

UNIVERSITY OF NAIROBI



DEPARTMENT OF DIPLOMACY AND INTERNATIONAL STUDIES

**EFFECTS OF THE AL-SHABAAB MOBILE AND ONLINE FUNDINGS ON KENYA'S
COUNTERTERRORISM MEASURES**

WILFRIDA ATIENO OMOLO

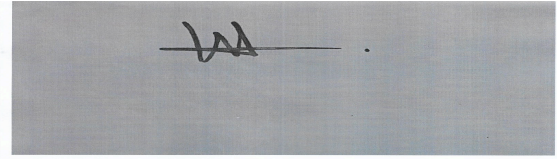
REG. NO.: R47/38595/2020

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF POST GRADUATE DIPLOMA IN
STRATEGIC STUDIES, UNIVERSITY OF NAIROBI**

2021

DECLARATION

I declare that this project is my original work and has not been presented to any university for award of any other degree.

Signature 

Date **25.11.2021**

NAME: Wilfrida Atieno Omolo

REG No.: R47/38595/2020

This research project has been submitted for presentation with my approval as supervisor.

Signature..... 

Date . **25TH NOVEMBER 2021** ..

Supervisor: Dr. John Lekuton

DEPARTMENT OF DIPLOMACY AND INTERNATIONAL STUDIES

UNIVERSITY OF NAIROBI

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
FTF	Foreign Terrorism Financing
NIE	National Intelligence Estimate
TF	Terrorism Financing
UG	Union of Good
VC	Virtual Currenc

ACKNOWLEDGEMENT

First, my sincere gratitude to my supervisor Dr. John Lekuton who dedicated his time and expertise to ensure that my research meets the standards it deserves to meet the minimum requirements for the award of Post Graduate Diploma in Strategic Studies in the International Studies to the Department of Diplomacy and International Studies (IDIS). His guidance and constructive feedback made this research a success.

I am greatly indebted to my colleagues and course mates of Grade 2 staff course, No. 36-2020/2021 whose involvement in this research has left me with a wealth of experience.

I extend my utmost gratitude to my dear husband, Geoffrey Amuhaya and my two children Gabriel and Yvette whose immense love and support gave me the courage and strength to face the challenges I went through in the course of this research.

Finally, I thank God Almighty who has been my shield and source of strength in everything I did.

DEDICATION

This work is dedicated to my children who motivated and gave me the reason to pursue further studies and a reminder to them on the practicality of understanding that hard work leads to success.

ABSTRACT

Al-shabaab extensive use of online platforms for purpose of funding their activities is a threat to the efforts to counter terrorism. The calculated use of social media where many donors participate, resulting in significant amounts, in a well-organized and wide-ranging attempt to collect extremist funding is challenge to the combined efforts by various organisations to thwart terror growth. While Kenyan security forces have been working together in the development of rigorous counter-terrorism policies to fight funding of mobile and online extremism, there has been little research on how effectively counter-terrorism methods are to deter Internet-based funding of terrorism activities. The competition between counterterrorism efforts and the expanding terrorism funding is a worrisome trend. The study aims to examine Al-Shabaab's mobile and online funding schemes in Kenya, to evaluate the impact of Al-Shabaab's mobile and online money funding schemes on counterterrorism measures in Kenya and to assess the counter-terrorism strategies that can be used to prevent Al-Shabaab's mobile and online money funding schemes in Kenya. The study will use the Identity Politics Theory to explain the relationship between terrorism funding scheme (mobile and online funding) and terrorism. The study will also use secondary data from library sources i.e. books, e-books, government publications, journals, magazines, and newspapers for content analysis. The study will be beneficial to security agencies, policy makers, the government and the Kenyan allies in the fight against terrorism. The research findings will help the security agencies to enhance their strategies by enacting policies that will require online payment platforms and Internet pages to develop stringent measures and report any suspicious activities. Also the Kenyan government and its allies will be able to enact policies that will restrict online money platforms from dealing with suspicious consumers, which will help prevent transfer of money across terrorist networks.

TABLE OF CONTENTS

DECLARATION	i
LIST OF ABBREVIATIONS	ii
ACKNOWLEDGEMENT	iii
DEDICATION	iv
ABSTRACT	v
CHAPTER ONE: INTRODUCTION AND BACKGROUND OF THE STUDY	1
1.1 Introduction	1
1.2 Background of the Study	2
1.3 Problem Statement	7
1.4 Research Questions	8
1.5 Research Objectives	8
1.6 Literature Review	8
1.7 Theoretical Framework	22
1.8 Research Hypothesis	25
1.9 Justification of the study	25
1.10 Research Methodology	26
1.11 Study Limitations	26
1.12 Chapter Outline	26
CHAPTER TWO: AL-SHABAAB MOBILE AND ONLINE FUNDING SCHEMES IN KENYA	27
2.0 Introduction	27
2.1 Al-Shabaab Funding Schemes	27
2.2 Methods Used by Al-Shabaab to sustain Funding schemes	28
2.3 The Benefit of Funding schemes to Al-Shabaab	29
2.4 Challenges faced by Al-Shabaab	29
2.5 Conclusion	30
CHAPTER THREE: THE IMPACT OF AL-SHABAAB'S MOBILE AND ONLINE MONEY FUNDING SCHEMES ON COUNTERTERRORISM MEASURES IN KENYA	31
3.0 Introduction	31
3.1 High Levels of Illicit Financial Flows as a Blow to the AML and CFT	31

3.2 Using Economic Incentives to Beat Kenya’s Efforts to Rehabilitate Youth from Violent Extremism	33
3.3 Increased Radicalization	36
3.4 Conclusion.....	37
CHAPTER FOUR: COUNTER-TERRORISM STRATEGIES THAT CAN BE USED TO PREVENT AL-SHABAAB’S MOBILE AND ONLINE MONEY FUNDING SCHEMES IN KENYA	38
4.0 Introduction	38
4.1 Introducing Legal Measures to Guide Online Financial Companies	38
4.2 Uses of the Internet to Counter Terrorist Activities.....	40
4.3 Developing Operational Cybercrime units.....	41
4.4 Establishing Computer forensic triage units	43
4.5 Training Counter-Terrorism Units	45
4.6 International cooperation.....	46
4.7 Conclusion.....	48
CHAPTER FIVE: SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS.....	49
5.0 Introduction	49
5.1 Summary of Key Findings	49
5.2 Conclusions	51
5.3 Recommendations	51
REFERENCES.....	53

CHAPTER ONE

INTRODUCTION AND BACKGROUND OF THE STUDY

1.1 Introduction

Terrorist groups have not only used the Internet to spread and attract propaganda, but also to finance the organisation. The Islamic militant groups, Al Qaeda, Hamas, Lashkar Taiba, Hezbollah, and Al Shabab have used the Internet for the purposes of collecting and sending money to financing their operation.¹ The Internet offers a broad reach, timely efficiency, as well as a certain degree of anonymity and safety for jihadist organisations, both donors and beneficiaries. This fact provides an avenue for the terrorist organization to use the internet platform for financial activities. Unfortunately, while many lawmakers acknowledge that the Internet is being made a more efficient platform for terrorist groups, there are conflicting responses to such threats.² This collection and movement of money by a donor to a recipient lead to terrorist funding (TF) and foreign terrorist funding (FTF).

The concept of terrorist funding and foreign terrorist funding has made Kenya and its counter-terrorism allies rethink their strategy in addressing and handling terrorism activity. In an article by The East African of 19th January 2020 titled Al-Shabaab attacks challenge counter terrorism strategies, it states that the group has been setting up at least two attacks every week in Kenya and Somalia for the last three months. It further states that the group had been dormant between 2012 and 2015 but regrouped and are carrying out ambushes to maintain their connection with people who share in their ideas or statements that are either false or exaggerated.

