematic outlets since 2010. Similarly, the International Network Against Cyber hate, 2013 has argued that over recent years 'the amount of cyber hate has grown to enormous proportions', with 'Islam, Jews, lesbians and gays, blacks, Roma, liberals' and 'left-wingers' representing the main targets of online abuse. It is of note that of all the referrals made by the UK's counter-terrorism internet Referral Unit (which seeks material that glorifies terrorism and asks for its removal from internet service providers), Facebook, Twitter, Blogger and/or Blogspot were most frequently identified as the hosts of the

[52] Neumann J., (1996) Lights, camera, and war: is media technology driving international politics? New York: St. Martin's Press.

[53]Weng, J., Christopher Wolf J (2010) 'TwitterRank: Finding Topic Sensitive Influential Twitterers'*WSDM 10,* February 2010

[54] Lynda Peters (2012) *Utilising Social Media to Further the Nationwide Suspicious Activity Reporting Initiative*, Masters Degree Disseration, Calhoun University

problematic, referred material. Another study, found that false rumours are questioned more on Twitter by other users than true reportage[55].Using topically agnostic features from the tweet stream itself has shown an accuracy of about 85 per cent on the detection of newsworthy events.[56] The study under the subject, "Twitter under crisis", asked whether it was possible to determine 'confirmed truth' tweets from 'false rumour' tweets in the immediate aftermath of the Chilean earthquake. The research found that Twitter did tend toward weeding out falsehoods: 95 per cent of 'confirmed truth' tweets, were 'affirmed' by users, while only 0.3 per cent were 'denied'. By contrast, around 50 per cent of false rumour tweets were 'denied' by users. Nevertheless, the research may have suffered a number of flaws. It is known, for example, that the mainstream media still drives traffic and that tweets including Uniform Resource Locator (URL) links tend to be most re-tweeted, suggesting that many users may have simply been following mainstream media sources. Moreover, in emergency response, there tends to be more URL shares (approximately 40 per cent compared to an average of 25 per cent) and fewer 'conversation threads'.[57] In late 2007 and early 2008 most Kenyans didn't have access to the Internet. Not even through cell phones as today. Those who were online experienced a wave of heightened activity. Many experienced the down side of uncontrolled communication, but others were able to even save lives though their blog posts. There was a strong intertextuality within these communications and SMS messages have therefore been included in this section. However, According to a report released in May 2013 by Umati, an online monitoring firm that documented some of the hate messages circulated; there was a dramatic rise in online offensive

[55] Mendoza, M., Poblete, B., Castillo, C , Twitter Under Crisis: Can we Trust What we RT?, KDD Workshop on Social Media Analytics, 2010

[56] Castillo, C., Mendoza, M., & Poblete, B. (2011). Information credibility on twitter. Proceedings of the 20th international conference on World wide web - WWW '11, 675. doi:10.1145/1963405.1963500

[57] A Hughes "Twitter adoption and use in mass convergence and emergency events" IGCRAM, 2009

speeches circulated mainly through Facebook between the month of March 2013 (the election month) and February 2013, the month prior to the elections. In February 2013 there were 197 extremely inflammatory speeches which rose to 321 in March and general offensive messages rose from 122 in February to 405 in March (Umati Report, 2013)[58]. During these political events, [59]Makinen and Kuira[60] argue that social media functioned as an alternative medium for citizen communication or participatory journalism but it was also used as channels for biased information, tribal prejudices, and hate speech. Digitally networked technologies were a catalyst to both predatory behavior such as ethnic-based mob violence and to civic behavior such as citizen journalism and human rights campaigns' during the post-election crisis. According to wa-Mungai,[61] there was a strong intertextuality between sources of information. Mass e-mails were shortened to fit SMS, tweets mixed with rumor. Like SMS, cyberspace-based discussions were also fed on rumor and misinformation from the press. Due to the rampant spread of SMS messages, the government decided despite a weak legal standing on the issue, to send a warning that it advises that the sending of hate messages inciting violence is an offence that could result in prosecution.[62]Many of the citizens were wary in fear of government action.

1.6.3 Social Media Users and Social Networking

Social Media users are single individuals who use media tools to communicate, share information and content, interact with other people, develop their personality and strengthen their

[58] Umati (2013): Umati: Monitoring Online Dangerous Speech. Nairobi, Kenya.
[59]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.
[60]Mäkinen M. and KuiraW., (2008). Social Media and Postelection Crisis in Kenya,' Press/Politics, 13(3).
[61]Wa-Mungai, M., (2010). Soft Power, Popular Culture and the 2007 Elections,' in KarutiKanyinga and Duncan Okello (eds.), Tensions and Revisals in Democratic Transitions: The Kenya 2007 General Elections, Nairobi: Society for International Development.
[62] Ibid

social identity.[63]Zinzocchi states that single individuals are able to satisfy all their basic needs (except for physiological needs such as drinking, eating or sleeping) using Social Media. The basic needs include security needs, membership needs, appreciation/esteem needs, and self-fulfillment needs. Individuals can use Social Media not only for strictly personal purposes, but also for the interests and/or purposes of the organized group they are part of.[64] Hence, although the use of Social Media is necessarily linked to the interaction between a person and the information medium, organized groups in the broadest meaning of the term; states; public agencies; companies; movements; and terrorist groups are potential Social Media users, too.[65] In this case, the single members in terms of affiliation or association of these organized bodies are to manage the institutional accounts and become the factual users of Social Media on behalf of the entire group, pursuing the purposes and protecting the interests of the group itself.

In Kenya and Eastern Africa region, there is a void in terms of literature on the subject matter of this study. This is more the reason why this study is important. The findings and recommendations of this study shall, arguably, initiate more debate and research on information, social media cyber security, information warfare and national security in Kenya.

During the past decade, individuals have extensively used social media to interact with others and to pursue personal interests. Social media enable individuals to follow these interests, share their ideas, and expand their knowledge in ways that are faster and more efficient than ever before. For social interaction purposes, social media offer users a nearly limitless amount of

[63]Zinzocchi R., (2009), Da Facebook a Twitter vogliamolasciaretracce, Il Tempo. According to Maurizio Ferraris, professor of Theoretical Philosophy at Università di Torino, interviewed by the author of the article, for many people Social Media create a personality as if a rich digital identity, connected with endless other digital identities was the condition for a complete real identity.
[64]Montagnese A (2012): Impact of social media on National Security, Published MA Thesis. University of Rome. P 2
[65] Ibid

possibilities on the Internet.[66] Persons may share, collaborate, follow, and correspond to their hearts' content, restricted only by their privacy preferences or security concerns. In this way, social media are slightly more useful for individuals over organizations, businesses, or governments which are subject to multiple preferences and often stricter security concerns.[67] Though they integrate seamlessly with businesses and organizations, social media offer the greatest number of possibilities to individual users. Social media and the Web 2.0 revolution provide a greatly enhanced Internet experience to individuals by enabling them to contribute to content, harnessing collective intelligence and user-added value. By "crowdsourcing" the perceptions and opinions of millions of web users, websites improve their abilities to provide useful content.[68]

1.6.4 Social Media Growth and Characteristics

The term social media or "new" media refers to the group of technologies associated with rapid information dissemination via highly accessible web-based platforms. Social media represents a fundamental transformation of broadcast media monologues into multiple community dialogues, mirroring the Web 2.0 revolution of the Internet. "Web 2.0" refers to the fundamental shift that swept across the Internet at the dawn of the 21st century, transforming the information producer-consumer model into a network in which every user has the ability to produce and consume

[66] Howe, Jeff. Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business. New York: Crown Business, 2008.
[67] Surowiecki, James. The Wisdom of Crowds. New York: Doubleday, 2004.
[68] Rosenberg, Scott. Say Everything: How Blogging Began, What It's Becoming, and Why It Matters. New York: Crown Publishers, 2009.

Internet content. Through these terms, O'Reilly[69] has probably the most successful work in explaining the Web 2.0 revolution and the rise of social media.

Important examples of Web 2.0 social media include blogs (individuals or groups producing ongoing narratives of information), wikis (collaborative information productions and collections), Facebook and MySpace (streamlined social networking programs), eBay reputation (performance-based user reviews), Flickr (highly accessible photo sharing software), YouTube (community-based video sharing software), Google Maps (mapping software enabling collaborative point of interest sharing), Amazon user reviews (comprehensive user contribution to product reviews), and Twitter.[70] For a technological application to be considered a "2.0" technology is not for it to be the second version of something, or the twentieth version of something; instead, it means that the technology is characterized by data sharing and collaborative information collection and organization.

Social Media began at the beginning of the 21st century in the United States (US) and, since that date they have been growing and spreading exponentially, especially in the last two years. It took a relatively short time for Social Media to change from "an interesting emerging communications trend to a critical part of the media landscape".[71] According to some 2010 estimates, all Social Media users add up to over two billion people worldwide.

In their early stage (2000-2005), Social Media started to spread chiefly in the more developed countries, with a high technological power in terms of broadband speed, number of per capita computers, and whose governments guarantees complete freedom of expression and

[69] O'Reilly, Tim. "What Is Web 2.0." O'Reilly Media. September 30, 2005. Accessed March 2, 2010. http://oreilly.com/web2/archive/what-is-web-20.html

[70] Safko, Lon, and Brake, David. The Social Media Bible: Tactics, Tools, and Strategies for Business Success. Hoboken, NJ: John Wiley & Sons, 2009.

[71] Burson-Marsteller, (2011). The Global Social Media Check-up 2011, New York.

communication. In this very stage Social Media took root especially in North America, Europe, Russia, Japan, South Korea and Australia.[72] Nevertheless, since 2005 they have started to catch on in less developed, both technologically and economically, and non-democratic countries too. Thus, new media started to spread in Northern Africa, Middle East, China, Southeast Asia, in the Persian Gulf states, in Southern and Central America.

According to Emanuela,[73] differently from other communication revolutions where the diffusion of media happened before in the developed states and only after in less developed states, Social Media is spreading everywhere contemporaneously. In fact, today some areas of the World are no more marginalized; instead they become aware of their freedom of expression, share thoughts and customs and endorse them. The only discrimination left is maybe about social classes and genre.

Social media have well known characteristics. Through the tools of social media, users can communicate with each other different kind of contents -videos, photos, images, texts and sounds among others. Also build and strengthen networks in one or more fields, professional, family, social, culture, religious and political and develop and define their social identity.[74] According to Montagnese, an expert on "intelligence and strategic deception techniques and methods of information manipulation" and a high ranking official in the Italian National Security, Social media are found to have an extremely high level of interaction among the users, differently from traditional media, which are characterized by a one way communication flow. In fact social

[72]http://www.vincos.it/world-map-of-social-networks/.
[73]Emanuela D., (2011) La Rete, strumento di partecipazione, mobilitazione e lotta, Gnosis – RivistaItaliana di intelligence, vol. 2/2011, Roma.
[74]Carafano J.C. (2009). From Social Networks to National security. Australia Policy Institute p.3

media users can be at the same time both senders and recipient of information, and creators and users of content.

While some studies identify text messaging as a form of social media, text messaging does not characterize collaborative information sharing and organization in the same manner as do the other technologies. Text messaging would likely fit better under the "new media" label than the "social media" label. As a direct extension of cell phone technology, text messaging is likely part of a broader technological revolution of which social media tools are a distinct part that likely has greater implications on the field of disaster relief.[75] As Webster[76] wrote about his time as a part of the Haiti relief effort, "In the initial weeks of Operation Unified Response, Blackberry text messages became the primary means of communication, chiefly because they were the simplest and most reliable means of corresponding with the host of U.S. Government agencies, United Nations offices, and Non-Governmental Organizations (NGOs) coordinating the relief efforts." To study the role of cell phones and satellite technology in national security is important. The findings of this study will speculate that their use/ misuse has been and will continue to be revolutionary. In any case, this study seeks to explore the potential threats and counter threats of specifically social media technologies on the field of national security, examining whether social media technologies comprise an original revolution of national security. Their capability to integrate with existing phone and text messaging services will be central to this study.

[75] Abbot, C. Spencer. Presentation: "Humanitarian Intervention in Emergencies: Principles, Practices, and Perspectives." Georgetown University Center for Peace and Security Studies. April 13, 2010.
[76] Webster, Kelly L. "Lessons From a Military Humanitarian in Port-au-Prince, Haiti." Small Wars Journal. March 28, 2010. 2.

1.6.5 Theoretical Framework

This study utilized the social responsibility theory which was first introduced in 1947 and was recommended by the Hutchins Commission on Freedom of the Press. It stated that "the media should serve the public, and in order to do so, should remain free of government interference".[77] Social responsibility theory defined guidelines that the media should follow in order to fulfill its obligation of serving the public. It claimed that the media could be self-regulating by adhering to various precepts which include: media has obligations to fulfill to a democratic society in order to preserve freedom; media should be self-regulated; media should have high standards for professionalism and objectivity, as well as truth and accuracy; media should reflect the diversity of the cultures they represent; and that the public has a right to expect professional performance.

The social responsibility does not only fall upon the reporters and producers of media. The responsibility also falls to the consumers to become media literate and maintain high, yet reasonable expectations of the media. In theory, if these things happen, there will be no need for government intervention in terms of regulating the media and its participation in spreading roamers and propaganda to the public.

Shuchman and Wilkes[78] have tried to explain what it means by the press to be socially responsible and in the interest of improving the media's service towards the society. In their analysis about the effectiveness of communication between medical scientists and health news reporters, they found that in journalism, failures to be accurate, to identify vested interests to follow up on stories and to cover important health issues are the negative consequences of social

[77] 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.
[78] Shuchman M,. Wilkes M. S. (1997). *Medical Scientists and Health News Reporting: A Case of Miscommunication.* Volume 126 Issue 12, Pages 976-982.

media. The basis of self-regulation in journalism lies in the existence of ethics codes, whose actual impact on ethical standards in media organizations is largely questionable, given that a certain portion of journalists are not fully aware of their content, and there is no formal structure to ethics code violations.[79] These types of preventive procedures constitute a first step in controlling the extent to which media is carrying out its responsibility toward the public. However, the debate on regulation and whether it is appropriate that laws be applied as a means to enforce social responsibility in the media remains controversial.

1.7 Research Methodology

This study largely depends on both qualitative and quantitative research methods. Main sources of data will be primary and secondary. It covers the research design, target population, sample size, data collection, and data analysis.

Research Design

Given the research objectives and questions, this study shall use the survey research method. The survey method 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.[80] The survey method is perceived as authoritative by people in general and is both comparatively easy to explain and to understand. It is suitable for descriptive and exploratory research as is this study. In addition the data collected using a survey strategy can be used to suggest possible reasons and to provide conceptual models of these relationships.

[79] Middleton, M., (2008). The RCTV Cliffhanger: Flagging social responsibility in the media, Visages d'Amériquelatine, Sciences.