¹ Cohen-Almagor, R. (2017). "Jihad online: How do terrorists use the Internet?" *Media Metamedia Management*, 55-66.

² Neumann, P. (2015). "Remarks on Terror on the Internet. The White House Summit to Counter Violent Extremism," Washington DC (February 19).

It is upon this background that the study seeks to examine the effectiveness of counterterrorism strategies on thwarting Internet use for terrorism activities, more so funding, using Kenya counterterrorism against Al Shabaab as a case study.

1.2 Background of the Study

Terrorist organizations have used the omnipresent availability of the internet and its anonymity to gather and find financial assistance from people all over the world, in particular the exponential increase in networking.³ Terrorism organizations often use social media to spread their message to supporters around the world. Through social media, many western and European FTFs are living their war zone experience. Rather than according to the official accounts of insurgent organisations, the majority of this "FTFs" turn to the "disseminators" for and collect data on combat. These disseminators are not formally associated with a militant organization but sympathize with ideologies and actively participate financially in the conflict. This has damaged the capacity of terrorist organizations to control the narrative leaving the private parties to have an influence on how those concerned see war.⁴

Terrorists also organize fundraising activities via social media. Many of the donors will participate, resulting in significant amounts, in well-organized and wide-ranging attempts to collect extremist funding. Terrorist organizations have reached a wide audience with horizontal peer-to-peer networking, starting from chat and forums and continuing through social media platforms like Twitter, Facebook, Instagram as well as instant messaging apps like Viber and

³ AUSTRAC (2014), "*Terrorism financing in Australia 2014*," Commonwealth of Australia, West Chatswood, Australia, www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf.

⁴ Ibid.

WhatsApp and secure communication networks such as VoIP and Surespot. Donors are a demographic focus of users compared to desirable social media FTFs.⁵

A modern challenge of terrorism finance is often the use of well-coordinated crowdfunding platforms. Crowdfunding is defined as a way to raise money from multiple individuals by means of donations or investments for businesses, organizations or individuals allowed by Internet. Via crowd funding online platforms you can easily create a funding page and receive donations.⁶ Crowdfunding is nevertheless vulnerable to abuse for unlawful purposes, even where it disguises the true purpose of the financing effort. Via charities and humanitarian activity, persons and organizations seeking to fund terrorist and extremist recruitment may be able to form NPOs. Donors did not realize the end use of crowdfunding and social media funds in certain cases." In addition to sourcing for resources for TF purposes, crowdfunding strategies could be used to avoid managed financial institutions by transferring money abroad.

Genuine reasons have generated broad social media programs for supporting donations and followers of appeals. Fake NPOs, individuals or organizations who seek to raise funds for terrorism and extremist financing could, according to the study, try to cover up their acts by pretending to engage in legitimate charitable activities or humanitarian activities and could set up NPOs for those purposes.⁷ In the guise of humane aid or outright assistance, contributions should be made. The collection of funds may be done using traditional crowdfunding or social media approaches.

⁵ Carter, J.A., Maher, S. and Neumann, P.R. (2014), "*Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*," Inter

⁶ CGTF (nd), "Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists," CGTF, <https://www.thegctf.org/documents/10162/159874/Algiers+Memorandum-English.pdf>

⁷ US Department of State (2015), "*Counter-ISIL Finance Group Kidnapping for Ransom Communiqué*," US Department of State, Washington.

The raised funds are usually used to finance "mobile touch FTF payments, air fares and other products and services purchased over the internet, or serve as operational funds for a terrorist attack." However, a number of situations have shown that social networking and crowdfunders are unaware of the ultimate destination of the funds. There are, for example, investigations into the use of disappointing crowdfunding campaigns by jihadist radicals to raise funds.

Much of the social media platforms that extremists use offer funding to terrorist organizations and supporters to collect terrorist funds.⁸ Research has however proved that the owners of these platforms are more often than not, not aware of the end users intent. Once known, these networks usually either close or block these sites. Websites like Twitter have augmented their efforts to bring down accounts that are critical to terrorist propaganda distribution in the second half of 2014. To attract more people, online fundraisers may utilise various instruments and systems of payment to collect money common a number of potential sponsors.⁹ those conducting fundraising activities may use social media to promote finance transactions such as exchanges of information on prepayment cards, credit card numbers and account ID.

The use of virtual currency (VC) by terrorist organizations has posed a great challenge to security agents. Several pages linked to terrorist groups have raised Bitcoin donations worth millions of dollars. In addition, the law enforcers have pointed out discussions on the Internet between extremists on the utilisation of VC to acquire arms and educate those who are yet to be savvy to use the platform. For instance, an ISIL-affiliated blog post suggested that Bitcoin be used to finance terrorist international activities.¹⁰

⁸ CGTF (nd), "Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists," CGTF, <https://www.thegctf.org/documents/10162/159874/Algiers+Memorandum-English.pdf>

⁹ Ibid.

¹⁰ Ibid.

Clients using payment procedures based on the Internet have access to pre-financed accounts to "move the electronic money or value deposited into those accounts to other people or businesses who previously have accounts with the same company."¹¹ One of the most common payment systems online is for customers using 'online auction shopping' pre-funded accounts. In order to authorize a transfer of money, beneficiaries should not be obliged to give their details to the platform service provider. A variety of extremist allegations are linked by online payment sites such as PayPal with many low-valuation TF events.' Though a possibility it is unclear if these transfers have been used to finance terrorism.¹²

Terrorist offenders are using guest accounts as well as authenticated identities for online purchases.¹³ Payments tend to be linked, rather than direct payments for the financing of terrorist events, to the Internet sales of equipment and clothes before the departure of persons traveling to war zones. The use of online payment structures is shocking given the ages of the majority of terrorist suspects and their familiarity with internet shopping.¹⁴ Customers between the ages of 21 and 35 are exposed to the bulk of the reports that show suspicious financial transactions linked to violence. According to the report, utilizing digital payment facility to help finance activities related to terrorism is a clear indication such virtual platforms are widely used by terrorist groups to promote their funding agenda.¹⁵

Even though online media is now the most common means used for the passive enlistment of future jihadists, conventional approaches such as publications of indoctrination and leaflets,

¹¹ Oftedal, Emilie (2015), "*The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment (FFI)," Norway, 6 January, 2015, www.ffi.no/no/Rapporter/14-02234.pdf

¹² Ibid.

¹³ Ottawa Citizen (2014), "ISIL using social media to lure young teenagers, accountants, engineers to its cause" (David Pugliese), Ottawa Citizen, Ottawa, December 16.

¹⁴ Ibid.

¹⁵ Ibid.

regular meetings and the broadcast of particular programs continue to be used.¹⁶ The monthly Dabiq ISIL, published on the Web since 2014 and based on Inspire's Al Qaeda magazine, is an example of this combination of conventional methods and modern means of communication. Passive recruitment services and supplies are subject to fixed costs and may require continued financial support and investment.¹⁷

While websites and social media accounts can be created, social media can be used free of charge, a variety of terrorist groups produce high-quality content which may require sophisticated and specialized equipment.¹⁸ Because of "the size and variety of means of distribution" the material can also be disseminated by many bloggers and editors. Recruitment on the Internet is frequently linked to requests for financing and other types of terrorist assistance.¹⁹ Recruiters and persons use the same tools for recruiting and raising funds for "extremist propaganda. Terrorist organizations use passengers and Internet chat groups to spread disinformation on their own, but often share confidential details, like bank accounts, and real charitable donation intentions."²⁰

The helpers and supporters are drawn by contemporary technologies, particularly social media. As previously reported, online recruitment is also related to requests for financial support from jihadists.²¹ Facile delivery and small donation opportunities would draw supporters, contribute to fund-raising and increase the ideological support of the terrorist group. Those organizations

¹⁶ Telegraph (2014), "How ISIL is funded, trained and operating in Iraq and Syria" (Harriet Alexander and Alistair Beach), August 23, 2014.