[80] Saunders, M, Lewis P &Thornhill, A (2009) Research Methods for Business students. FT Prentice HQ, India p 66

Population

For purposes of gathering primary data, the target population will target military officers based in Nairobi, and more particular in specialized units of operation. The composition of the population will consists of all ages from 20 years and above, with diverse qualifications, gender, career mix and exposure.

Sample Design Size

Sampling design of the study will be proportional, stratified sampling method. Saunders[81] has argued that sample size is almost always a matter of judgment rather than calculation. In view of this contention and the fact that any sample size above 30 is considered a large sample, the researcher will regard a sample size of 50 members of the military from Nairobi based units of the appropriate stratification as adequate for the objective of this study.

Data Collection

Questionnaires and interviews will be the main methods that will be used to collect data. The questionnaires will be given and picked from the users of social media to ensure a higher percentage of responses. Interviews will be extensively used in conjunction with the observation method in as much as interviews sometimes elicit inaccurate data as respondents are unwilling to divulge information on sensitive issues of security for fear of being quoted or misquoted, and fears of having no authority to comment on such issues.

[81] Ibid

1.8 Scope and limitations of the study

The study will provide an up-to-date picture of the situation concerning the use of Social Media by states, movements, terrorist groups, criminal organizations, and individuals and how it threatens national security. Time frame or time taken to complete the research will be a limitation in that with a very demanding career, the research will be affected for a while due to travel during data collection and conducting interviews. Due to the sensitivity in discussing security information, busy schedule of the military officers, they might not give their full concentration to answer to the researchers request or give little time thus limiting the study.

1.9 Chapter Outline

Chapter two will discuss the threats of social media to national security.

Chapter three will discuss the use of social media by the military in removing or reducing threats to national security.

Chapter four will give a comparative analysis of the impact of social media on national security.

Chapter five will provide the summary of the study, conclusions and recommendations.

CHAPTER TWO

THREATS OF SOCIAL MEDIA TO NATIONAL SECURITY

2.1 Introduction

Recent world events have shown that social media, just like traditional media, can act as a tool that threatens national security. Social media can act as a tool for widening democratic space, but on the other it can lead to destabilization. The media can be used to spread propaganda and hate speech and incite to violence and others. Any debate about the role of the social media must therefore be grounded on the larger debate between information flows and stability of state. Social media has well-known security risks to nations.[82] These risks of social media are what are termed as threats of social media to national security. In this section, the threats of social media to national security are presented.

2.2 Threats of Social Media and National Security

Threats of social media can manifest themselves in many ways. Social Media are more and more used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training.[83] In addition to this, terrorist groups take advantage of Social Media to communicate with cyber-crime groups and to coordinate along with them fund-raising activities carried out in part or completely on the Internet. The link between organized crime and

[82]Wanner, G. (2011). Risks of social media to organizations: Oaks publishers UK. P 64

[83] UN Counter-Terrorism Implementation Task Force, (2011), *Use of the Internet to Counter the Appeal of Extremist Violence, Conference Summary*, Riyadh.

terrorist organizations is increasing considerably in the cyber-world, and this coalition will be able to produce new offensive technologies.[84]

To date the terrorist groups which make the most substantial use of Social Media for their own purposes are the Islamic-jihadist ones. Facebook and YouTube channels are often used by al-Qaeda with the aim of recruiting and increasing the number of sympathizers and jihad-supporters, especially in the West for example, spreading photos and videos of successful terrorist attacks, publishing lists and biographies of the martyrs, preaching or ideological texts. Lorraine Bowman-Grieve[85] pointed out that Social Media "play an important role in influencing the behavior of the individual and their readiness to take part in collective action because of their inherent socializing, recruitment and decision shaping functions", besides, they "facilitate social interaction and the formation of social bonds, which in turn can lead to changes in attitudes and behavior over time. These changes in attitude might include adopting the most prevalent ideology expressed within the community". Social Media, and, more generally speaking, the Internet allow the publication and diffusion of extremist ideas and material that may lead a vulnerable individuals to recruit themselves, sometimes unaided by any intermediary.

Apart from being used for recruitment purposes, Social Media are also used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, at throwing civil population into a panic. Since spreading news and content on Social Media can be considered viral, this kind of propaganda can be able to considerably overdraw the media effect already produced by traditional means of information and communication and cause

[84]Blitzblau S., (2011). Analisitecnicadellecapacità di NetINTdeigruppiterroristici, Information Warfare Conference 2010, Franco Angeli, Milano.

[85] Bowman-Grieve L., (2010). A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment, Euro ISI Conference Submission, Leeds.

consequences even more dangerous than those caused by the terrorist attacks themselves like circulating the news of an attack to communication and connection infrastructures used by the stock market might throw investors into a panic, and, consequently, lead small money-savers to behave irrationally; in so doing, it could cause even more severe economic damage than the damage itself to the very material infrastructure.

The US Congressional Research Service conjectured that some organized groups, mainly terrorist groups, could use Social Media with the aim of knowingly spreading false information in part or in full during a disastrous event like an earthquake, a flood, the accidental blast of a nuclear reactor, a pandemic, or immediately after it ends, in order to overdraw their damaging effects, mystifying the people and delaying emergency operations and the response of a country.[86] According to a report by the US Army[87], Social Media can also be used as a vehicle for malwares so as to cause damage to computers or other mobile terminals like smart phones and tablets. Social Media tools such Twitter and Facebook can be used by terrorist groups to expand networks and not only to spread propaganda, but can also host embedded malicious software in links and applications that can corrupt an unsuspecting user's electronic device.[88]

Jones[89] argues that al-Qaeda developed a well-framed strategy committed to using Social media in order to achieve their own goals. According to Jones, Anwar al-Awlaki was one of the major promoters of such strategy. al-Awlaki took cleverly advantage of Social Media potentialities and worked actively on most of social networking sites, and used them to spread a huge amount of propaganda material especially addressed to members scattered all over the world in order to

[86] Ibid
[87] US ARMY, 304th Military Intelligence Battalion, (2008), Sample Overview: al Qaida-Like Mobile Discussions & Potential Creative Uses, Fort Huachuca, Arizona.
[88] Ibid
[89] JONES S. G., (2011), Awlaki's Death Hits al-Qaeda's Social Media Strategy, RAND Corporation, Santa Monica, CA.

push them into committing terrorist acts. Since al-Qaeda has a net-like decentralized structure, Facebook and Twitter can be effectively used as platforms to organize and connect the single groups linked to al-Qaeda, and also the "lone wolves" and the leadership. Furthermore, Social Media are used to communicate coded messages, to arrange plans for terrorist acts, to manage the training of new terrorists, and provide logistical support and operative assistance which involve giving advice about how to go through a roadblock, build themselves and handle arms and explosives, find and use cyber weapons, dodge and counter investigation by security agencies.[90] To demonstrate the power of social media and online magazines, following is rather long quotation titled "Al-Shabab attempts to terrorize Kenyans with online magazine". Written by a Kenyan journalist, Bosire Boniface. "Al-Shabaab is using its new online magazine to instill fear among Kenyans and motivate its demoralized fighters after suffering a string of defeats and defections, Kenyan security officials and analysts say. The first edition of Al-Shabaab's online magazine mocks the Kenya Defence Forces' Operation Linda Nchi (Protect the Country) with its title, Operation Protect Islam. The second edition of Al-Shabaab's online magazine *GaidiMtaani* focuses on Kismayo, the militant group's last remaining major stronghold in Somalia. *GaidiMtaani*, or "Terrorist on the Street" in Swahili, was introduced in April and has published two issues in Swahili and English. The magazine's editorial says it drew inspiration from Inspire, an English-language online magazine published by al-Qaeda in the Arabian Peninsula." This illustrates that Social Media are more used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training.

In conducting criminal activities, criminal organizations use Social Media as support, communication and coordination tools to conduct their illicit activities. This kind of illicit

[90] Rollins J., (2011), Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy, Congressional Research Service, Washington, DC.

activities can be either purely information ones like spreading child pornography with fee, virtual identity thefts, phishing, spread of viruses, and worms or traditional ones like drug smuggling, human trafficking, money-laundering and transfer of documents from industrial espionage.[91] Criminal groups which use Social Media are made of people coming from the same geographic area and who know each other personally, but also of people scattered all over the world who are linked exclusively by "virtual" relations. These criminal communities are generally coordinated by one or more moderators who have the power to remove the members who do not provide high-quality information or tools and to assign an increasing level of reliability to those who make more contribution than others.[92] The use of Social Media and, in general, of IT technology for criminal purposes is dramatically expanding, not only because they are spreading increasingly, but also because the individuals perceive the actions they commit as less serious if compared to what happened in the past. The same happens for the extent of the damage caused by their behavior, and the risk of being found.[93]

Social media is also used during the time of war to spread and increase the magnitude of war according to the nature of organized war group like state, company, terrorist group, criminal organization and cracker group. This happens through Information war (IW) activities which are derived from cyber war and cyber terrorism for counter-cyber terrorism. During cyber war, conflict among nations, fought systematically pulling down an adversary's critic protection barriers of security, that is disturbing or "switching off" strategic communication networks, and complementing these activities with merely war operations. Cyber terrorism for counter-cyber

[91] Intelligence And National Security Alliance, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA.

[92] Campobasso P., (2011), Le nuovesfideallasicurezzadellospaziocibernetico, Information Warfare Conference 2010, Franco Angeli, Milano.

[93] Ramacciotti S., (2011), La sicurezzadelleinformazioni al tempo di Wikileaks, InformazionidellaDifesa – SMD, n. 3/2011, Roma.

terrorism is referred to as the use of the net by Terrorist organizations for propaganda, detraction, or affiliation purposes or to put out of order critical transmission points of structures or processes related to national security.[94]

During the second Israeli-Lebanese war in 2006, Mayfield carried out several Information Warfare activities through the use of Social Media. In all the conflicts, they used Social Media to publicize several videos and photos on blogs, social networking sites and YouTube so as to foster their own image and decry Israel's one and their security services. Further to this activity, Mayfield managed to instil a perception of failure in the Israeli political-military establishment which conditioned the course of the conflict. During the following war (2008-2009), instead, Israel showed a much effective management of Social Media, employing them in information and counter-information campaigns.

Further on that, cases of non-authorized and uncontrolled publication of classified or sensitive information or content (print, audio, photo etc) through Social Media are more and more frequent. In these cases national security can be severely compromised by the use of Social Media. Examples include the famous leaks of Wiki leaks of US Cable Communications. Other cases include Four Indian senior naval officers who were court-marshaled after they were reportedly found divulging information about the location of warships and other confidential data on social networking websites, which was even being accessed by foreign nationals. The four officers were being tracked for quite some time by naval authorities for allegedly leaking

[94]Stoler. P. 1986, The War Against the Press: Politics, Pressure and Intimidation in the 80‟s. (New York: Dodd, Mead & Cog 99

confidential information, including location for warships, armaments being carried by them and their patrolling patterns.[95]

New technologies and in particular Social Media constitute an asset of great importance both for social movements/groups and for revolutions.[96] Rebels and revolutionary groups turn to such tools to better organize and spur masses to action, to arrange protest or struggle activities and manage their tactical and operational aspects. Since Social Media are gaining a great deal of clout in determining the conclusion of protests and revolutions, their employment is likely to increase remarkably in the immediate future. According to Papic and Noonan,[97] Social Media are tools which enable revolutionary groups to lower the costs of participation, organization, recruitment and training. The two experts studied the recent protest movements in Tunisia and Egypt, and discovered that there was a noticeable increase in the use of Social Media by revolutionary groups, especially to spur civil disobedience and manage protest and struggle actions; together with mobile phones, Social Media guarantee rapidity in spreading information and spurring masses to action, protest movements can reach hundreds of thousands of adherents with a single Facebook post or Twitter feed, launching a massive call to action in seconds; and that thanks to their being extremely cheap, Social Media allow revolutionary movements to be more autonomous and, therefore, less easily influenced by people not involved in the organization and less dependent on external financing.

[95]Moskos Charles C. "The Media and the Military in Peace and Humanitarian Operations." Special Report, Cantigny Conference Series, Robert R. McCormick Tribune Foundation, Chicago, 2000 pg 321

[96]Pedde N., (2011), La crisilibica, e le differenze con le rivolte in Tunisia edEgitto, InformazionidellaDifesa – SMD, n.2/2011, Roma.

[97]Papic M., Noonan S., (2011), Social Media as a Tool for Protest, STRATFOR, Austin, TX.

General Lombardi[98] examined the role of Social Media in the social movements and/or revolutions and affirmed that in the future such movements will not be different as for the procedure (conflicts, occupations, manifestations, civil disorders) and the purposes (improvements of social and economic conditions, change of the political system), but will surely be different for what concerns the interactions among the protesters themselves, among them and the power they want to counter, and among them and the external world. Lombardi adds that Social Media let their users "bypass" the censorship and the control the government usually makes on the media, creating an alternative channel to spread (true) news.

Del Re[99] agrees on this very observation, and talks about the role of Social Media in the course of the protests in Libya, Tunisia, Egypt and Syria, claiming that the regimes lost the absolute control on the information, gradually losing power while the population has acquired the power to handle and spread the information, in turn. The Algerian writer and journalist Lakhous[100] also points out how Social Media and the Internet make information censorship and manipulation almost impossible. Similarly, Hamam[101] studied the recent protests in Egypt and noticed that in societies where traditional public media are controlled by the government and private ones are censored by the companies they work for, Social Media represent a unique opportunity for civil population to counter the regime and enhance their freedom of speech and communication.

Social Media is also used for electronic financial fraud and hacking. It has become very common for financial institutions in Kenya and elsewhere to experience huge financial losses every year through internet technologies and these includes identity fraud through social media and other

[98] Ibid
[99] Gabriel Weimann, Terror on the Internet: The New Arena, the New Challenges (Washington, D.C., United States Institute of Peace Press, 2006), pp. 37-38.
[100] Lakhous A., (2011) La Rete, strumento di partecipazione, mobilitazione e lotta, Gnosis – RivistaItaliana di intelligence, vol. 2/2011, Roma.
[101] Ibid

technologies. In 2011, it was reported by Kenya's Central Banks Anti-fraud unit the loss of over Kshs. 1 billion by the financial sector in Kenya through this method[102]. Computer hacking is so common that in 2011 alone, the websites of about 105 big companies and government departments in Kenya websites have been hacked, including the website of Communication Commission of Kenya (CCK). This therefore is a major security threat to the nation.

Social Media has been threatening the various organizations. In 2009, the Secure Enterprise 2.0 Forum issued its annual industry report which focused on social media security threats[103]. The Enterprise 2.0 Forum consists of executives at Fortune 500 companies which have adopted social media tools and services in their businesses. The forum promotes awareness, industry standards, best practices, and interoperability issues related to the use of the new tools in the workplace. This report was intended to help institutions that were considering adopting social media tools in their businesses by providing a basis for assessing the security risks. The report described the types of threats that social media technologies could pose in a business environment. Some of the eight main threats identified in the report were information leakages and malware.[104]

Social media sites like Facebook and Twitter create the perception of familiarity and intimacy on the internet. Most of young people use the same technologies in the office and at home. The outcome is that people may be tempted to share information on the internet that their employers would have preferred to keep private.[105] Individuals may not be leaking organizations secrets

[102] Cleveland, William L., and Martin Bunton. A History of the Modern Middle East. CO: Westview Press, 2009 P. 88
[103] Moskos Charles C. "The Media and the Military in Peace and Humanitarian Operations." Special Report, Cantigny Conference Series, Robert R. McCormick Tribune Foundation, Chicago, 2000 p. 321
[104] SANS Institute (2011). Reducing the risks of social media to your organization: Online watchman
[105] Fogel, J., &Nehmad, E. Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior (2009). P. 153

but the cumulative effect of small details can enable institutional or business competitors to gain valuable intelligence about that organization's present and future secrets.

For Civil Servants, turning to Social Media enables the diffusion of confidential or job-related news whose subsequent use or possible manipulation cannot be predicted and circumscribed. Cases of non-authorized and uncontrolled publication of classified or sensitive information or content (audio, video, and photo) through Social Media are more and more frequent. In these cases national security can be severely compromised by the use of Social Media.[106] Freedom of expression and communication has to stop where the need to protect the confidentiality and integrity of sensitive data starts, that is to fulfil the general duty of confidentiality at work. Since the civil service is making more and more use of Social Media for their institutional purposes, as well as civil servants are doing for personal interests, a series of information campaigns should be launched so as to increase the level of civil servants' awareness about the Social Media risks for personal and national security.

The sociological influence of Social Media has brought risks of accessibility risks, relationally risks, risks related to professionalism, political risks and conversationally risks to the nation.[107] In relation to this, the members of national security are part of the larger society of Kenya. As part of that larger society, they are influenced by the ever expanding wave of social media as it influences the Kenyan and other global societies worldwide. These days anyone can access their online network while sitting at their favorite clubs, coffee shops or homes, allowing their leisure time, personal communication and work environment to merge together. This dramatic visibility and ability to converse with others promptly may create timely opportunities that otherwise

[106] Cleveland, William L., and Martin Bunton. A History of the Modern Middle East. CO: Westview Press, 2009 p. 88
[107] Berkman, R. I., & Shumway, C. A. (2003). Digital dilemmas: Ethical issues for online media professionals. Ames: Iowa State Press. p 5

would have existed[108]. One core disadvantage to this accessibility is that people may lose the ability to virtually unplug from an area of life without consequences.[109]

In social relationship we have two ties; one called "strong ties" and another called "weak ties". The strong ties are relations of families and people closely related. Weak ties are about relation of acquaintances[110]. It is said that our greatest sources of new ideas and information are the weak ties social media relationships offer. Many Kenyans have Twitter or Facebook "friends" or followers. "Friends" they have no intention of ever seeing or meeting them face to face, but are contributing ideas, information and support when and where needed.

Social media has also influenced our way of professionally associating with one another. Classes and seminars on social media have made businesses and institutions more aware of the impressions people have about their company, products, services and public sector institutions. Public opinion can amass itself in real-time, whether people speak responsibly or reactively[111].

Social media have ways of amplifying valid local and global news sources when people post links to content on social media websites. Our social media friends have increasingly become a trusted resource of real-time information. However, it should be noted that people who continually post strong opinions about elected officials as common in Kenya may inadvertently discourage others from reading their posts. That tells that platforms of social media have to be used strategically in the political arena or else the ability to influence others may not count when someone really need it to.

---

[108]Kirkpatrick, D (2011). The Facebook Effects. Oaks Publishers NY

[109]Moskos Charles C. "The Media and the Military in Peace and Humanitarian Operations." Special Report, Cantigny Conference Series, Robert R. McCormick Tribune Foundation, Chicago, 2000 p. 36

[110]Williams, F. (2008). Sociological impact of social media: Oxford Press, U.K.

[111] Kirkpatrick, D (2011). The Facebook Effects. Oaks Publishers NY

Finally, social media have brought major impact on how people have conversation with one another. Social media tends to create out of us "online personalities and entities"[112]. Social media offers a greater capacity to send quick messages by increasing the methods by which we can communicate. Some people may use this as an easy way out, however, having a face-to-face conversation with someone in a tense situation. Those patterns over one situation can create future problems relationally and professionally[113].

According to a recent NATO provisional study[114], future conflicts will occur in more and more connected environments, which will be characterized by the use of new communication and information technologies, Social Media included. It is a few years since Social Media have been employed by the Armed Forces in several countries, and now they are ready to be employed more and more frequently to accompany traditional offensive means. In particular, the use of Social Media during a conflict adds to the employment of other mass media like newspapers, TV, radio, and many more for propaganda, influence and deception activities. Since in the last decade the number of wars between entities with international subjectivity has been very low, and that open-source material is sparse, it is not possible to investigate cases of military campaigns conducted with an actual employment of Social Media in support of military operations.

In order to mitigate the risks for national security coming from the improper use of Social Media, a specific national policy is desirable, on whose basis all the institutions can elaborate their own guidelines for their staff, according to their area of expertise. The US government followed this

[112]Berkman, R. I., & Shumway, C. A. (2003). Digital dilemmas: Ethical issues for online media professionals. Ames: Iowa State Press.p 5
[113] Ibid p44
[114] NATO Allied Command Transformation, (2009), Multiple Futures Project – Navigating Towards 2030, Norfolk

direction, in fact in 2009 the above-mentioned Chief Information Officers Council adopted a series of guidelines to assist federal departments and agencies in developing a strategy to enable the safe use of Social Media.[115] In brief, the document supplies nations with a special policy, and stresses that policies should not be adopted on the basis of technology itself, instead, they should focus on public servants' behavior, whose professional knowledge cannot be lacking of an appropriate security culture, and whose use of Social Media needs to be responsible. Government information systems are a constant target of attacks from malicious individuals. There are a variety of threats, but most that are perpetrated through social media fall into one of two types: identity theft and malware[116].

Identity theft is a crime that may occur to individuals or groups as large as hundreds of thousands of people at a single time. The damage may be as little as the loss of a hundred dollars (usually borne by financial institutions, in the case of stolen credit or debit cards) or hundreds of thousands of dollars in the case of fraudulently opened bank, credit, or even mortgage accounts; resulting in more losses from the legal work that must be done by both financial institutions and individuals to achieve resolution and restitution. To mitigate this risk, it is essential to understand how identity theft is perpetrated. Identity theft can occur by information scraping via social media websites and social media applications; social engineering; phishing; and spoofing.

It covers a range of threats, including viruses, worms, trojans, bots, and other harmful codes. Hackers develop malware for a number of reasons, including the desire to cripple the government or simply the potential of personal gain. Some malware is designed to attack the system in which it is installed; other forms are intended to take over their host system to launch

[115] Chief Information Officers Council (CIO), (2009), Guidelines…cit.
[116] Scherer, M. (2011, May 30). Can They Win, One Tweet at a Time? , Time. State of California, Office of the State Chief Information Officer.

an attack on a third party; and yet other applications are written not to cause any damage to the system, but to enable the creators to steal data residing on that system[117]. Whatever the goal of the malware, there are steps that end users, managers, and technical staff can take to mitigate the risk of malware. The point of attack determines the best counter measures.

People put an amazing amount of personal information online: a phone number on one website, a picture on another, a birthdate on a third, an address on a fourth, and so on. What they fail to realize is that this information can be harvested or "scraped" from many websites and compiled into a single, comprehensive portrait of the user. This information can then be used by cybercriminals either to commit identity fraud or to sell to organizations who will commit identity fraud[118]. Social engineering is a method used by hackers to acquire confidential personal information through fraud. Sometimes the hacker will contact the victim directly and try to solicit personal information over the phone, through a web-based application like e-mail, or through a social media website. Another tactic is for a hacker to contact a third party, like an office administrator, executive assistant, or even IT staff. The hacker may ask for personally identifiable information such as birthdates, home or work addresses, or other data. Social media websites are especially tempting targets for information scraping. There are two ways that this can happen. The first way is simply through accessing a person's information page. Often, people will divulge information through a social media website, and then relax their privacy controls. Also allow users to personalize their pages and to run third-party applications such as games. However, this grants the application access to all of a user's personal information,

[117] Ibid
[118] Obama B. (2009). Memo on Transparency and Open Government

irrespective of any privacy setting made in the social media website[119]. The vast majority of these applications only need basic personal details of a user. Furthermore, anyone can write an application and so some applications will have no security controls. Worse still, an application could have been developed by a cybercriminal. Managers, IT staff, and end users alike must recognize that connecting with people online poses privacy and security risks. One form of social engineering occurs when a cybercriminal on a social media website tries to befriend others. The intention is to build up trust so that confidential private information can be more easily extracted. The cyber criminal can create a fake Facebook profile or a bogus Twitter account.

Finally, on social media websites there are difficulties in establishing the authenticity of a person's identity when communicating with them, and in determining the accuracy of posts. Social media providers may be ineffective at detecting compromised accounts and subsequently restoring them. Another cyber criminal ploy is to try to befriend someone by claiming to have something in common; the cyber criminal may then contact the person through e-mail, over a social media website, or even on the telephone. Both managers and end users can help mitigate the risk of information scraping by creating and then following prudent social media guidelines. Though the specifics will be different for each office, the guiding principle is the same: don't put any more personally identifiable information online than is strictly necessary. To protect citizens who are accessing government services or communicating with their government online, management and IT staff must work together to ask for the least amount of personally identifiable information possible from citizens, and either delete that information once it is no longer necessary.

[119] Thomas, K., Grier, C., Nicol, D.M. (2010). unFriendly: Multi-party Privacy Risks in Social Networks, in Privacy Enhancing Technologies, eds. Atallah, M.J., Hopper, N.J., Lecture Notes in Computer Science, Springer Berlin / Heidelberg.

CHAPTER THREE

STRATEGIES USED BY THE MILITARYTO REDUCE THREATS OF SOCIAL MEDIA TO NATINAL SECURITY

3.1 Introduction

Social Media can represent an effective opportunity to preserve national security and/or reach the strategic interests of a state if used properly by civil institutions and in particular, by security services such as the military. In this respect, the before-mentioned Strat for analysts Papic and Noonan stressed that if Social Media are presenting a demonstrable threat to governments, it could be vital for security services to continually refine and update plans for disrupting new Internet technology". Besides, these tools can be used by governments for content creation, external collaboration, community building, and other applications and that failure to adopt these tools may reduce an organization's relative capabilities over time. More importantly Social Media can also be employed at the same time both for defence activities such as prevention, Early Warning Tool, prevision, strategic communication, open source intelligence (OSI), psychological operations and counter-propaganda.

3.2 Kenyan Military use of social media for Counter-propaganda Strategies

Any analysis into the strategy used to diffuse Al-Shabaab's ideological content must arise from the fact that the propaganda is multidirectional. Al-Shabaab's future depends not only on its aptitude to support an operative nucleus capable of realizing ostentatious assaults, and its ability to obtain funding and secure recruits. Eroding and neutralizing this image of a mighty fortress must be the ultimate goal of any action designed to offset Al-Shabaab's propaganda campaign.

Turn Al-Shabaab's Violent Discourse into an Unjustifiable discourse: The challenge is the uprooting of opinion that terrorism constitutes an acceptable way, independent of the legitimacy of the ends it seeks. Seating within the Muslim populations the idea that terrorist violence delegitimizes those that employ it can help to erode the supposed popular representation that terrorists always claim. A global rejection must be achieved in the long term to this type of violence. Kenya's military incursion into Somalia against the militant group Al-Shabaab dubbed "Operation Linda Nchi" (Swahili for "Operation Defend the Country") has turned into Twitter war. This came after the official military spokesperson Major E. Chirchir posted old photos claiming that a Kenyan Al Shabaab recruit had been stoned to death recently by the group members because of "a difference of opinion". It later became apparent that the photos were actually taken by a Somalian journalist in 2009 and does not even feature a Kenyan Al-Shabab recruit[120].

In some countries that have suffered for years, for example, Spain, terrorism is defined in legislation and punishable by a jail sentence. This strategy can be transplanted to other countries. Working against the apologists of terrorism does not hit against the public's general freedom of expression because the expression of support for the murder of innocents is a way of endorsing those who commit such actions[121]. In addition, in an interconnected world, without real restrictions to the flow of information on social media platforms, tackling this dilemma solely within a national arena is pointless. The mass media should be activated to spread an anti-terrorist message, as was done during the Cold War with the anti-Soviet Western radio listened to on the other side of the Berlin wall. In the current case, not perceiving these means as foreign agents of manipulation is difficult. Phenomenal successes like Al-Jazeera show the need to

[120]http://siku moja.blogspot.com/2012/01/kenya-defense-forces-and-al-shabaab.html.
[121]Kamalipour, Y. & Snow, N., eds., (2004). War, media, and propaganda. Lanham, MD: Rowman and Littlefield.

detract attention from these mediums, and take part in expressing opposing opinions and facilitating contrary information; otherwise the mass media become easy prey to systematic terrorist manipulation[122].

Any informative action that tries to offset the effects of terrorist imagery must use the mobilizing power that symbols possess. In this struggle to erode the image of terrorists being a fortress, such actions as the loud and clear advertising of the detentions of the terrorist, the publication of their confessions and of any act that shows their lack of loyalty to the organization and to their colleagues, and any other measures that cast a mistrust over Al-Shabaab's heroic image of fallen or captured members, can prove enormously helpful[123].

Rumor and misinformation occupy an important place in the terrorist network's propaganda strategy. Through them, Al-Shabaab manages to question the legitimacy and the honor of its opponents, without the need to justify the truth of its accusations. Rumors can consist of all kinds of delirious statements, conspiracy theories, and odd suggestions. Though the public first grants only limited credibility to this type of statements, the long-term effect supposes an internalization of doubt about all those involved: the political and security leaders, the security agencies, and the terrorists. The often secret nature of the authorities, the frequent lack of coordination, and the damage of the allegations, allow the „„fire to spread. Neutralization of the pernicious effects of these statements can perhaps be achieved through the creation of an agency or foundation that devotes itself exclusively to denying, in an informed manner, the misinformation, and to providing clear and forceful proof to end rumors. Keeping its composition neutral, by including

[122]Hall, L. (2006). Capers in the churchyard. Darien, CT: Nectar Bat Press.
[123]Manjoo, F, (2004), A Picture is no Longer Worth a Thousand Words

academics and professionals outside the political or military arenas, would contribute to its credibility and efficiency[124].

Terrorist propaganda relies on a wide use of the emotional impact of certain visual material. Without any type of available or effective restriction, crude images of corpses and mutilations can be found on terrorist-sponsored sparse Web pages, including disabled persons and injured men portrayed as supposed evidence of the results of Kenya Defence Forces (KDF) military action. Terrorists are conscious that appealing to the emotions is one of the most rapid and effective ways of modifying public and personal attitudes, and they do not hesitate to resort to any type of material that they consider to be useful to this end. Without committing to excesses, and always respecting ethical criteria, the Kenya counter-informative strategy cannot ignore the emotive perspective of this information war. Illustrating the results of terrorist action, through actual images of its victims and the resulting human tragedy, is one of the most powerful ways of delegitimizing terrorists. Together with respect due to the victims and their families, the exhibition of certain images can constitute a revolt against terrorists much more powerful than a long series of official communique´ s regarding penalty. Indeed, concealing the real results of terror only helps to generate an idealized stereotype removed from what terrorism actually is[125].