¹⁷ Ibid.

¹⁸ Sanchez-Franco, M. J. (2010). "WebCT—The quasimoderating effect of perceived affective quality on an extending Technology Acceptance Model." *Computers & Education*, 54(1), 37-46.

¹⁹ Ibid.

²⁰ Ibid.

²¹ Keatinge, Tom (2015), "Identifying Foreign Terrorist Fighters: the role of public-private partnership, information sharing and financial intelligence, Royal United Services Institute (RUSI)," United Kingdom, July 2015.

also employ persons involved in the funding of terrorist acts to participate later in violent activity.²² Crowd loan and crowd finance are legitimate methods in which funds can be collected through the internet. They enable a wide range of people, via direct messaging systems, to communicate directly or through third parties. Terrorist organizations may use such sites for terrorist purposes, including for the movement of foreign terrorist fighters. The aim of this study was to investigate the effects of Al Mobile Shabaab's online funding on Kenya's counter-terrorism efforts.

1.3 Problem Statement

Since September 11, the world over increased its spending on counter-terrorism to deal with the evolving nature of terrorism activities. On the other hand, terrorist groups also enhanced its funding capability by expanding and establishing other means of funding to include the use of mobile and online fundraising connections. As near ally to the United States, Kenya has been a victim of terrorism for several years. The latest examples are the Westgate Mall attack, the Garissa University assault and the DusitD2 Complex attack. Al Shabaab, the largest aggressor, has heavily invested in the internet to fund its service, to spread even poisonous tweets as the government attempts to close down any gaps in terrorist attacks. While Kenyan security forces have been working together in the development of rigorous counter-terrorism policies to fight funding of mobile and online extremism, there has been little research on how effectively counter-terrorism methods are to deter Internet-based funding of terrorism activities. Where the vulnerability in the fight against terrorism can be identified without considering existing counter-terrorism policies, notably mobile and online financing. As a consequence the impact on Al-

²² Ibid.

Shabab smartphone and online finance links in Kenya should be studied particularly the terrorist groups' financing systems.

1.4 Research Questions

1. How widespread is Al-Shabaab's mobile and online funding schemes in Kenya?
2. What is the impact of Al-Shabaab's mobile and online money funding schemes in Kenya?
3. What are the counter-terrorism strategies that can be used to prevent Al-Shabaab's mobile and online money funding schemes in Kenya?

1.5 Research Objectives

1.5.1 Broad Objective

To examine the effects of the Al-Shabaab mobile and online fundings on Kenya's counterterrorism measures.

1.5.2 Specific Objectives

1. To examine Al-Shabaab's mobile and online funding schemes in Kenya
2. To evaluate the impact of Al-Shabaab's mobile and online money funding schemes on counterterrorism measures in Kenya.
3. To assess the counter-terrorism strategies that can be used to prevent Al-Shabaab's mobile and online money funding schemes in Kenya.

1.6 Literature Review

1.6.1 Terrorist Groups Mobile and Online Funding Schemes

The use of online networks by terrorists for financial drives has been increasing since 11 September. Terrorist groups have been using networks to fund their activities before, however,

this became more apparent after the broader public and the US government started investigating the 9/11 attacks. The most influential example was Babar Ahmad, young South London-based British citizen, who put his programming skills to use at an early stage for the jihadist cause.²³ Azzam Publications and related web pages were founded in 1997 by Babar, which aimed primarily to support the Taliban in Afghanistan and the Chinese Mujahides. Babar requested donations, tried to recruit troops and provided detailed advice on how funding and recruits could reach these war zones.²⁴ The website's purpose was clearly specified. Babar wrote on a questionnaire and a response to the question: Azzam Publications were established to spread the Jihad call between the Muslims, who do not know the basic obligation. Consequently, as explained the aim of Azzam Publications was to inspire the faithful" and "to share some funding for the brothers." In response to an extradition request from the United States, the UK detained Babar in 2004. Appeals are still pending against the extradition request of Babar.²⁵

In his website, Babar used a familiar argument that persons should donate and that it was the responsibility of every Muslim to join the jihad in every way. Whereas an individual did not go to the jihad contest, Babar wrote that the individual had a moral duty to donate money, noting that the most crucial thing that those subscribing to Islam faith can do in the Western world is give out money and help collect from other sources, including relatives and families. For those who are unable to fight for a just cause, they have to raise and donate money.²⁶

²³ US Department of State (2015), "*Counter-ISIL Finance Group Kidnapping for Ransom Communiqué*," US Department of State, Washington.

²⁴ Ibid.

²⁵ US Department of Treasury (2015), "*United States National Terrorist financing risk assessment*," US Department of Treasury," Washington, United States.

²⁶ Oftedal, Emilie (2015), "*The Financing of Jihadi Terrorist Cells in Europe*," Norwegian Defence Research Establishment (FFI)," Norway, 6 January, 2015, www.ffi.no/no/Rapporter/14-02234.pdf

Samy al-Hussayen, a doctoral Saudi student at Idaho State University, was the terrorist website webmaster before 9/11. According to the report, the location of al-Haramain, a Saudi-based NGO later called by the US Department of Finance for its ties to Al Qaeda. These pages contained lectures and speeches in Israel on the issue of armed jihad. On his website platform, participants were invited to donate money against the dictatorial Zionist Jewish organization in their noble jihad to help their brothers and sisters in a special forum. In 2003, Al Hussayen was charged with the offense of supporting Hamas and on the grounds that he had a clear intention of using his computer skills and tools to gain and finance violent jihad activities in Israel among other places.

Terrorist groups have increased their internet use since 9/11 to enhance the operations and objectives of their organisations. Much Internet use has been centralized into recruiting, recruitment and education, by the terrorist organization with the aim of reaching a wider audience the world over.²⁷ The number of web pages connected to al-Qaeda stepped up from twelve in 1998 to about 2,600 in 2006. A number of various terrorist organizations have websites or have actively used the Internet at some stage.²⁸ In the 2006 “National Intelligence Estimate (NIE),” the USA government predicted that terrorist will not only use the internet to try and hire new people, but also use it to raise money to keep their organizations afloat. The NIE cautioned that logistical and financial support would ultimately be available online from all forms of organizations. More broadly, technology and globalization not only have enabled the connection

²⁷ Sanchez-Franco, M. J. (2010). “WebCT–The quasimoderating effect of perceived affective quality on an extending Technology Acceptance Model.” *Computers & Education*, 54(1), 37-46.

²⁸ Ibid.

of small groups of disgruntled people, but also the raise of funds for terrorist attacks by individuals or groups who are not affiliated to any existing terrorist organization.²⁹

Criminal activities is also seen as a source of funding for Internet-based terrorist groups. Recent cases are that of Younis Tsouli, one of British young people best known for being Irhabi, the most renowned cyber terrorist. Evan Kohlman, a well-known terrorism expert, said that he was an indiscriminate king over just two years of internet terrorism.³⁰ By posting terrorist photographs on a variety of websites, Tsouli started his "carriage." In Iraq, he has taken Al-eye Qaeda's (AQI) to become an organization's strong partner, whose leaders have been inspired by its computer talent and determination. AQI began feeding the videos directly to Tsouli after proving its credentials.