3.3 Kenya News Management by the Military

Much as the media abhor being "managed", all governments try to influence publics via the media, placing positive spin on their own actions and eroding the stance taken by adversaries, as during key negotiations. The existence of global information networks producing instant transmission of news to world audiences makes it hard to manage news. Some democratic

[124]Dinan, W., & Miller, D., eds. (2007). Thinker, faker, spinner, spy. London: Pluto.
[125]Andrew, H. (2009). Meeting Somalia‟s Al-Shabaab, BBC news, July 3.

governments understand that the relationship between the official establishment and the media is necessarily adversarial. It becomes virtually impossible to customize news for one audience, since it spills over to other audiences. Yet politicians address domestic audiences with themes that will resonate with them, as during elections; foreign audiences are expected to treat such rhetoric with indulgence[126].

Often the best news management comes from the military; they have a range of options for communicating their standpoint. Leaders who have media skills gain an advantage. A consequence of the rising importance of domestic publics is that foreign ministry spokesmen now focus mainly on the home reactions to foreign affairs issues, to the point of reduced attention to projecting home policy to the foreign media. This is an inversion of the past role of foreign ministries. By the same token, even on overseas visits, leaders are much more interested in what the home media say than on reaching out to foreign publics via the media in the countries visited. Ideally, the one should balance the other, and foreign ministries have their work cut out in ensuring that the latter are treated as an equal priority[127].

The Diaspora is often a key multiplier, in terms of spreading messages about the country of origin and helping in image projection. Diaspora Communities can potentially play a huge role in favourably promoting a nations image conversely therefore, because public diplomacy tried to influence mind space abroad and is conditioned by a society's belief in itself, a society that has

[126]Kishan S. (2011). 21st Century Diplomacy A Practitioner's Guide, The Continuum International Publishing Group, p. 88
[127] Ibid

self-doubts and does not have confidence in its government has citizens and diaspora communities that will not be allies in a governments public diplomacy efforts[128].

Mbugua wa Mungai argued that media coverage of events that focus solely on national issues and exclude peoples experiences in everyday life does not do people or peace justice. He argued that coverage of Kenyan's experiences of conflicts failed to represent effectively the conflict situation and the condition the people are in. He added that merely presenting the voice of the officials and government agents who may not be at conflicts scenes instead of highlighting the opinions and experiences of the people on the ground especially the women and children, presents a skewed representation of the violence[129].

In an unprecedented television coverage to the post-election violence effect on displaced families, CITIZEN TV brought to the homes of Kenyans in February 2008 images of what life in internally displaced people's camps looked like. The channel also engaged the voices of survivors of the violence as well as families who had lost children and other family members. This enabled Kenyans to feel the pain of their brothers and sisters living as refugees in their own country. Kenyans then mobilized through churches, mosques, social groups, NGO's and the international community to get food, clothes and other necessities to the families living in the camps[130].

[128]Evan H. Potter (2009). Branding Canada: Projecting Canada's Soft Power Through Public Diplomacy, McGill-Queen's University Press, P. 58

[129]MbũguawaMũngai, G. M. Gona (2010). Remembering Kenya. Identity, Culture and Freedom, published by Twaweza Communications Ltd. Westlands Nairobi Kenya p.166

[130] Ibid

3.4 Military Intelligence and Social Media Analytics

The ability to forestall future strategic and tactical contexts is of paramount importance in order to reduce the possibilities to be caught by surprise by threats and increase the resilience to them. In this regard, General Nicola Gelao - Chief of the Information and Security branch of the Italian Defense General Staff - affirmed that the ability to "hypothesize" the future is not an exact science, and it is very hard to foresee in advance and accurately how, when and where a threat will materialize[131]. From this perspective Social Media can become an invaluable resource for the benefit of the military, since they "can quickly turn into a valuable intelligence-collection tool"[132],as all Social Media users leave marks about their identity, abilities, predilections, movements, contacts, etc, which can be easily collected and analyzed, even though they have a no more updated or active profile.

A continuous and deep monitoring of these media can be carried out as a warning tool in case of present and future threats to national security, since the use of Social Media by criminal organizations, terrorist groups, adversary states and other competitors is more and more increasing. For this reason a continuous analysis of Social Media by military can serve as an early warning system. For example, military monitoring of Social Media in order to recognize the first signs of an hostile or potentially dangerous activity for a state's security (i.e. collecting and analyzing messages by opposing movements sent via social network sites for the organization of a violent protest can be useful in order to forestall a rebellion or to mitigate its negative consequences, studying the information shared by crackers in specialized blogs in order to launch an information attack to a critical infrastructure can concur in adopting suitable

[131] GELAO N., (2011), *Cyber Warfare: unnuovofronte per le ForzeArmate*, Information Warfare Conference 2010, Franco Angeli, Milano.
[132] PAPIC M., NOONAN S., (2011), *Social…*cit.

protection counter-measures, tracking teaching videos for military recruitment, spread via YouTube by an al-Qaedist group can help military who make use of them, understand the attack methods and techniques and devise effective methods to react and counter the terrorist threat, the continuous control of a Facebook profile updates and a careful exam of the photos published on that very profile can allow to trace the movements and the activities of the members of a criminal group and mapping their connections[133]. Another important aspect is the for the strategic warning and horizon scanning aimed at outlining the long- and medium-term trend of threats, at identifying the orientation of the opposing groups and forecasting their choices (i.e. collecting signs of protest from young people through the monitoring of the principal social networking sites can help forecast and maybe nip in the bud a dissent which could change into an organized protest movement or even in a revolutionary group, analyzing the discussions on blogs specialized in international politics and strategic studies can be useful to understand the possible long-term evolutions of foreign policy and of the strategic thinking of a state's leadership[134], studying the discussions of blogs specialized in science and technology can help military measure the possible long-term development of scientific and technological expertise in a certain place and mapping the relational networks developed on Social Media by members of subversive groups and analyzing their evolution can allow to forecast the possible development of the group itself.

US military launched a research program, called Open Source Indicators (OSI), and means to actively involve the academic world and the technologic industries with the aim of developing automatic systems for provisional analysis applied to forestalling national security related events: political crises, migrations, epidemics, humanitarian emergencies, protests, periods of economic

[133] DOZIER K., (2011), Exclusive: CIA following Twitter, Facebook, Associated Press, New York.
[134] OLIMPIO G., (2011), *Twitter osservatospecialedella CIA*, Corrieredella Sera, Milan.

instability, etc. In particular, OSI is based on the principle that relevant social events are always anticipated by changes of behavior through the population. Plotting and studying such behaviours can, in fact, be useful to anticipate the events themselves. The observance and measure of such changes can be carried out through monitoring data publicly available and coming from different sources, among which Social Media are placed first[135].

Using Social Media to obtain and analyze data for info-prevision and tactic-strategic warning purposes was of great interest to the US Deparment of Defence, which developed a specific program called "Social Media in Strategic Communication" (SMISC)[136] through DARPA, with the aim of monitoring such media so as to obtain a better knowledge of the environment, some units deployed abroad work into, and collect useful information to support military missions. Therefore, using Social Media helped the commanders of the US deployed locations to better understand the socio-politic, religious, economic and cultural characteristics of the area they work in and detect emerging threats. At this regard Thomas Mayfield, a US army colonel, claimed that "maintaining a Social Media presence in deployed locations allowed commanders to understand potential threats and emerging trends. The online community can provide a good indicator of prevailing moods and emerging issues"[137]. The DARPA affirmed that the general purpose of the 42 million dollar SMISC program was "to develop a new science of social networks built on emerging technology base including, but not limited to, information theory, massive-scale graph analytics and natural language processing", to be achieved creating

[135] WEINBERGER S., (2011), *The Spy Who Tweeted Me: Intelligence Community Wants to Monitor Social Media*, Wired, San Francisco.
[136] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), *Stories, Neuroscience and Experimental Technologies: Analysis and Decomposition of Narrative in Security Contexts*, DARPA-SN-11-20, Arlington County, VA.
[137] MAYFIELD T. D., (2011), *A Commander's Strategy for Social Media*, Joint Force Quarterly vol. 60/2011, National Defense University, Washington, DC.

automated and semi-automated support techniques and tools for analysts who systematically use Social Media for military purposes[138].

Open-source intelligence (OSINT) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources; it is not related to open-source software or public intelligence. Conducting OSINT for wider intelligence, counter-terrorism and risk management work in Kenya has become a complex and increasingly resource intensive task for both Government and Intelligence agencies and the commercial risk management sector alike. There are a large number of open-source activities taking place throughout the Kenyan Government. Frequently, these open-source activities are described as media monitoring, "media analysis", "internet research" and "public surveys" but are open source nonetheless[139].

A good illustration which depicts a clear and expected spike in OSINT by the predicted surge in media and online user generated content following a major terrorist or crisis event. In this case, the Westgate Mall attacks in Kenya by Al Shabaab in September 2013. By analyzing the results surrounding this surge in activity new leads and sources could be identified from within the content. Persons who generate content which indicates inside knowledge of the event or being close to a Persons of Interest, or those who have connections to terror groups can be isolated through analysis of this data for subsequent addition into social network analysis (SNA) and link analysis.

Analysis of this segment of data also leads to further discovery and identification of source types that may be of further interest. An individual, even if using false credentials online will often

[138] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), *Social Media…*cit.
[139] BrelsfordP. (2013). Employing a social mediamonitoring tool as an OSINTplatform for Intelligence,Defence& Security

have published other material which divulges essential elements of information or links to other online sources or individuals of interest that feed into building an increasingly accurate intelligence picture and horizon scanning function[140].

3.5 Military use of Social Media for Public Diplomacy

Many US Army reports warn of social media's potential misuse by terrorists, government policies are evolving to embrace the use of tools such as Facebook and Twitter as a means of strategic communications and public diplomacy. The federal government begun to embrace using these same tools to allow free access to information, spread democratic values and ideas, and combat the misinformation spread by terrorist groups' media campaigns. In February 2010, Department Of Defense issued a Directive-Type Memo (DTM) outlining the department's new social media policy, citing Internet-based capabilities including social networking services as integral to operations[141].

US diplomacy actively uses Social Media for influence and propaganda activities, too. In fact, in 2008, the program Public Diplomacy 2.0 was developed and officially presented by the then Under Secretary of State for Public Diplomacy James Glassman during an event specially organized191 at the New America Foundation. Public Diplomacy 2.0 has been defined by Glassman himself as a new communication process which takes advantage of Social Media potentialities and credits the diplomatic corps with a significant competitive advantage, both in the relationships with other states in the economic, scientific, technologic and geo-strategic fields and with regard to soft power activities aimed at countering radicalized ideologies, religious extremism, and politic violence. Public Diplomacy 2.0 activities must be based on specific

[140] Ibid

[141] Office of the Deputy Secretary of Defense, Directive-Type Memorandum 09-026, *Responsible and Effective Use ofInternet-Based Capabilities*, February 25, 2010.

central strategic planning, coordinated with all the institutions involved in diplomatic activities, and well-integrated with the military apparatus. Talking about Public Diplomacy 2.0, Helle Dale argued that Social Media can become a primary vehicle with which the US government addresses public opinion around the world, in addition to traditional means such as radio, TV, libraries, student exchange programs. She further claims that "public diplomacy and strategic communications experts within the US government are exploring the potential of the new social media in the effort to win hearts and minds abroad, especially in the Muslim world where today war of ideas is being fought. Enemies of the United States are already expert in using these low-cost outreach tools that can connect thousands, potentially even millions, at the touch of a computer key or cell phone button"[142]. In order to better understand how important Social Media are for the US Department of State it can be useful to briefly cite a cablegram, released by the site Wiki leaks, thanks to which on February 2010 the US embassy in Jakarta required immediate additional funding to use new media and social networking tools so as to support the visit of President Obama in Indonesia, scheduled for the following March[143]. In summary, Taylor argued that public diplomacy for US military was intended to improve U.S. credibility and legitimacy, weaken an adversary's credibility and legitimacy, convince selected audiences to take specific actions that support U.S. or international objectives and cause a competitor or adversary to take (or refrain from taking) specific actions[144].

In Kenya, Military uses Diplomacy as Tool for gathering and Disseminating Information. Through blogs, Facebook, emails and Twitter, Kenyans can source and comment on topical

[142] DALE H. C., (2009), *Public Diplomacy 2.0: Where the U.S. Government Meets "New Media"*, Backgrounder n. 2346 – published by The Heritage Foundation, Washington, DC.
[143] **http://www.wikileaks.org.**
[144] TAYLOR D., (2011), *Social Media Targeted by Pentagon for* «*Strategic Communication*», Infowars, website: **http://www.infowars.com/social-media-targeted-by-pentagon-for-strategic-communication/.**

political, economic as well as social issues. For instance during the 2002 and 2007 General Elections, most Kenyans learnt of the results through mobile phones, not the conventional media. The internet blogs and emails allow Kenyans to read and comment on issues that conventional media houses prefer to ignore[145].

As much as the internet plays an important role in getting Kenyan stories out into the world, where people could be rescued from situations of grave danger because an SMS was sent via the internet, the virtual media can also be seen as a double-edged sword. Mungai[146] states that diaspora Kenyans used virtual media such as internet chat rooms and email to actively summon their kinsmen resident in Kenya to dismember the country. That ethnic bigotry was a key feature of these interactions in which even highly educated academics blithely took part.

3.6 Military use of social media for Psychological Operations (PsyOps)

Military doctrine includes the possibility of exploiting the wide audiences of social media to conduct psychological operations (PsyOps) in a context of information warfare with the primary intent to influence the "sentiment" of large masses e.g., emotions, motives, objective reasoning. PsyOps is defined by the U.S. military as "planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals[147]." "Psychological operations" is not a new concept. In the past, on many occasions and in different periods, the military has used the diffusion of information to interfere with opponents divulging artifact information or propaganda messages. Military intelligence has used

[145]MbũguawaMũngai, G. M. Gona (2010). Remembering Kenya. Identity, Culture and Freedom, published by Twaweza Communications Ltd. Westlands Nairobi Kenya p.152
[146] Ibid
[147]NATO Doctrine on Psychological Operations AJP 3.10.1. SHAPE 2007, page 1 – 6. NATO UNCLASSIFIED.

secret agents infiltrated behind the enemy lines or launched leaflets with a plane over enemy territories; today, social networks have the advantage over these types of missions. The terms "psychological operations" and "psychological warfare" are often used interchangeably; "psychological warfare" was first used in 1920 and "psychological operations" in 1945. Distinguished theorists like Sun Tzu have highlighted the importance of waging psychological warfare: "One need not destroy one's enemy. One only needs to destroy his willingness to engage. "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the supreme excellence"[148].

Military consider PsyOps a crucial option for diplomatic, military, and economic activities, the use of new-generation media and large-diffusion platforms such as the mobile and social media gives governments a powerful instrument to reach critical masses instantly. PsyOps consist in conveying messages to selected groups, known as target audiences, to promote particular themes that result in desired attitudes and behavior that affect the achievement of political and military objectives[149]. NATO promoted a doctrine for psychological operations defining target audience as"an individual or group selected for influence or attack by means of psychological operations."In the document, "Allied Joint Doctrine for Psychological Operations AJP-3.10.1(A)," NATO has highlighted the possibility of supporting military operations with PsyOps intend to weaken the will of the adversary or potential adversary target audiences, reinforce the commitment of friendly target audiences and gain the support and cooperation of uncommitted or undecided audiences. Obviously, a psychological operation has been well contextualized in today's military because of advanced state of technology at the disposal: the Internet, virtual

[148] Sun Tzu,The Art Of War,
[149]US Joint Publication 3-13.2. Psychological Operations, 07 January 2010, page V-2 can be found on: http://www.fas.org/irp/doddir/dod/jp3-13-2.pdf

reality, blogs, video games, chat bots, and, of course, social network platforms is used by military for various purposes. The military sector is investing largely in PsyOps professionals and is exploring these technologies to influence individuals to support their cause or the sentiment of an entire population.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION

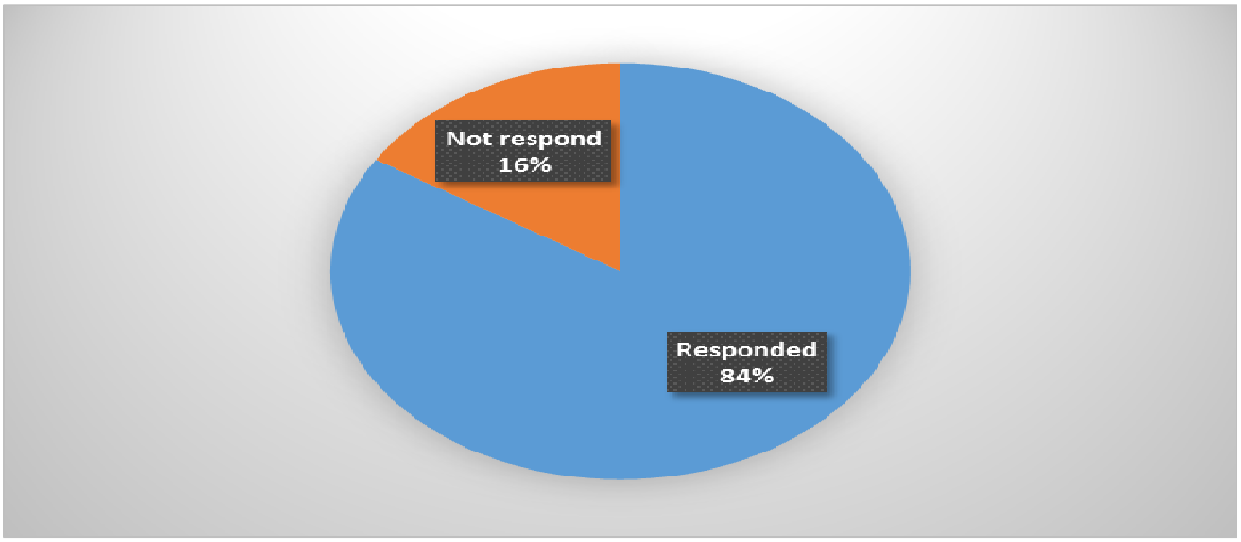
4.1 Introduction

This chapter presents an analysis of data collected about social media and national security threats in Kenya. The main objective of the study was to analyze social media and national security threats in Kenya. The chapter is arranged according to the research objectives. Data is presented in graphs, tables containing means, standard deviations, frequencies and percentages.

4.2 Response Rate

The study was conducted on a sample size of 50 members of the military from Nairobi based units. However, out of the issued questionnaires, 42 were duly filled and returned making a response rate of 84% as shown in figure 4.1 below.

Figure 4.1: Response Rate

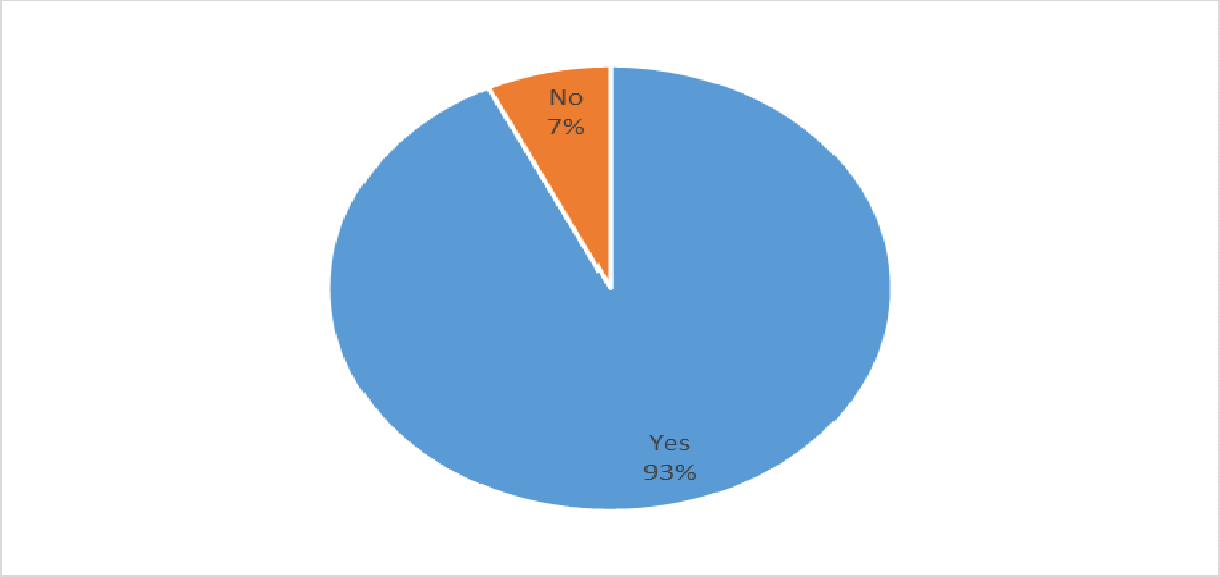


This response rate was sufficient for data analysis and therefore the researcher analyzed the responses and presented the following findings.

4.3 Threats of Social Media

This section sought information about threats of social media technology to Kenya's national security. The study started by requesting respondents whether social media is a threat to national security. Findings are presented in figure 4.2.

Figure 4.2: Social Media as a Threat



From the findings, majority of the respondents (93%), were in agreement that social media is a threat to national security while 7% were in denial.

4.3.1 Social Media as a Tool

The study asked respondents if they agree that social media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members. All of the respondents (100%) agreed to the statement. The study continued and requested the

respondents to state the extent to which terrorists use social media as a tool for ideological radicalization, recruitment, communication and training. Respondents agreed that terrorists use social media as a tool for training, and recruitment with a mean score of 2.45 and 1.90 respectively, as shown in table 4.1

Table 4.1: Social Media as a Tool

	Mean	**Std. Deviation**
Ideological radicalization	1.21	0.415
Recruitment	1.90	0.778
Communication	1.62	0.582
Training	2.45	0.942
Propaganda	1.19	0.397
Threats of violence	1.55	0.633

Those who agreed that social media is used for communication (1.62), threats of violence (1.55), ideological radicalization (1.21) and propaganda (1.19). Social Media are more and more used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training.[150] In addition to this, terrorist groups take advantage of Social Media to communicate with cyber-crime groups and to coordinate along with them fund-raising activities carried out in

[150] UN Counter-Terrorism Implementation Task Force, (2011), *Use of the Internet to Counter the Appeal of Extremist Violence, Conference Summary*, Riyadh.

part or completely on the Internet. The link between organized crime and terrorist organizations is increasing considerably in the cyber-world, and this coalition will be able to produce new offensive technologies.[151]

Although the strength of social ties strongly influences recruitment on the individual level, weak social ties can be effective in communicating and spreading the message of a social movement across diffuse networks hence an effective network structure would have dense networks of weak ties to outside entities in addition to strong interpersonal ties within those groups.[152] Lorraine Bowman-Grieve[153] pointed out that Social Media "play an important role in influencing the behavior of the individual and their readiness to take part in collective action because of their inherent socializing, recruitment and decision shaping functions", besides, they "facilitate social interaction and the formation of social bonds, which in turn can lead to changes in attitudes and behavior over time.

Apart from being used for recruitment purposes, Social Media are also used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, at throwing civil population into a panic. Respondents agreed that social media was used for propaganda during and after the KDF entered Somalia in 2010. There was communication from the Kenya military as well as Al-shabaab and the public were important to ensure they obtain the actual news not fabrications by the enemy. The military advised journalist to countercheck facts and the most convenient source was the Kenyan military who were often available for the press and put right facts. Here Elite sources such as the Kenyan government and military are important

[151]Blitzblau S., (2011). Analisitecnicadellecapacità di NetINTdeigruppiterroristici, Information Warfare Conference 2010, Franco Angeli, Milano.
[152]McAdam D., Sidney T. and Charles T. (2008). Methods for Measuring Mechanisms of Contention. Qualitative Sociology 31, no. 4 (2008): 310.
[153] Bowman-Grieve L., (2010). A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment, Euro ISI Conference Submission, Leeds.

for all informants. Military keenly considered what the Al-Shabaab is communicating via social media websites, but are extra cautious and always countercheck all information before publishing it. When the Al-Shabaab posts something, the Kenyan military gets to comment on it. Respondents stated that if you look at their Twitter page, Al-Shabaab keeps on posting propaganda. And when counterchecked, it is realized that either nothing happened at all or if an incident happened, they usually try to exaggerate the death toll.

According to the study Al-Shabaab was not the only ones spreading propaganda. The respondents also described how the Kenyan military uses propaganda as a morale-booster or as a way of confusing the enemy. The military and Al-Shabaab lied more often, respondents argue. The case example here was the ongoing war of KDF in Somalia. One case in point illustrated cited was where ,respondents noted that after counterchecking facts by making phone calls to local Somali sources and independent expert or by reading reports from international news agencies, the informants publish what they consider to be the truth.

Respondents indicated reasons as to why Al-Shabaab will wanted to use propaganda. It was found that Al-Shabaab always positioned themselves as winners. Al-Shabaab wanted to appear like they are never losing the battle. For example, whenever KDF said it had killed 20 Al-Shabaab for example, Al-Shabaab never wanted to admit that. Even if it was true, Al-Shabaab wanted to position themselves as the winners. They wanted to deny, that none of their troops had been killed', even when it was true. According to military respondents, Al-Shabaab are not well equipped in terms of weaponry and all that. They termed them as just a militia group, with a backing of al-Qaeda. Respondents said that, because of the border issues, Al-Shabaab did not have a way of shipping in weapons. The troops that are fighting in Somalia, be it the AU backed troops and the Kenyan of course; had proper equipment to fight al-Shabaab.

Social media is also used by terrorists for communication purposes. The use of social media as a new communication platform introduces serious security and privacy concerns, including new vectors for cyber-attack that the government and the military cannot ignore. Social Media are connection and mass communication tools, characterized by a global diffusion and an ever-growing level of use, considering their handiness and flexibility, as well as their extreme cheapness.[154] Since spreading news and content on Social Media can be considered "viral", this kind of propaganda is able to considerably overdraw the media effect already produced by traditional means of information and communication and cause consequences even more dangerous than those caused by the terrorist attacks themselves in the country.

4.3.2 Criminal Organization Threats

The study requested respondents to rate the extent to which criminal organizations are threats to national security. Majority of the respondents were in agreement that criminal organisations are threats on drug smuggling, human trafficking and money-laundering with a mean scores of 2.6, 2.5 and 2.35 respectively as shown in table 4.2

[154]Hasni A, 'Hacker group Anonymous claims attacking Greek official websites' As seen in The News Tribe, 9 October 2012, viewed on 29 November 2012.

Table 4.2 Criminal Organization Threats

	Mean	Std. Deviation
Spread of viruses	2.12	0.739
Trojans	2.07	0.745
Drug smuggling	2.60	0.798
Human trafficking	2.50	0.707
Money-laundering	2.35	0.975
Spreading child pornography	1.33	0.612
Mobilization	1.76	0.790

Those respondents who were in agreement that criminal organisations use social media for spreading child pornography and for mobilization had mean scores of 1.33 and 1.76 respectively. although the use of Social Media is necessarily linked to the interaction between a person and the information medium, organized groups in the broadest meaning of the term; states; public agencies; companies; movements; and terrorist groups are potential Social Media users, too.[155] To date the terrorist groups which make the most substantial use of Social Media for their own purposes are the Islamic-jihadist[156] who have their operations in the country.

[155] Ibid

[156] Blitzblau S., (2011), Analisi tecnica delle capacità di NetINT dei gruppi terroristici, Information Warfare Conference 2010, Franco Angeli, Milano.

Criminal groups which use Social Media are made of people coming from the same geographic area and who know each other personally, but also of people scattered all over the world who are linked exclusively by "virtual" relations. These criminal communities are generally coordinated by one or more moderators who have the power to remove the members who do not provide high-quality information or tools and to assign an increasing level of reliability to those who make more contribution than others[157]. The social networks or ties bring them together and by use of social media are able to organize themselves, recruit new members, communicate and engage in covert operations resulting to achievement of its organizational strategy.

The study further requested respondents to rate the extent to which community criminal organizations like Mombasa Republican Council (MRC) and '*Mungiki'* use social media as a tool to recruit, communicate, Spread propaganda and radicalization. Findings show that majority of the respondents agreed that community criminal organizations like Mombasa Republican Council (MRC) and '*Mungiki'* use social media for recruitment and communication having means of 3.19 and 2.67 respectively as shown in table 4.3.

Table 4.3: Extent to Which Community Criminal Organizations

	Mean	**Std. Deviation**
Recruit	3.19	1.018
Communicate	2.67	1.119
Spread propaganda	2.40	1.270

[157]Campobasso P., (2011), Le nuovesfideallasicurezzadellospaziocibernetico, Information Warfare Conference 2010, Franco Angeli, Milano.

Radicalize youths	2.50	1.174

Those who depict disagreement stated that criminal community groups use social media to spread propaganda and radicalize youths with mean scores of 2.4 and 2.5 respectively. In conducting criminal activities, criminal organizations use Social Media as support, communication and coordination tools to conduct their illicit activities. This kind of illicit activities can be either purely information ones like spreading child pornography with fee, virtual identity thefts, phishing, spread of viruses, and worms or traditional ones like drug smuggling, human trafficking, money-laundering and transfer of documents from industrial espionage.[158]

Social Media are used by Islamist groups for propaganda activities aimed at making Kenyans feel that they have successful terrorist attacks, and, consequently, at throwing Kenyans into a panic. Since Al-Shabaab has a "net-like" decentralized structure, Facebook and Twitter is used effectively as platforms to organize and connect the single groups linked to Al-Shabaab, and the leadership.