Tsouli and Tariq Al-brother Daour started buying stolen numbers of credit cards online from several on-line sites, including Card Planet. With his skills Tsouli took to the Internet and collected the money to pay for these pages.³¹ After Tsouli and his wife were arrested, Al-Daour obtained 37,000 stolen card numbers on the phone worth over \$3.5 million. In order to launder money through many online gaming outlets including absolutepoker.com and paraisepoker.com, Tsouli cast-off stolen credit card numbers. In total, he carried out hundreds of acquisitions on 43 different platforms. The money was thus lawfully earned and laundered efficiently. 72 of those credit cards, and 95 organizations hosting 180 websites, were used by Tsouli.³² These credit cards were also bought by Tsouli for femahidine equipment by delivering it to locations or properties that he and his partner were temporarily renting.

²⁹ Ibid.

³⁰ Keatinge, Tom (2015), *"Identifying Foreign Terrorist Fighters : the role of public-private partnership, information sharing and financial intelligence,* Royal United Services Institute (RUSI)," United Kingdom, July 2015.

³¹ Ibid.

³² Ibid.

NGOs and charities are reported to be a major problem with the terrorist funding sector and their events on websites appear to be a major problem. The Financial Action Task Force, which is based in Paris, has admitted to the abuse of non-profit organizations in the funding of terrorists as a crucial blind spot in the global battle against their sources.³³ Terrorists and their backers are in particular targeting charities, solely through charitable or humane organizations. For several years terrorist organisations have been using charities for many purposes.³⁴ The term "terror funding" is used by all charities, while others already exist and are cooperated by Jihadist agents and supporters from inside. A key issue, not just with intelligence services and law enforcement, but as well as the personnel at their headquarters is the way money is distributed in warfare areas can be effectively tracked. This normally result in easy diversion of resources from the original intention. Besides, extremists find refuge in charitable events to fund their activities because they can easily come up with a legit humanitarian cause to start up contributions but then channel resources elsewhere.³⁵

Since their fund-raising is supposed to be benevolent, militant groups, NGOs and charities still have a great deal to do with their fund-raising efforts. This has led to the creation of online forums and blogs in various terrorist-linked organizations to ask for funds and to publicly publicize their operations.³⁶ In 2002, for its relations with Al Qaeda and Taliban, the Global Relief Foundation (GRF) was appointed by the treasury, according to the report. GRF stated on its website that their aim, including development, promotion and carrying out aid and charitable activities, services, organizations, institutions and funds, has been exclusively developed for humanitarian, religious, scientific and educational purposes. The Mission Statement of GRF

³³ FATF (2015b), "*Guidance to a Risk-Based Approach to Virtual Currencies*, FATF," Paris, France, www.fatf.

³⁴ Ibid.

³⁵ FATF (2015a), "*Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL)*," (the 'FATF ISIL report'), FATF, Paris

³⁶ Ibid.

stressed its work in disaster relief, humanitarian aid, education and social welfare, and its dedication to good faith for all.³⁷ GRF “has accepted donations via its website, with donors able to pay by credit and debit card, wire transfer and other means. In addition, websites of the Saudi-based Al-Qaeda Islamic Foundation,” a United States-related NGO linked to Al-Qaeda in November 2008 are available.³⁸

Other terrorist organizations also have online humanitarian fronts. The Holy Land Foundation, a charity based in Texas that founded Hamas in 2008, was arrested as reported. The Foundation's ostensible objective, explanatory to alleviate poverty by providing assistance to needy, deprived and homeless people affected by human and natural disasters, was summarized on the website. According to the government of the United States, the Union of Good (UG) has been a Hamas front created in 2000 to enable Hamas to flow in funding by the leadership of the organization. The UG web-site “was hosted by Interpal, a member based in the United Kingdom. Both Interpale and UG have been designated by the Treasury but still run.”³⁹

1.6.2 The impact of Terrorist Groups Mobile and Online Money Funding Schemes on Counterterrorism Measures

There is no surprise about the increased use of the Internet by terrorists, fuelled by a number of fundamental reasons. First of all, Internet use has expanded exponentially worldwide over the last ten years, including the use of jihadists and others.⁴⁰ Mainly more than 800 million users can easily access the Internet and there is a likelihood that this number might continue to increase during the coming years, especially in Arabic countries, where the Internet usage in

³⁷ Ibid.

³⁸ Ibid.

³⁹ Ibid.

⁴⁰ Europol (2015), “*EU Terrorism Situation & Trend Report (TE-SAT) 2015*,” Europol, The Hague, Netherlands, www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015

2006 had only attracted few users. The use of money by Internet criminals is part of a broader global trend in foreign trading technology. Online transfers of money or Internet transfers have become more common thanks to platforms such as PayPal.⁴¹

Mobile telephones can now be used as "M-payments" for the conduct of transactions. In countries where the Organized Finance System is less than stable as many African nations, it is much more desirable and readily available that the Internet or mobile phones can facilitate payments. The laundering of money on the Internet, a phenomenon that terrorist groups in the last years, has also made online poker portals and other institutions cheaper than ever before. Terrorists like Tsouli can dissimulate their identity on these online sites, but through this form of behavior can be detected.⁴²

The Al Qaeda terrorist group was instrumental in the funding and management of its Afghan headquarters prior to September 91.⁴³ The group financed the 1998 bombings of the East African Embassy, the 2000 attack on Yemeni USS Cole, and the 2001 attacks in the US. The terrorist groups became more widespread, to an extent that the central Al Qaeda facility is no longer financed all terrorist operations as it once did. This therefore meant that the groups were left to their own devices. Emerging terrorist groups turned to illegal activities to fund them.⁴⁴ The cell which tried to attack Madrid in 2004, where nearly 200 people were killed, collected the money from the hashish.⁴⁵ Terrorists attacking the London transport system also received self-

⁴¹ Ibid.

⁴² Ibid.

⁴³ CGTF (nd), "Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists, CGTF."

⁴⁴ Ibid.

⁴⁵ Carter, J.A., Maher, S. and Neumann, P.R. (2014), "*Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, International Centre for the Study of Radicalisation and Political Violence (ICSR)," London, United Kingdom "

funded credit card fraud on 7 July 2005. Jamaah Islamiyah (JI) affiliate of Al-Qaeda, backed Bali's attacks in 2002 in part, through robbery of jewelry stores in South East Asia.⁴⁶

Imam Samudra, a former JI agent convicted of the Bali bombings in 2002, for example, was in prison and wrote a book with a chapter on 'Hacking'. Hacking is one's ability to secretly manipulate private and confidential information and access points on another person's electronic gadget such as computer without their permission. Samudra, in his book, encouraged jihadists to attack US computer networks as 'credit card fraud and laundering possibilities.'⁴⁷ Whilst Samudra has no explicit instructions on how to do this in the chapter, he has directed readers to some websites to give them access to chat rooms that could help them in identifying hacking mentors. This would be useful for potential hackers, according to the head of an Internet security consultants' company, because it is just the kind of advice that anyone wishing to participate in cybercrime would want to get.⁴⁸

The hacking operations of Samudra were at least tacitly blessed by Abu Bakr Bashir, head of JI, who declared it as religiously admissible to hack foreign bank accounts. "If you can take their blood, why not take their property?" he is quoted to have said.⁴⁹ Tsouli also wanted to encourage others in a common jihadist forum to hack with a 'Hacking Websites seminar.' He gave tips on how to hide ones identity online to prevent from being detected.⁵⁰

The anonymity factor is the clearest explanation to the fact that terrorist organizations, cells and agents are constantly on the net. Terrorists have been able to find new ways to escape

⁴⁶ Ibid.