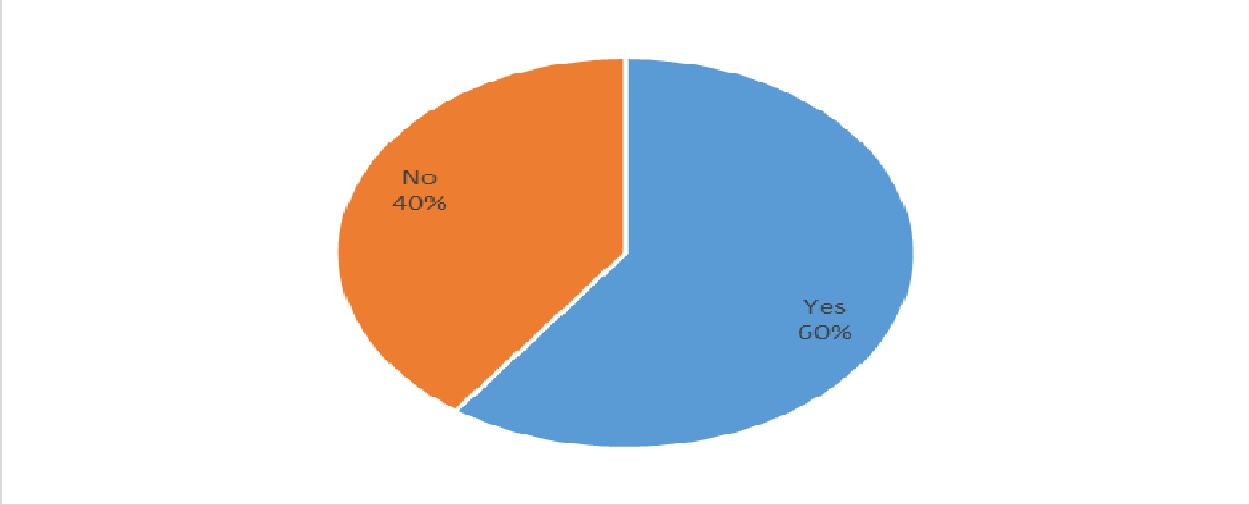
Respondents noted particular emphasis on MRC postings advocating that coastal Kenya was not part of Kenya. Such was commonly posted on social media as a tool to influence local community to rally behind them and revolt against the government. Accordingly, responded noted that MRC was able to attain national attention through mass and social media, and were able to convience local community that they were engaged in a justifiable course.

[158] Intelligence And National Security Alliance, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA.

4.4 Military use of Social Media for National Security

This section sought information about the use social media by the military to reduce threats and promote national security. The study started the section by asking respondents if the military use social media for military operations. From the findings, majority of the respondents (60%) agreed that the military use social media for military operations while 40% disagreed as shown in figure 4.3.

Figure 4.3: Military Use Social Media for Military Operations



From the responses, respondents indicated that military use social media for communicating process of operation, boost morale of soldiers, clarify on propaganda messages sent by enemies & dispelling rumours, for updating civilians on progress of military operation, for public relations and operation linda Kenya. Dinan & Miller[159] agrees that military use social media in discrediting those who spread rumors. Rumor and misinformation occupy an important place in

[159] Dinan, W., & Miller, D., eds. (2007). Thinker, faker, spinner, spy. London: Pluto.

the terrorist network's propaganda strategy. Through them, Al-Shabaab manages to question the legitimacy and the honor of its opponents, without the need to justify the truth of its accusations. Rumors can consist of all kinds of delirious statements, conspiracy theories, and odd suggestions. Though the public first grants only limited credibility to this type of statements, the long-term effect supposes an internalization of doubt about all those involved: the political and security leaders, the security agencies, and the terrorists.

The study further asked respondents if there are officers whose job functions include spending time on social media sites to monitor any security threat that spreads around. All respondents except 2 agreed to the statement which indicated that members of the military from Nairobi based units believe there are officers whose job functions include spending time on social media sites to monitor and analyze any security threat that spreads around. About the tools that helps in the analysis of social media threats to national security, 81% of the members of the military from Nairobi based units agreed that they have the tools while 19% indicated they don't have. They stated that they have sniffer soft wares, use of customized web crawlers, news aggregators, internet, Topsy twitter and Facebook as well as customized software to perform social media analytics.

The active use of social networking by the Israeli military and the Persona software project reveal a clear military application[160]. The Persona software, and social media in general, may be used for targeted attacks against individuals; examples of false-flag operations were provided above. Such social-engineering attacks can be seen as a form of psychological operation. These attacks can trick or coerce the target into providing information in an intelligence-gathering

[160] Hodge, N. (2008, December 30). *YouTube, Twitter: Weapons in Israel's info war*. Retrieved from http://www.wired.com/dangerroom/2008/12/israels-info-war

operation or downloading malicious code. Applications to manage fake profiles, such as the Persona software mentioned above, may be used to set up these honey pots and automatically record any activity or invitations on the profiles. Analysis will aid in discovering attack patterns, allowing for the profiling of the attackers, such as their regional origins, or provide signatures to identify the attacker in future incidents. This intelligence may prove to be crucial in awareness training, as specific attack signatures and examples can be provided, allowing for better identification and improved reporting of false-flag attempts.

US military launched a research program, called Open Source Indicators (OSI), and means to actively involve the academic world and the technologic industries with the aim of developing automatic systems for provisional analysis applied to forestalling national security related events: political crises, migrations, epidemics, humanitarian emergencies, protests, periods of economic instability, etc. In particular, OSI is based on the principle that relevant social events are always anticipated by changes of behavior through the population. Plotting and studying such behaviors can, in fact, be useful to anticipate the events themselves. The observance and measure of such changes can be carried out through monitoring data publicly available and coming from different sources, among which Social Media are placed first[161].

Open-source intelligence (OSINT) is intelligence collected from publicly available sources. Conducting OSINT for wider intelligence, counter-terrorism and risk management work in Kenya has become a complex and increasingly resource intensive task for both Government and Intelligence agencies and the commercial risk management sector alike. A good illustration which depicts a clear and expected spike in OSINT by the predicted surge in media and online

[161] WEINBERGER S., (2011), *The Spy Who Tweeted Me: Intelligence Community Wants to Monitor Social Media*, Wired, San Francisco.

user generated content following a major terrorist or crisis event. In this case, the Westgate Mall attacks in Kenya by Al Shabaab in September 2013. By analyzing the results surrounding this surge in activity new leads and sources could be identified from within the content. Persons who generate content which indicates inside knowledge of the event or being close to a POI, or those who have connections to terror groups can be isolated through analysis of this data for subsequent addition into social network analysis (SNA) and link analysis.

4.4.1 Mechanisms by the Military to Counter Social Media Threat

The study requested respondents to rate the extent to which respondents the military use mechanisms to counter threats of social media to national Security. From the findings, majority of the respondents were in agreement that counter propaganda is used by the military to counter social media threats with a mean score of 2.33 as shown in table 4.4.

Table 4.4: Mechanisms by the Military to Counter Social Media Threats

	Mean	**Std. Deviation**
Counter propaganda	2.33	1.199
Public diplomacy	2.17	1.231
Open source intelligence	2.00	0.946
News	2.26	1.019

Respondents also agreed that the military use news, public diplomacy and open source intelligence with mean scores of 2.26, 2.17 and 2.00 respectively. Often the best news

management comes from the military; they have a range of options for communicating their standpoint. Leaders who have media skills gain an advantage. A consequence of the rising importance of domestic publics is that foreign ministry spokesmen now focus mainly on the home reactions to foreign affairs issues, to the point of reduced attention to projecting home policy to the foreign media. This is an inversion of the past role of foreign ministries. By the same token, even on overseas visits, leaders are much more interested in what the home media say than on reaching out to foreign publics via the media in the countries visited. Ideally, the one should balance the other, and foreign ministries have their work cut out in ensuring that the latter are treated as an equal priority.

US diplomacy actively uses Social Media for influence and propaganda activities, too. In fact, in 2008, the program Public Diplomacy 2.0 was developed and officially presented by the then Under secretary of State for Public Diplomacy James Glassman during an event specially organized191 at the New America Foundation. Public Diplomacy 2.0 has been defined by Glassman himself as a new communication process which takes advantage of Social Media potentialities and credits the diplomatic corps with a significant competitive advantage, both in the relationships with other states in the economic, scientific, technologic and geo-strategic fields and with regard to soft power activities aimed at countering radicalized ideologies, religious extremism, and politic violence[162].

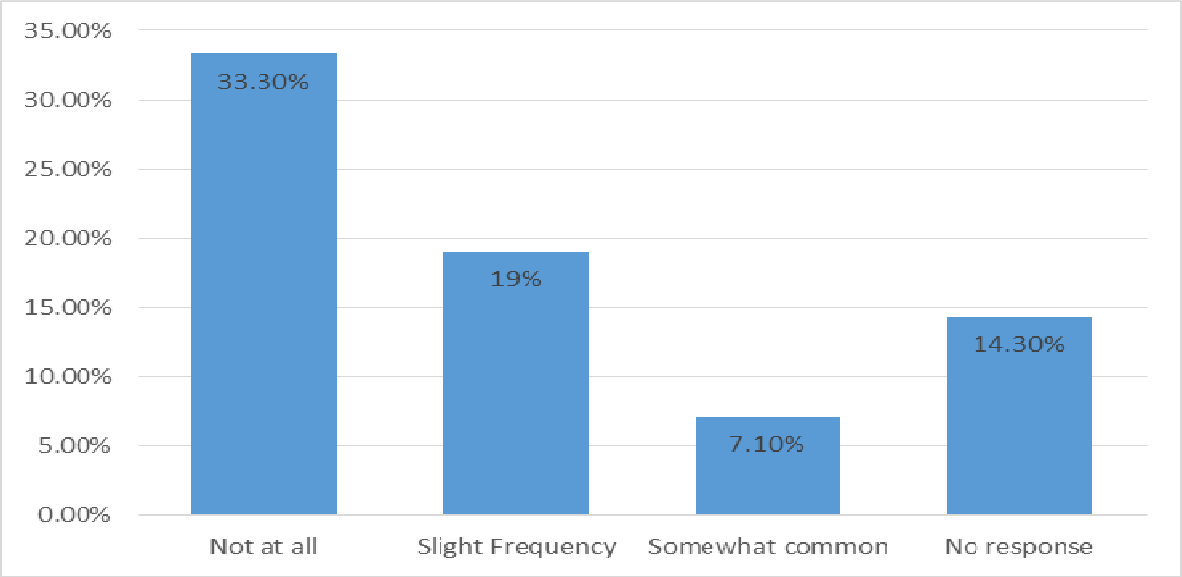
In Kenya, Military uses Diplomacy as Tool for gathering and Disseminating Information. Through blogs, Facebook, emails and Twitter, Kenyans can source and comment on topical political, economic as well as social issues. Another case in point was during the 2002 and 2007

[162] DALE H. C., (2009), Public Diplomacy 2.0: Where the U.S. Government Meets "New Media", Backgrounder n. 2346 – published by The Heritage Foundation, Washington, DC.

General Elections, most Kenyans learnt of the results through mobile phones, not the conventional media. The internet blogs and emails allow Kenyans to read and comment on issues that conventional media houses prefer to ignore[163].

The study further requested respondents to state how frequent there has been incidences in the military of inadvertent disclosures of sensitive information. Findings are presented in Figure 4.5 below.

Figure 4.4: Incidences in the Military of Inadvertent Disclosures of Sensitive Information



From the findings, majority of the respondents (33.3%) indicated that there has not been incidences at all in the military of inadvertent disclosures of sensitive information to the public, 19% stated that there has been a slight incidence while 7.1% indicated that it is somewhat common.

[163]MbũguawaMũngai, G. M. Gona (2010). Remembering Kenya. Identity, Culture and Freedom, published by Twaweza Communications Ltd. Westlands Nairobi Kenya p.152

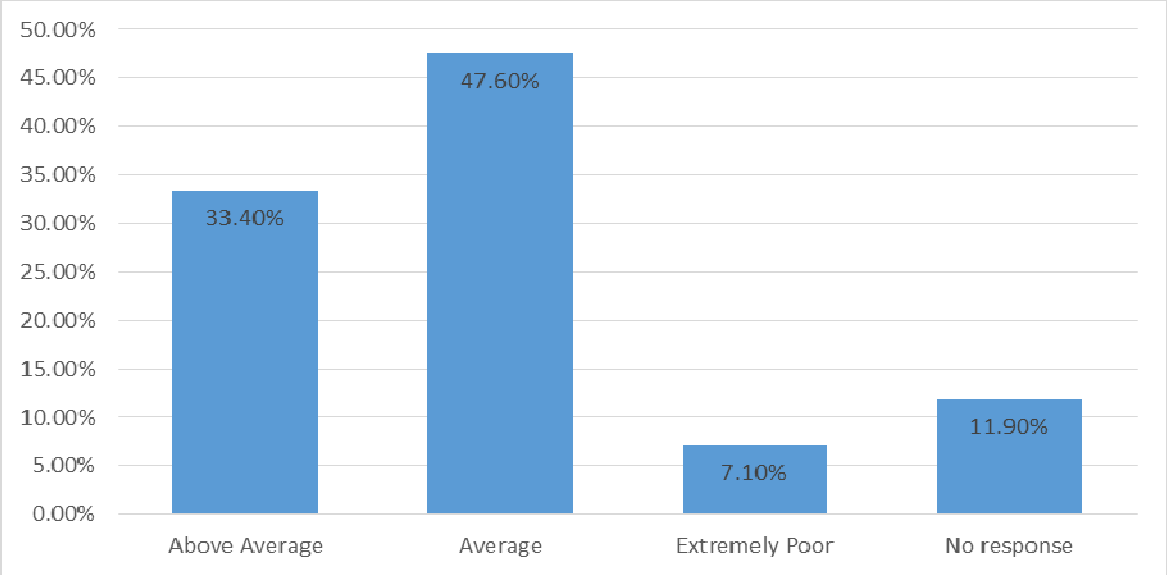
Restricting access to among military officers may have some impact; however, it does not prevent posts after the person has left the service. A former Israeli soldier posted a photo of herself posing with prisoners, causing a public outcry. She was no longer serving in the military, so the legalities were not clear; however, the pictures were removed[164]. The Russian Federal Security Service has banned its active members from certain social media websites over security concerns. These concerns are well founded, because more than 50 mentions of Russian strategic military assets were found by researchers on Russian social networks, including the location of nuclear weapons bases and major warships[165]. A similar study conducted by the U.S. Air Force found that 60% of active-duty members posted sufficient information on Myspace to be vulnerable to targeted attacks, such as blackmailing or kidnapping of deployed personnel[166]. These incidents indicate an intended use of social media for perception management and an underlying concern that adversaries can gain intelligence through information leaks. During the operation of KDF in Somalia, a Kenyan military apologized for posting on social media an old photograph that misrepresented stoning of an Al-Shabaab member accused of being a Kenyan spy. The photographs that KDF posted to twitter were taken by the Associated Press in 2009, and showed a man buried in the ground up to his chest being stoned to death by masked men belonging to militant group Hizbul Islam, not Al-Shabaab. Journalists, bloggers and the Harakat al-Shabaab al-Mujahideen(HSM) Twitter account pointed out the error. KDF acknowledged the tweet upload error, its reprint in the local press and regretted the embarrassment caused to the publics. However, it was true that a Kenyan was stoned to death in Kismayo.

[164] Wood, P. (2010, August 17). Israeli woman soldier denies Facebook photos wrongdoing. *BBC.* Retrieved from http://www.bbc.co.uk/news/world-middle-east-10997011
[165] Carr, J. (2010). *Inside cyber warfare*. Sebastopol, CA: O'Reilly.
[166] ibid

4.5 Kenya's Current National Security

The study sought information about Kenya's national security status. It started by asking respondents to rate the current state of Kenya's national security with regard to threats from social media. From the findings, 47.6% of members of the military from Nairobi based units stated that the security in Kenya is average.

Table 4.5: Current State of Kenya's National Security



However, 33.4% indicated that Kenya's security with regard to social media is above average while 7.1% felt that it is extremely poor. The Internet has revolutionised the way people communicate through e-mail, chat rooms, electronic messaging and instant information access. Although there is no known country that has prosecuted social media crimes, a number of countries have come up with measures to curb some vices promoted on the Net. Kenya, however, is still grappling in the dark as the monster of hatred spreads. And also Al-Shabaab has been using social media to send messages to Kenya and Kenya's inability to dilute the message before it reaches citizens shows instability in the Kenyan security.

4.5.1 Social Media Contribution towards Insecurity in Kenya

The study requested respondents to rate the extent to which insecurity in Kenya been contributed by social media. From the findings, members of the military from Nairobi based units agreed that social media has contributed towards cattle rustling and poaching both having scored means of 3.98 and 3.36 respectively as shown in table 4.5.

Table 4.6: Social Media Contribution towards Insecurity in Kenya

	Mean	**Std. Deviation**
Terrorism attacks	2.55	1.273
Hate speech	1.33	0.902
Poaching	3.36	1.046
Information warfare	1.81	0.707
Tribal clashes	1.95	0.987
Cattle rustling	3.98	0.811

Members of the military from Nairobi based units also agreed that social media has contributed towards terrorism attacks with a mean score of 2.55, tribal clashes (1.95), information warfare (1.81) and hate speech with a mean score of 1.33. No research was found that comprehensively measures the amount of hate speech that occurs online. The Simon Wiesenthal Centre's annual Digital Terror and Hate Report from 2012 was based on 15,000 'problematic' websites, social

networks, forums, online games and apps. They believe this has seen an increase of around 3,500 problematic outlets since 2010. Similarly, the International Network Against Cyber hate, 2013 has argued that over recent years 'the amount of cyber hate has grown to enormous proportions', with 'Islam, Jews, lesbians and gays, blacks, Roma, liberals' and 'left-wingers' representing the main targets of online abuse.

The study finally requested respondents to give suggestions of how to protect ourselves against offensive use of social media and improve on our security situation. The findings as suggested by members of the military from Nairobi based units were to install soft wares that monitor hate speech and act on information gathered with firmness, through legislation, interception & censorship, taking punitive measures against persons identified propaganda hate speech , liaising with owners of social media platforms to monitor and shut down sites deemed to be propagating criminal activities., Constant monitoring of misuse of social media, coming up with policies to guard against misuse of social media, having necessary laws to control people on how to use social media, mechanisms to trace social inciters in place, teaching the public about the use of social media without hate speech, block sources of threat in the social media, campaign for positive use of social media and prosecute hate speech mongers.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

In this chapter, summary of the study is presented according to the research objectives. The chapter also provides conclusions of the study as well as recommendations to the study.

5.2 Summary of the Study

From the findings, it was found that social media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members. Social media is also used as a tool for training, recruitment, propaganda and communication. The study found that terrorist groups take advantage of Social Media to communicate with cyber-crime groups and to coordinate along with them fund-raising activities carried out in part or completely on the Internet. Although the strength of social ties strongly influences recruitment on the individual level, the study found that weak social ties can be effective in communicating and spreading the message of a social movement across diffuse networks hence an effective network structure would have dense networks of weak ties to outside entities in addition to strong interpersonal ties within those groups. The study found that social media are also used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, at throwing civil population into a panic. It was found that the military advised journalist to countercheck facts and the most convenient source was the Kenyan military who were often available for the press and put right facts as may have been said by Al-Shabaab. The study found that criminal organisations are threats on drug smuggling, human trafficking and money-laundering with a mean score of 2.6, 2.5 and 2.35 respectively. The study found that terrorist

groups which make the most substantial use of Social Media for their own purposes are the Islamic-jihadist. It was found from the study that community criminal organizations like Mombasa Republican Council (MRC), '*Mungiki'* and '*Sungusungu'* use social media as a tool to recruit, communicate, spread propaganda and radicalization to a great extent.

The study found that 60% of the members of the military agreed that the military use social media for military operations, communicating process of operation, boost morale of soldiers, clarify on propaganda messages sent by enemies & dispelling rumours, for updating civilians on progress of military operation, for public relations and operation Linda Kenya. It found that members of the military from Nairobi based units believe there are officers whose job functions include spending time on social media sites to monitor any security threat that spreads around and 81% of the members of the military from Nairobi based units agreed that they have the tools that helps in the analysis of social media threats to national security. It was found from the study that the military uses Open-source intelligence (OSINT) collected to analyse social media threats since it was used in Westgate attack. The study found that counter propaganda is used by the military in to counter social media threats. Respondents also agreed that the military use news, public diplomacy and open source intelligence. The study found that often the best news management comes from the military; they have a range of options for communicating their standpoint. The study found that the Kenyan Military uses Diplomacy as Tool for gathering and Disseminating Information. Through blogs, Facebook, emails and Twitter, Kenyans can source and comment on topical political, economic as well as social issues. The study found that 33.3% of the members of the military believe that there have little or no incidences at all in the military of inadvertent disclosures of sensitive information to the public.

It was found from the study that 47.6% of members of the military from Nairobi based units stated that the security in Kenya is average. It cited that Kenya is still grappling in the dark as the monster of hatred spreads. Al-Shabaab has been using social media to send messages to Kenya and Kenya's inability to dilute the message before it reaches citizens shows instability in the Kenyan security. Furthermore, members of the military from Nairobi based units agreed that social media has contributed towards cattle rustling, poaching, terrorism attacks, tribal clashes, information warfare and hate speech. The study finally found that over recent years, the amount of cyber hate has grown to enormous proportions, with Islam, Jews, lesbians and gays, blacks, Roma, liberals and left-wingers representing the main targets of online abuse.

5.3 Conclusions of the Study

The study concludes that social media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members. It concludes that terrorist groups take advantage of Social Media to communicate with cyber-crime groups and to coordinate along with them fund-raising activities carried out in part or completely on the Internet. It concludes that social media are also used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, at throwing civil population into a panic. It was found that the military advised journalist to countercheck facts and the most convenient source was the Kenyan military who were often available for the press and put right facts as may have been said by Al-Shabaab. The study concludes that criminal organisations are threats on drug smuggling, human trafficking and money-laundering. It concludes that community criminal organizations like Mombasa Republican Council (MRC), '*Mungiki*' and '*Sungusungu*' use social media as a tool to recruit, communicate, spread propaganda and radicalization to a great extent. The study concludes that the military use social

media for communicating process of operation, boost morale of soldiers, clarify on propaganda messages sent by enemies & dispelling rumours, for updating civilians on progress of military operation, for public relations and operation Linda Kenya. It also concludes that the military uses Open-source intelligence (OSINT) collected to analyse social media threats. It concludes that counter propaganda is used by the military to counter social media threats. It concludes that the best news management comes from the military since they have a range of options for communicating their standpoint. The study concludes that security in Kenya is average since it is still grappling in the dark as the monster of hatred spreads. The study finally concludes that social media has contributed towards cattle rustling, poaching, terrorism attacks, tribal clashes, information warfare and hate speech.

5.4 Recommendations to the Study

The government through relevant agencies should closely monitor terrorist social media and conduct a variety of activities aimed at countering them. Although given the sensitivity of government programs responsible for monitoring and infiltrating social media suspected of supporting terrorism related activities, much of the information regarding the organizations/groups and their specific activities is deemed classified or law enforcement-sensitive and is not publicly available. However, security agencies should conduct covert operations on development, surveillance, and analysis of social media for purposes of attracting existing and potential jihadists searching for forums to discuss terrorism-related activities, or potential criminal activities threatening state and human security. But more importantly, government agencies should have cyber security responsibilities focused on policy development, public awareness campaigns, and intergovernmental and private sector coordination efforts to deal with these threats. Information gleaned from the agencies noted above may at times be used

to help inform and advise government entities responsible for safeguarding a geographic area or activity that has been targeted by terror groups.

The Government should construct and articulate a strategic, systematic and comprehensive 'big picture' of its use of social media intelligence, rather than allow a tactical and piece-meal one to implicitly emerge'. This Understanding of the first signs of hostile or potentially dangerous activity against a states security by violent organizations or groups can be beneficial in mitigating any disastrous consequences following the ability to pre-empt plans of the enemies, whether as hate speech, terrorism recruitment, training or any forms of extremism threatening national security.

Social media may introduce more transparency into the affairs of governments, the operations of belligerents and protesters, this openness can also have negative effects in the societies. There is a large amount of social media that may be harmful to peace, for example hate speech, propaganda, or mere misinformation. Hate speech needs to be regulated in societies, as in a manner that protects freedom of association, freedom of access to information and freedom of expression. Regulation on hate speech should not infringe on freedom of speech by censoring content except where absolutely necessary – when there is an imminent threat of violence, and there is a clear relationship between the hate speech and the threat of violence.

There is need to have data protection and privacy policies. In most developing countries, there is no contemporary data protection and privacy legislation and regulations related to internet and digital personal data, which may serve as guidelines. Data protection and privacy may be a matter of life and death, when users report violence or politically sensitive issues via mobile phones or the Internet. Data protection and privacy, information security, and operational

security are also essential for maintaining trust in any ICT platforms to make use of best practices in information security and data protection.

Security officers, just like general public cannot be expected to refrain from maintaining a social presence on the Internet. Therefore, as such, they should establish criteria for social media usage that balances the constitutional rights of officers while protecting the operations of military, intelligence or police agencies. There is need for the development and implementation of a comprehensive agency wide policy on social media use as a logical first step. This policy should be sufficiently broad to address the use of social media today and in the future as well as its opportunities and threats to national peace and security. Consideration must be given to protect the free speech rights of officers using their own computers or mobile phones. However, personnel who choose to provide information about their work on social media sites will be subject to scrutiny by the government. But this depends on the content shared on social media wherein it should not compromise either personal security or state security, regarding disclosure of sensitive security matters. Government entities can restrict the speech of their employees under certain circumstances, such as if the expression interferes with or compromises the operations of the agency or brings into question the professionalism of the officers or the agency. Social media policy should clearly delineate between protected free expression and the speech that could impact agencies or officers. Agencies generally are permitted to regulate officers' conduct on social media sites if the individuals list law enforcement as their occupation or post agency-related content. Administrators must decide the conduct and information to regulate, for instance photos or videos of officers, suspects, evidence, security facilities, equipment, uniforms, or weapons, Employment, job assignment, work hours, or other related information, Profanity or unprofessional language and harmful images, Work-related matters or other named officers in

posts, blogs, or micro-blogs and Personal social media activities while on duty and with agency resources. An agency's social media policy also should address the official purpose for use and the desired objectives. It should define the person or group authorized to create and maintain the social media presence on behalf of the agency. The policy also must provide guidance on what officers can share and when.

Training officers on social media guidance also in very important and it can be done in two steps. The first should address general computer, mobile, Internet, and social media security and privacy issues, while the second should look at the practical application of social media policy as related to officers. The training curriculum should be frequently updated and repeated to keep up with evolving technology and ensure the information remains fresh in officers' minds. Once educated, officers can take the initiative to properly protect themselves and their departments. Compliance can occur when officers understand the problem of social media on security and buy into the solution.

In relation to training, there is need for general public awareness campaign aimed at educating the public on the threats of the social media on the national security. Emphasis should be focused on the consequences of perpetuating on hate speech on legal basis. More important, the government should educate citizens on refraining on joining suspicious social media sites/ groups with extremist agenda and use social media responsibly.

Further, there is need for security apparatus to develop automated systems for collection and analysis of social media tailored to specific work environments. The availability of open source tools is not adequate in analysis of content of social media. Therefore research and development of social media analytic tools or pieces of software should be focused that are able to capture

data on social media feeds, filter it and analysis based on subjects of interest such as terrorism. The government should commit human and financial capital of research in the area of strategic communication and social Media. The military, in its efforts for counter propaganda on terrorism activities should develop a strategic communications as a process to synchronize efforts that will weaken an extremism credibility, misinformation and legitimacy as well as convince selected audiences to take specific actions that support kenya or international objectives.

REFERENCES

Abbot, C. Spencer. Presentation: "Humanitarian Intervention in Emergencies: Principles, Practices, and

Aday, S., Henry F., Marc L., and John S. (2010), Blogs and Bullets: *New Media in Contentious Politics. Peaceworks,* no. 65 (2010). P.11.

Albert L. (2006), First Informers in the Disaster Zone: *The Lessons of Katrina. Washington*: The Aspen Institute,

Andrew, H. (2009). Meeting Somalia□s Al-Shabaab, BBC news, July 3.

Berkman, R., & Shumway, C. (2003), Digital dilemmas: *Ethical issues for online media professionals*. Ames: Iowa State Press.p 5

Blitzblau S. (2011), Analisitecnicadellecapacità di NetINTdeigruppiterroristici, *Information Warfare Conference 2010,* Franco Angeli, Milano.

Bowman-Grieve L., (2010), A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment, Euro ISI Conference Submission, Leeds.

Brelsford, P. (2013), Employing a social media monitoring tool as an OSINTplatform for Intelligence,Defence& Security

Burson-Marsteller, N. (2011), *The Global Social Media Check-up 2011*, New York.

Campobasso, P. (2011), Le nuovesfideallasicurezzadellospaziocibernetico, *Information Warfare Conference 2010,* Franco Angeli, Milano.