⁴⁷ US Department of State (2015), "*Counter-ISIL Finance Group Kidnapping for Ransom Communiqué*," US Department of State, Washington.

⁴⁸ Ibid.

⁴⁹ US Department of Treasury (2015), "*United States National Terrorist financing risk assessment*," US Department of Treasury, Washington, United States.

⁵⁰ Ibid.

surveillance during the US and international community attacks.⁵¹ The Tsouli case is another example of how hackers benefit from security defects and online "anonymity" options. Though he engaged in widespread illegal activities on the Internet, Tsouli was able to hide his footprints, pay for purchases using fake credit cards and identify details while never utilizing his real name. To hide his IP address from his phone, Tsouli used anonymisation software and proxy servers.”

52

After breaking in and publishing information on the Arkansas government website and George Washington University's website, the United States authority suspected that Tsouli could be in the USA. Interestingly Tsouli was, for the first time, meeting Tariq Al Daour⁵³ He was eventually apprehended not through the advanced electronic methods but using the old fashion police arrest. The Bosnian police, in October 2005, arrested two men charged with involvement in activities related to terrorism. A search of their phone and email accounts revealed Tsouli and his associate members.⁵⁴ Babar was often very cautious in his company, using fake names and other tactics to hide the fact that he runs the terrorist sites and mostly used to transact in cash. In his email messages, Babar also used cryptography to encrypt data on his computer.⁵⁵

In fact, terrorists seem so confident of Internet security that many of their websites have companies based in the United States. Experts conclude that the US 'content is appealing and cost-effective.⁵⁶ There are several instances of American websites linked to terrorist groups. A

⁵¹ United Nations Security Council (2012), “*First report of the analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban and associated individuals and entities*,” S/2012/683, 5 September 2012.

⁵² FATF (2015a), “*Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL)*, (the FATF ISIL report),” FATF, Paris.

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ Ibid.

⁵⁶ United Nations Al-Qaeda & Taliban Sanctions Monitoring Team, “*First report of the Analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban*

Taliban-related forum suspected to be hosted by a Texas company, which boasted and facilitated a terrorist organization in conducting attacks on US forces in Afghanistan, the study says. Further worrying is that the Pakistani Lashkar e-Taiba organization suspected to have committed the 2008 Mumbai attack, is said to have made Internet calls whose routing was done via a Texas server.⁵⁷ In some situations, Hamas has taken self-driven actions and has established its personal internet service provider in the United States. Hamas head, Abu Musa Marzook, provided seed funds to the Holy Land Foundation in Infocom. Infocom's leaders were then found guilty of violating US export control laws by providing Libya and Syria with services.⁵⁸

Jihadist groups have consistently used the Internet to send a radical message, however, they are becoming more conscious of the dangers of use of electronic payments.⁵⁹ One of the jihadist in a well-known militant website Al-Fallujah, advised others against making payment online, indicating that governments track and regulate electronic payment systems closely and were thus able to detect them and possibly unlock entire networks. The extremist suggested that when using online payment, then they should use 'circumvented ways and means' in order to make monitoring more difficult.⁶⁰ According to this jihadist, this level of security only became important as governments acted more proactively to track and record electronic transactions.

Hamas has also provided potential donors guidance on how to avoid detention. For instance, they advised that when submitting donation on Hamas's Qassam Brigades website, donors should use

and associated individuals and entities," http://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2012_683.pdf.

⁵⁷ Ibid.

⁵⁸ Ibid.

⁵⁹ Ottawa Citizen (2014), "ISIL using social media to lure young teenagers, accountants, engineers to its cause" (David Pugliese), Ottawa Citizen, Ottawa, December 16, 2014.

⁶⁰ Ibid.

fake names in the emails.⁶¹ Hamas also informed supporters of the ‘stable’ handling of donations to the ‘fighters’. Hezbollah spokesman Ahmed Jabril, boosted of its Internet prowess, through particular use of Quran verses encrypted messages to protect interception. According to Ahmed Jabril, it was possible to send particular Quran verses as a call to charity or a call to jihad without being detected.⁶²

1.6.3 The Counter-Terrorism Strategies that can be used to prevent terrorist groups Mobile and Online Money Funding Schemes

Terrorists will always go on to use the Internet in most of their activities, including the collection of funds and money transfer. The size and scope of most modern technologies, including the Internet advances are expected to only increase.⁶³ Governments globally now accept that steps must be taken in order to tackle this rising threat and that the Internet is vulnerable against terror. Nevertheless, there are no clear accords on what best measures can be assumed.

The USA has assumed the lead in the bid to regulate the usage of the Internet, especially for terrorist activities. Some of the action they have taken is convicting suspected terrorists who were involved in internet related activities, including Babar and al-Hussayen.⁶⁴ besides, the US has also applied its capabilities in law enforcement to target companies that offer online transaction services and fail to observe counterterrorist/ anti money laundering systems of internal compliance. Non US citizens who target US market in transacting online, also faced criminal charges if their companies are not registered in the United States, as required by law.⁶⁵

⁶¹ Oftedal, Emilie (2015), “*The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment (FFI),” Norway, 6 January, 2015, www.ffi.no/no/Rapporter/14-02234.pdf

⁶² Ibid.

⁶³ Ibid

⁶⁴ FATF (2015a), “*Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL)*, (the FATF ISIL report),” FATF, Paris.

⁶⁵ Ibid.

The United States has gone further to have suspected websites shut down through the respective Internet Service Providers. During the Obama administration, the US government created a Cyber czar, after a 60-day comprehensive policy review, to address the cyber-threat.

The United Kingdom has also been active in its effort to deal with online funding by terrorist groups. The UK government established a post of cybercrime coordinator, located at the Whitehall, which was to take the lead in countering online funding and cybercrimes.⁶⁶ In addition, the government has used its legal instruments to track internet users suspected to be carrying out terrorist activities. While Tsouli's case was the most prominent one, others also emerged, though with no much successful outcome, confirming how difficult and challenging these cases can be. For example, Sulayman Zainulabin, a London based chef, was charged after it was established that his website was giving trainings known as 'Ultimate Jihad Challenge'. He was however not charged.⁶⁷

The European Commission is reportedly vigorous on the issue of countering online funding and cybercrimes and has recommended that the EU member nations beef up criminal penalties in cases involving cybercrime. In addition they may also move to pressure member countries to augment collaboration on cyber-investigations and publish measures on how fast enough states should retort to fact-finding requests for assistance. Currently no such guidelines or restrictions exist.⁶⁸

Both USA and UK remain on the forefront on the fight against terrorist online financing. Lack of technical capacity to investigate online terrorist activities has posed a major setback to many

⁶⁶ Keatinge, Tom (2014), "The Role of Finance in Defeating Al-Shabaab, *Whitehall Report 2-14*, Royal United Services Institute (RUSI)," United Kingdom, December 2014,

⁶⁷ Ibid.

⁶⁸ Ibid.

countries in their effort to counter terrorist online financing. Indeed, in order for the international community to tackle this risk, the international community must make 100 or 1,000 efforts, Interpol's Secretary-General was quoted saying.⁶⁹ The UAE Government, for example, is now gaining skills on how to “track the Internet protocol addresses” and is not very familiar with the overall way to track money. In reality, there are only two CTF analysts in Dubai Police in the UAE, far too low to cover the region adequately considering Middle East is viewed as the financial hub for terrorist activities. Secondly, the extent to which Governments prosecute Internet-related crimes is also a source of contention. Some governments believe that such measures would limit people's freedom of speech. There is also a debate about what works best in the fight against terror, for example whether it is important that once these sites are known, then they be monitored for intelligence gathering or whether they should be shut down.⁷⁰

Thirdly, the existing laws in most countries are not up to date with the technological changes and in some cases, there is no agreement or consistency.⁷¹ For example, there is a regulation in Italy that requires cyber cafes to ask for identification to users. However, Rome is the only country in the European Union which enforces this regulation. The US has seen its obligations and laws more expanded; others are reluctant to allow their law enforcement agencies to comply with this broad and possibly extraterritorial standard.⁷²

Fourthly, although some states support the enactment of a global treaty or legal instrument for control in this particular scenario, not all respective regimes go ahead to assume the right

⁶⁹ Keatinge, Tom (2015), “*Identifying Foreign Terrorist Fighters : the role of public-private partnership, information sharing and financial intelligence*,” Royal United Services Institute (RUSI), United Kingdom,” July 2015.

⁷⁰ Ibid.

⁷¹ Oftedal, Emilie (2015), “*The Financing of Jihadi Terrorist Cells in Europe*,” Norwegian Defence Research Establishment (FFI),” Norway, 6 January, 2015.

⁷² Ibid.

direction.⁷³ This has also been augmented by the inaction of the technocratic Financial Action Task Force FATF, which is tasked with coming up with international principles for terrorist finance. Although the FATF has recognized the Internet, more so the Internet financial systems as one of the main financial vulnerability, there is still no clear guidelines on how countries can alleviate these threats. There are currently no widely agreed measures, for instance, on what internet transactions should be recorded and reported, an area that FATF is obliged to weigh in. These records are especially useful for international law enforcement agencies when it comes to online terrorist funding charges.⁷⁴

Terrorists are actively changing how funds are raised and transferred in reaction to government efforts to further avoid surveillance.⁷⁵ The actions of terrorists are supported by new technology that also hamper government surveillance efforts. One such issue is the use of virtual currency, which can only be digitally used for internet transactions. Second-life, America's largest virtual economy, with a market of nearly \$500 million each year, which demonstrates how fast these businesses grow. The fast increasing computer-generated currency market in the far east, especially China, makes it more difficult to watch from an American perspective, currently growing at 800 million dollars a year and at a rate of 30 percent per year.⁷⁶

Unfortunately, what the USA or other countries can do in this area alone is limited.⁷⁷ The internet knows no boundary hence if the US curves in these terrorist groups operating within their borders, then terrorists can move to other jurisdictions less vigilant to track and continue

⁷³ FATF (2015b), “*Guidance to a Risk-Based Approach to Virtual Currencies*,” FATF, Paris, France.

⁷⁴ Ibid.

⁷⁵ FATF (2015a), “*Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL)*, (the FATF ISIL report),” FATF, Paris.

⁷⁶ Ibid.

⁷⁷ Europol, “*TE-SAT 2014: European Union Terrorism Situation and Trend Report 2014*,” Europol, The Hague, Netherlands, 2014

operating these unlawful acts. Terrorists' ability to use the internet to execute their unequal agenda can be impeded only by a more organized and coordinated global response. American efforts are a step in a right direction, but effective counter effort is what can be done collectively by the broader international community.⁷⁸

1.7 Theoretical Framework

1.7.1 Identity Politics Model

The Identity Politics Theory can be used to explain the relationship between terrorism funding scheme (mobile and online funding) and terrorism. The key proponents, James Khalil and Martine Zeuthen, states that people become members of a violent extremist association either in rejection of or to rebel when certain state affairs are not favoring them, or even triggered by incentive personal returns.⁷⁹ It explains the need for an individual or group of people joining a radical terrorist organization, in order to fight or avenge the injustice committed against them. In this political identity, the idea of marginalization, occupation and injustice is fundamental. This theory would explain the mobile and online funds collection schemes of terrorism because the vulnerable groups can be encouraged to fund or contribute to terrorist groups.

Example of such groups are the Sunni and the Shia. The Sunni whose identity is based on the interventions that were drafter after World War I of USA in Arab affairs. This was further aggravated by Israel's step of occupying Palestinian lands and other appalling activities not taken into consideration by the West, and the US assaults on Iraq and Afghanistan. The Shia, whose weakened political authorities and territorial sovereignty are considered the adversary by the Sunnis, are another such group. The Jordanian and Syrians who considered themselves justice

⁷⁸ Ibid.

⁷⁹ Ball, N., "The Evolution of Security Sector Reform Agenda. In Sedra, M. (Ed.), *The Future of Security Sector Reform*," (Ontario: Canada, CIGI, 2010). Pp. 29-44

agents coming in the defense of Syrian children and women against regime attacks, is also another example of identity political group according to key information collect by the WANA Institute and the Mercy Corps. It is a binary process seeing how identity policy motivates people to join terrorist groups.⁸⁰

This may particularly apply in Islamic societies where Islamic political philosophy emphasizes justice rather than peace. Victor points out that revenge of humiliation by oppressors is an ancient tribal tradition, one strongly related to recent Middle East violence and, to a lesser degree, the Horn of Africa.⁸¹ Extremist forces also exploit these schisms with misinformation which both validates the sense of exclusion, including, for example, the videos of civilians killed by US drone strikes, violations of the rights of captives in the US extraordinary practices, Shiite paramilitary forces in Iraq and the bodies of tortuous Syrian kids. Al Shabaab is a group in Kenya that portrays itself as a group that struggles against avenging and defending Muslims from historic injustices, particularly on the coasts and the north. Harper claims that Al Shabaab decision to fight was more focused on an emotional reaction to the supposed inequity carried out rather than on a clear interpretation of religious obligation.⁸² As a result, the group attracted supporters and sympathizers who were ready to fund their efforts, particularly through online or mobile funding, with the aim of fighting historical injustices.

Relationship between the individual and the state is another form of identity politics. Much was written about the disappearance of the Arab Social contract and the profound sense of social unfairness it evoked. Social mobility has been impacted by unemployment among the youth,

⁸⁰ Ibid.

⁸¹ Prestholdt, J., "Kenya, the United States, and Counterterrorism." *Africa Today*, Vol. 57(4), 2011, pp. 3-27.

⁸² Harper, E., "Reconceptualising the drivers of violent extremism: An agenda for child and youth resilience." (WANA Institute 2018).

increase in prices and weak social safety nets. However, the unequal allocation of national resources, unequal opportunity to all and social economic marginalization has fueled poverty more than unemployment. The aspect of the interest of the few elite over the poor majority also contribute and stimulates injustices, marginalization and inequality, driving grievance and disenfranchisement.

When young people's expectations and grievances clash and their poor condition remain unchanged, then they go looking for ways to demonstrate their importance and relevance. This is what scholars argue as relative deprivation. Violent radical extremist take advantage of this situation and may tap into the opportunity in two ways; a promise of immediate jobs and potential prosperity, offer political leadership that embraces equality and meritocracy.⁸³ The efficiency of these powers can be seen in many cases. Research on Boko Haram in Nigeria shows how deeply corruption and inequality led frustrated youth become an easy target for recruitment into the terror group which sold out the idea of affiliation into tribal and religious ground rather than state. The success of the jihadists in Central Asia and the Northern Caucasus was related to grievances over poor governance, corruption and violations of human rights. Similarly, youths joining extremist groups in Kenya, cite historical injustices and state marginalization as the main reasons for their move.⁸⁴ They are also persuaded to join these groups through the social media and most of their contributions are made online to avoid suspicion. This model explains the relationship between terrorist activities and terrorist online and mobile funding schemes since it links individual frustration as a result of state injustices coupled with lack of opportunity as a catalyst to one being motivated into conducting acts of terror. Borum search research, quotes studies in the United Kingdom about Muslim youth, which

⁸³ Ibid.