Carafano J. C. (2009), *From Social Networks to National security*. Australia Policy Institute p.3

Castillo, C., Mendoza, M., & Poblete, B. (2011), Information credibility on twitter. *Proceedings of the 20th international conference on World wide web - WWW* '11, 675. doi:10.1145/1963405.1963500

Catone, J. (2010), *Developers Band Together to Create Apps for Haiti*. Mashable.

Chadwish, A. (2006), *Internet Politics*: States, Citizens and New Communication Technologies. NY: Oxford University Press, 2006.p.11.

Chief Information Officers Council (CIO), (2009), Guidelines…cit.

Clay, S. (2008), Here Comes Everybody: *The Power of Organizing Without Organizations* (New York: Penguin Books, p. 28.

Cleveland, W. L., and Martin, B. (2009), *A History of the Modern Middle East*. CO: Westview Press, pg 88

Cragg, J.(), *U.S. Military's Medical Role in Haiti Declines.* American Forces Press Service. US Department of Defense, (2010), *Emerging Media, Defense Media Activity*.

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

Dale, H. C., (2009), *Public Diplomacy 2.0*: Where the U.S. Government Meets "New Media", Backgrounder n. 2346 – published by The Heritage Foundation, Washington, DC.

Davies, C. (2011), *Yemen's Tribes 'Put Differences Aside' to Protest for Change*. CNN World. Defense Advanced Research Projects Agency (Darpa), (2011), *Social Media*…cit.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), Stories, Neuroscience and Experimental Technologies: *Analysis and Decomposition of Narrative in Security Contexts*, DARPA-SN-11-20, Arlington County, VA.

Dinan, W., & Miller, D. (2007), Thinker, faker, spinner, spy. London: Pluto.

Dozier, K. (2011), Exclusive: *CIA following Twitter, Facebook, Associated Press*, New York.

E. Barsky and M. Purdon, (2006), Introducing Web 2.0: Social Networking and Social Bookmarking for Health Librarians, *Journal of Canadian Health Librarian Association*, Vol. 27, p. 65)

Emanuela, D. (2011), La Rete, strumento di partecipazione, mobilitazione e lotta, Gnosis – RivistaItaliana di intelligence, vol. 2, Roma.

Evan H. P. (2009), Branding Canada: *Projecting Canada's Soft Power Through Public Diplomacy*, McGill-Queen's University Press, P. 58

Fogel, J., & Nehmad, E. (2009), Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behaviour*. Pg 153

Forrest, B. (2010), *Technology Saves Lives In Haiti*. Forbes. February 1, 2010. Accessed Febrary 4, 2010.

Gabriel, W. (2006), Terror on the Internet: *The New Arena, the New Challenges* (Washington, D.C., United States Institute of Peace Press, (2006), pp. 37-38.

Gamson, W.A., Wolfsfeld, G. (1993), Movements and Media as Interacting Systems. *Annals of the American Academy of Political and Social Science*: Citizens, Protest, and Democracy. 528, pp.

Gelao, N., (2011), Cyber Warfare: unnuovofronte per le Forze Armate, *Information Warfare Conference 2010*, Franco Angeli, Milano.

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).

Google Crisis Response, (2014), *National Security and Crisis Response Map*. Accessed on 2014.

Guadin, S. (2010), Facebook creates site dedicated to providing crisis info. *Computer World*. January 15, 2010.

Hall, L. (2006), *Capers in the churchyard. Darien*, CT: Nectar Bat Press.

Hallin, L. (2004), Analysed the media coverage of the conflict and concluded that initially the media was very supportive and only changed its stance on the Vietnam War after the public opinion had turned sour.

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

Hasni, A. (2012), Hacker group Anonymous claims attacking Greek official websites' As seen in The News Tribe, 9 October 2012, viewed on 29 November 2012.

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

Howe, J. (2008), Crowdsourcing: *Why the Power of the Crowd is Driving the Future of Business.* New York: Crown Business, 2008.

Human Rights Watch, (2012), Criminal Reprisals: *Kenyan Police and Military Abuses against Ethnic Somalis*.

Hughes, A. (2009). Twitter adoption and use in mass convergence and emergency events IGCRAM.

Intelligence And National Security Alliance, (2011), Cyber Intelligence: *setting the landscape for an emerging discipline*, Arlington, VA.

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.

James, J. C. and Andrew G. (2007), Nanotechnology and National Security: *Small Changes, Big Impact*, Heritage Foundation Backgrounder No. 2071, September 21, 2007.

JONES S. G. (2011), Awlaki's Death Hits al-Qaeda's Social Media Strategy, *RAND Corporation*, Santa Monica, CA.

Kamalipour, Y. & Snow, N. (2004), *War, media, and propaganda. Lanham, MD*: Rowman and Littlefield.

Kirkpatrick, D. (2011), *The Facebook Effects*. Oaks Publishers NY

Kishan, S. (2011), 21st Century Diplomacy A Practitioner's Guide, The Continuum International Publishing Group, p. 88

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

Amaral, L. A. N. and Ottino, J. M. (2004), Complex Networks: Augmenting the Framework for the Study of Complex Systems, *The European Physical Journal* (May 14, 2004), pp. 147–162,

Lakhous A. (2011), La Rete, strumento di partecipazione, mobilitazione e lotta, Gnosis – *RivistaItaliana di intelligence*, vol. 2/2011, Roma.

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

Lerner, M. (2010), Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt. *Journal of Muslim Minority Affairs* 30 no. 4 (2010): 557.

Lindgren, S. and Bandhold, H. (2009), Scenario Planning: *The Link between Future and Strategy*, 164–165.

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.

Lynda, P. (2012), *Utilising Social Media to Further the Nationwide Suspicious Activity Reporting Initiative*, Masters Degree Disseration, Calhoun University

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

Manjoo, F. (2004), *A Picture is no Longer worth a Thousand Words*

Mayfield, T. D. (2011), *A Commander's Strategy for Social Media*, Joint Force Quarterly vol. 60/2011, National Defence University, Washington, DC.

Mbũguawa, M. G. M. & Gona G. (2010), Remembering Kenya. Identity, *Culture and Freedom*, published by Twaweza Communications Ltd. Westlands Nairobi Kenya p.166.

McAdam, D. and Ronnelle, P. (1993), Specifying the Relationship between Social Ties and Activism. *American Journal of Sociology 99, no. 3 (1993): 642*.

McAdam, D., Sidney T. and Charles T. (2008), Methods for Measuring Mechanisms of Contention. Qualitative Sociology 31, no. 4 (2008): 310.

Mendoza, M., Poblete, B. & Castillo, C. (2010), Twitter Under Crisis: *Can we Trust What we RT*, KDD Workshop on Social Media Analytics, 2010

Middleton, M., (2008), The RCTV Cliff hanger: *Flagging social responsibility in the media*, Visages d'Amérique latine, Sciences.

Montagnese, A. (2012), *Impact of social media on National Security*, Published MA Thesis. University of Rome. P 2

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

Moskos, C. C. (2000), *The Media and the Military in Peace and Humanitarian Operations*." Special Report, Cantigny Conference Series, Robert R. McCormick Tribune Foundation, Chicago, 2000 pg 321

NATO Allied Command Transformation, (2009), Multiple Futures Project –*Navigating Towards 2030*, Norfolk

NATO Doctrine on Psychological Operations AJP 3.10.1. SHAPE (2007), page 1 – 6. NATO UNCLASSIFIED.

Neumann, J. (1996), *Lights, camera, and war: is media technology driving international politics?* New York: St. Martin's Press.

O'Reilly, T. (2005) What Is Web 2.0. September 30, 2005. Accessed March 2, 2010. *http://oreilly.com/web2/archive/what-is-web-20.html*

Obama, B. (2009), *Memo on Transparency and Open Government.* Office of the Deputy Secretary of Defense, Directive-Type Memorandum 09-026, Responsible and Effective Use ofInternet-Based Capabilities.

Olimpio, G. (2011), Twitter osservato specialedella CIA, Corrieredella Sera, Milan.

Papic, M., & Noonan S. (2011), *Social Media as a Tool for Protest, STRATFOR*, Austin, TX.

Pedde, N. (2011), La crisilibica, e le differenze con le rivolte in Tunisia ed Egitto, InformazionidellaDifesa – SMD, n.2/2011, Roma.

Perspectives. Georgetown University Center for Peace and Security Studies. April 13, 2010.

Peter Schwartz, The Art of the Long View: Planning for the Future in an Uncertain World (New York: Currency Doubleday, 1991), 36.

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.

Ramacciotti, S. (2011), La sicurezzadelleinformazioni al tempo di Wikileaks, InformazionidellaDifesa – SMD, n. 3/2011, Roma.

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

Rollins, J. (2011), *Al Qaeda and Affiliates*: Historical Perspective, Global Presence, and Implications for U.S. Policy, Congressional Research Service, and Washington, DC.

Rosenberg, S. (2009), *Say Everything*: How Blogging Began, What It's Becoming, and Why It Matters. New York: Crown Publishers, 2009.

Safko, L. and Brake, D. (2009), *The Social Media Bible*: Tactics, Tools, and Strategies for Business Success. Hoboken, NJ: John Wiley & Sons, 2009.

SANS Institute, (2011). Reducing the risks of social media to your organization: Online watchman

Saunders, M., Lewis, P. & Thornhill, A. (2009), *Research Methods for Business students*. FT Prentice HQ, India p 66.

Scherer, M. (2011), Can They Win, One Tweet at a Time? , Time. State of California, Office of the State Chief Information Officer.

Shuchman M. & Wilkes, M. S. (1997), Medical Scientists and Health News Reporting: *A Case of Miscommunication*. Volume 126 Issue 12, Pages 976-982.

Stoler, P. (1986), *The War Against the Press*: Politics, Pressure and Intimidation in the 80□s. (New York: Dodd, Mead & Cog 99.

Surowiecki, J. (2004), *The Wisdom of Crowds*. New York: Doubleday, 2004.

Sydney Morning Herald, 'Every Click They'll Be Watching' 12 July 2012, viewed 29 November 2012.

Taylor, D. (2011), Social Media Targeted by Pentagon for Strategic Communication, Infowars, website:http://www.infowars.com/social-media-targeted-by-pentagon-for-strategic-communication.

The Guardian (UK), (2012), Kenyan Muslims Fear the Worst Over Proposals to Boost Police Powers.

Thomas, K., Grier, C. & Nicol, D. M. (2010), Unfriendly: Multi-party Privacy Risks in Social Networks, in Privacy Enhancing Technologies, eds. Atallah, M.J., Hopper, N.J., Lecture Notes in Computer Science, Springer Berlin / Heidelberg.

Tilly, C. (2011), *Describing, Measuring, and Explaining Struggle*. Qualitative Sociology 31, no. 1 (2011): 2

UN Counter-Terrorism Implementation Task Force, (2011), *Use of the Internet to Counter the Appeal of Extremist Violence, Conference Summary*, Riyadh.

Ungerer, C. (2012), *Social media and national security*, ASPI Strategic Policy Form, 27 February 2012, p1.

US ARMY, 304th Military Intelligence Battalion, (2008), Sample Overview: al Qaida-Like Mobile Discussions & Potential Creative Uses, Fort Huachuca, Arizona.

US Joint Publication 3-13.2. Psychological Operations, 07 January 2010, page V-2 can be found on: http://www.fas.org/irp/doddir/dod/jp3-13-2.pdf

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.*

Wanner, G. (2011), *Risks of social media to organizations*: Oaks publishers UK. P 64

Webster, K. L. (2010), Lessons From a Military Humanitarian in Port-au-Prince, Haiti. *Small Wars Journal.* March 28, 2010. 2.

Weinberger, S. (2011), The Spy Who Tweeted Me: *Intelligence Community Wants to Monitor Social Media*, Wired, San Francisco.

Weng, J., & Christopher W. J. (2010), Twitter Rank: Finding Topic Sensitive Influential Twitterers’ WSDM 10, February 2010

Williams, F. (2008), Sociological *impact of social media*: Oxford Press, U.K.

Wolfsfeld, G., (2004), *Media and the path to peace*, Cambridge, Cambridge University Press.

Zinzocchi, R. (2009), *Da Facebook a Twitter vogliamolasciaretracce*, Il Tempo.

APPENDICES

SOCIAL MEDIA AND NATIONAL SECURITY THREATS: CASE STUDY OF KENYA

My name is Julius Kimutai, a student at the University of Nairobi, undertaking a master's project in International Relations. It is the University requirement that I undertake a project for me to finish my course work. I have chosen you to be part of my respondents. Kindly feel free to provide information and I assure you that it will be treated as private and confidential and will only be used for academic reasons.

Appendix One: Questionnaire for Military

Instructions

Kindly respond to the questions as honestly as possible.

Tick (√) inside the box to indicate your choice of answer.

Section One: Threats of Social Media

1) Is social media a threat to national security Yes [ ] No [ ]

2) Do you agree that social media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members?
   Yes [ ] No [ ]

3) If yes, to what extent do you agree that terrorists use social media as a tool for ideological radicalization, recruitment, communication and training? Use a five point scale provided in the table below.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Ideological radicalization					
Recruitment					
Communication					
Training					
Threats of violence					

4) Criminal organizations are threats to national security. To what extent do you agree they use social media to conduct their criminal activities?

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Spread of viruses					
Trojans					
Drug smuggling					
Human trafficking					
Money-laundering					
Spreading child pornography with fee					

5) Given the community criminal organizations like Mombasa Republican Council (MRC), '*Mungiki'* and '*Sungusungu'*, To what extent do they use social media as a tool to recruit, communicate, Spread propaganda and radicalization.

	Very great extent	Great extent	neutral	Low extent	Not at all
Recruit					
communicate					
Spread propaganda					
Radicalize youths					
Any other_____					

Section Two: Military use of Social Media for National Security

6) Does military use social media for military operations?

Yes { } No { }

7) If yes, specify

1._____

2._____

3._____

8) Are there officers whose job functions include spending time on social media sites to monitor any security threat that spreads around?

Yes ☐ No ☐

9) Do you have tools that helps in the analysis of social media threats to national security?

Yes [ ] No [ ]

If yes, which ones?

_____

_____

_____

10) To what extent does the military use the following mechanisms to counter threats of social media to national Security?

	Very great extent	Great extent	neutral	Low extent	Not at all
Counter propaganda					
Public diplomacy					
Open source intelligence					
News					

Any other_____					

11) How frequent has there been incidences in the military of inadvertent disclosures of sensitive information?

Not at all ☐ Slight Frequency ☐ Somewhat Common ☐

Common ☐ Very Common ☐

Section Three: Kenya's Current National Security

12) How do you rate the current state of Kenya's national security with regard to threats from social media?

Excellent [ ] Above Average [ ] Average [ ]

Below Average [ ] Extremely Poor [ ]

13) To what extent does the following insecurity in Kenya been contributed by social media?

	Very great extent	Great extent	neutral	Low extent	Low
Terrorism attacks					
Hate speech					

Poaching					
Information warfare					
Tribal clashes					
Cattle rustling					
Any other_____					

14) Give three suggestions of how to protect ourselves against offensive use of social media and improve on our security situation.

_____

_____

_____