⁸⁴ Ibid.

reported that most Muslim youths felt like they were in constant confrontation with the government, media, and the po overall security system. In Kenya, some security guidelines, for example, migration vetting and stop and search protocol, are seen as a form of targeted marginalization by some Muslim citizen. In both cases, recruiting companies capitalize on this perception. In their recruiting videos, Al Shabaab use police videos harassing Kenyan Muslims and unverified photos of illegal arrests, imprisonment, extrajudicial murder, alleged religious and ethnic discrimination, in an attempt to recruit Kenya Muslim youths.

1.8 Research Hypothesis

H₀ Counterterrorism strategies applied in Kenya do not have a noteworthy effect on thwarting Al-Shabaab's mobile and online money funding schemes in Kenya.

H₁ Counterterrorism strategies applied in Kenya significantly affect Al-Shabaab's mobile and online money funding schemes in Kenya.

1.9 Justification of the Study

This research is both scholarly and political. The research helps to address the current knowledge gaps in counter-terrorism field. While a number of studies have examined the counterterrorism strategies used by the Kenyan security agencies, no study has comprehensively evaluated the effectiveness of these strategies in thwarting terrorists' online and mobile funding schemes and activities. The study findings and conclusions will help enrich the knowledge bank in this particular area.

In terms of policy, the study might be beneficial to security agencies, policy makers, the government and the Kenyan allies in the fight against terrorism. The research findings will help the security agencies to enhance their strategies by enacting policies that will require online

payment platforms and internet pages to develop stringent measures and report any suspicious activities. Besides, the Kenyan government and its allies might enact policies that will restrict online money platforms from dealing with suspicious consumers, which will help prevent transfer of money across terrorist networks.

1.10 Research Methodology

This research will use secondary data from library sources. It utilized books, e-books, government publications, journals, magazines, and newspapers. Data was analyzed thematically to identify the key themes, which were used to infer recommendations and conclusions.

1.11 Study Limitations

This study was limited by the fact that, it only relied on secondary data. Utilizing primary data could have validated the research findings in a more concrete way. The researcher could not collect primary data because of the COVID-19 pandemic, which limited and restricted physical movement.

1.12 Chapter Outline

The current study is defined as follows: The context, the statement of issues, investigation concerns, the aims of the study and justifying the study are discussed in Chapter 1. The chapter also addresses related literature and theory. The chapter ends with the methods used to carry out the analysis. Chapter two will discuss on terrorist groups mobile and online funding schemes with a focus on Al-Shabaab. Chapter three will discuss on the impact of Al-Shabaab's mobile and online money funding schemes on counterterrorism measures in Kenya. Chapter four will discuss on the counter-terrorism strategies that can be used to prevent terrorist groups' mobile and online money funding schemes. Lastly, chapter five will provide the summary, conclusions, and recommendations.

CHAPTER TWO

AL-SHABAAB'S MOBILE AND ONLINE FUNDING SCHEMES IN KENYA

2.0 Introduction

This chapter will explore different funding schemes that terrorists use to fund their activities, the methods of funding and how they benefited and challenges along the way. This is to enable policy makers to understand and come up with counterterrorism measures that can adequately solve the problem.

2.1 Al-Shabaab Funding Schemes

In 2014 Tom Keatinge in his article on the Role of Finance in Defeating Al-Shabaab state that its funding schemes are (1) establishing itself as a government thereby establishing a system of collecting taxes, (2) as a violent group they make those in their territories give them money by threatening harm on them or their loved ones, (3) they willingly use their power to do illegal things in return for money, for example, in Kenya an Italian aid worker was abducted and later released while in Mogadishu in what is widely suspected that ransom was paid for her release and (4) taking bribes.

In an overview by Michael Freeman and Moyara Ruehessen on how terrorist move money titled Terrorism Financing Methods they give an example of how money service businesses (MSB) funded Al-Shabaab. An example of an entity used to vividly state what an MSB is Western Union..⁸⁵ ⁸⁶ . In 2009 Al-Shabaab raised 40,000 US dollars from Somalis who are away from their own country as stated in a study commissioned by the United Nations Development Programme (UNDP) to examine the social media use and online radicalization in Africa.

⁸⁵ Ibid.

⁸⁶ Ibid.

2.2 Methods Used by Al-Shabaab to sustain Funding schemes

A number of people that are connected by the need to apply violent tactics in order to attain political objectives and mileage or even compel a regime to take action have two options: first, the need to provide enough of what the group needs in order to exist and second, to make something continue for some time without becoming less.⁸⁷ Taking a look at the first option providing enough of what is needed in order to exist the study by UNDP provides an example of how Al-Shabaab had a two-week online campaign and raised funds for its fighters.⁸⁸ Another aspect that come in to play is the use of social networks, for example, Salafi and Al-Hirja networks.⁸⁹

The second option of making something continue for some time without becoming less is realized from social media platforms provided by the Internet.⁹⁰ One such platform is Twitter it has used tweets to instill fear (al-Shabaab's main objective) to reach out and appeal to sympathizers for funding.⁹¹ In Nairobi innovation is a common thread of daily life, which makes it easy for terrorists to solicit for funds. Twitter is also used to spread statements that are exaggerated in order to gain support for the group an example is the 2013 Westgate mall attack in Nairobi that depicted how capable they are in causing destruction.^{92 93 94 95 96 97 98}

⁸⁷ Ibid.

⁸⁸ Carmody, Pádraig. 2013. "A Knowledge Economy or an Information Society in Africa? Thintegration and the Mobile Phone Revolution." *Information Technology for Development Journal* 19 (1): 24–39

⁸⁹ Ibid.

⁹⁰ John Cassara, "Trade-Based Money Laundering," (New Jersey: John Wiley & Sons, Inc., 2016).

⁹¹ Ibid.

⁹² Kathleen Caulderwood, "Al-Shabab's Finances: The Militant Group Gets Funding From Local Businesses, Sources Abroad," *International Business Times*, September 4, 2014

⁹³ Ibid.

⁹⁴ Anderson, David M., & Jacob McKnight. 2015. "Understanding Al-Shabaab: Clan, Islam and Insurgency in Kenya." *Journal of Eastern African Studies* 9 (3): 536–57.

⁹⁵ I bid.

⁹⁶ Botha, Anneli. 2014. "Political Socialization and Terrorist Radicalization Among Individuals Who Joined

2.3 The Benefit of Funding schemes to Al-Shabaab

The funding schemes have provided an advantage that money gives to Al-Shabaab enabling it to enhance publicity, own Kata'ib news channel and a radio station –Radio Andalus. The money has a helpful and useful effect in that Al-Shabaab has achieved to find new people to join the organization, to persuade their members to do violent attacks to help their cause, get persons who supports and admires the groups set of ideas, to organize the different parts of an activity and the people involved in it so that it works well in order to achieve a particular aim for instance in the battle field.^{99 100 101 102103 104}

2.4 Challenges faced by Al-Shabaab

Some of the challenges faced by Al-Shabaab in mobile and online funding schemes are Internet users in the country is low since 1.7 per cent of the population has the opportunity to use Internet, in Somalia citizens rely on mobile money services that allows small amounts of cash to be transacted at ago,¹⁰⁵ and the banking system in the country is not fully developed.¹⁰⁶

A closer look at the mobile money services in 2010, in fear of tax and revenue reduction and possible interdiction by foreign countries, al-Shabaab stopped the use of mobile banking in its

al-Shabaab in Kenya.” *Studies in Conflict and Terrorism* 37 (11): 895–919.

⁹⁷ Ibid.

⁹⁸ Ibid.

⁹⁹ Seth G. Jones, Andrew Liepman, and Nathan Chandler, “Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab,” *Rand Corporation*, 2016.

¹⁰⁰ Ibid.

¹⁰¹ Ibid.

¹⁰² Ibid.

¹⁰³ Baro, Ebikabowei Emmanuel, & Benake-ebide Christy Endouware. 2013. “The Effects of Mobile Phone on the Socio-Economic Life of the Rural Dwellers in the Niger Delta Region of Nigeria.” *Information Technology for Development* 19 (3): 249–63.

¹⁰⁴ Ibid.

¹⁰⁵ Botha, Anneli. 2014. “Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya.” *Studies in Conflict and Terrorism* 37 (11): 895–919.

¹⁰⁶ Anderson, David M., & Jacob McKnight. 2015. “Understanding Al-Shabaab: Clan, Islam and Insurgency in Kenya.” *Journal of Eastern African Studies* 9 (3): 536–57.

areas of control.¹⁰⁷ Al-Shabaab later decided to cease opposing mobile banking. The UN sanctioned an individual for the creation of ZAAD- a popular money network that was possibly used by the Al-Shabaab for payments and transferring funds.¹⁰⁸ At the end of 2014, the terror group adopted the use of mobile money service for payments. By 2016, the Al-Shabaab changed its negative attitude towards the use of mobile money services and used it in salary payment to fighters and other staffs.¹⁰⁹

As for the banking system, even though there are regulations in monetary services in Somalia, several banks in the U.S.A stopped their banking services to Somali organizations in 2015 due to its lack of sufficient protections on counter-terror finance. In the wake of the 2015 terror attack at Garissa University, 13 money transfer services belonging to Somali were shut down by the Kenyan government and several Al-Shabaab-linked bank accounts were frozen.¹¹⁰ Somali intelligence center, a newly formed strategy, will face challenges in fighting terror finance owing to its unstable systems of compliance as well as insufficient workers.

2.5 Conclusion

From this section, in order to gain more support and control for its insurgency, Al-Shabaab recruits, pays their fighters as well as providing financial support and welfare to the people living in the regions under its control, using mobile money strategy. Like other terrorist groups, Al-Shabaab relies on financing. The financial support enables the Al-shabaab to not only launch dangerous attacks but also to contain pressure from the military forces

¹⁰⁷ Botha, Anneli. 2014. 'Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya.' *Studies in Conflict and Terrorism* 37 (11): 895–919.

¹⁰⁸ Ibid.

¹⁰⁹ Ibid.

¹¹⁰ Ibid.

CHAPTER THREE

THE IMPACT OF AL-SHABAAB'S MOBILE AND ONLINE MONEY FUNDING SCHEMES ON COUNTERTERRORISM MEASURES IN KENYA

3.0 Introduction

This chapter examines the impact of Al-Shabaab's mobile and online money funding schemes on counterterrorism measures in Kenya. Some of the counterterrorism measures in Kenya that have suffered the blow of Al-Shabaab include: (i) engaging the marginalized communities in the Coastal and North Eastern parts of Kenya to address the root causes of violent extremism (ii) public diplomacy efforts, (iii) financial regulation measures and financial sanctions (iii) constraining terrorist mobility, and (iv) the AMISOM mission in Somalia.

3.1 High Levels of Illicit Financial Flows as a Blow to the AML and CFT

Al-Shabaab's funding schemes have been the main reasons why the group has succeeded in penetrating Kenya, despite the counterterrorism measures in place. Al-Shabaab has been launching several attacks in Kenya since 2011 to avenge the Operation Linda Nchi.¹¹¹ These terror activities are aimed at the withdrawal of Kenyan soldiers who are fighting in Somalia alongside the AMISOM -African Union Mission in Somalia. The regions that have experienced most of these terrorist activities are: Garissa, Wajir, Nairobi, Mandera and Mombasa. North-Eastern region in particular has been largely affected by the attacks. The main targets of these attacks includes military bases, churches, passengers' vehicles, bars and restaurants, shopping

¹¹¹ Kathleen Caulderwood, "Al-Shabab's Finances: The Militant Group Gets Funding From Local Businesses, Sources Abroad," *International Business Times*, September 4, 2014.

malls and market places. The success of such attacks can be explained by Al-Shabaab's expanded mobile and online founding networks.¹¹²

One of the tools in targeting terrorism is through addressing the ability for groups to operate by targeting funding and financial flows. This has largely been through the introduction and implementation of legislation "addressing Anti-Money Laundering and Combating the Financing of Terrorism (AML and CFT)."¹¹³ Whilst there have been notable successes in curbing how international terrorist groups operate, in Central, East and West Africa "this legislation has had limited impact in curbing financial flows. Africa experiences high levels of illicit financial flows as well as relatively high levels of terrorism. According to the Global Terrorism Index (GTI), Sub-Saharan Africa had the fourth highest levels of terrorism in 2016, behind "South Asia, the Middle East and North Africa and North America."¹¹⁴ AML/CTF legislation has been inadequately implemented in Africa. The levels of compliance with international norms is below the international average. This is largely for two reasons: limited political will as money laundering taps into the same loopholes used for corruption and other leakages of government spending; and high vulnerability of many African countries with a large informal economy, limited state capacity and high costs for successful implementation.

Kenya has high vulnerability to problems such as terrorism finance, monetary fraud and laundering of money. It is the East African financial powerhouse and the leading user of mobile money scheme.¹¹⁵ Criminal activities both in foreign and domestic settings are the source of

¹¹² Neumann, P. (2015). "Remarks on Terror on the Internet. The White House Summit to Counter Violent Extremism," Washington DC (February 19).

¹¹³ Keatinge, Tom (2014), "The Role of Finance in Defeating Al-Shabaab, *Whitehall Report*" 2-14, Royal United Services Institute (RUSI), United Kingdom, December 2014,

¹¹⁴ Ibid.

¹¹⁵ Harper, E., "Reconceptualising the drivers of violent extremism: An agenda for child and youth resilience." (WANA Institute 2018).

money laundering that is so prevalent in the informal and formal sectors. These crimes include smuggling, cybercrime, corruption, smuggling, manipulation of trading documents, drugs trafficking, poaching and illegal trade in charcoal or timber. The terror activities are also aimed to make the group more popular.¹¹⁶

Emir Godane discussing the terror attack at the Westgate Shopping Centre in his recording before the U.S drone killed him, related the attack with the Jihadist in Syria, Sinai and Afghanistan. He went ahead to encourage the Al-Shabaab group that through perseverance they would succeed in their war against Kenyan and Ethiopian Christians.¹¹⁷ The number of individuals recruited into the Al-Shabaab group in Somalia raised since 2010 when they started launching their attacks. Apart from Somalia, the terror group utilizes terror activities in other countries to raise funds especially through social media platform. It shows how they are determined to protect the Muslims against the regional governments and non-believers (kuffar). The videos of the terrorist events are taken and the narration made in Arabic language. These videos are spread online with a request for funds. People from different countries are featured in the videos giving testimonies to validate the appeal of the Al-Shabaab.¹¹⁸

3.2 Using Economic Incentives to Beat Kenya's Efforts to Rehabilitate Youth from Violent Extremism

As from 2015, the Kenyan local government and security officers established more developed strategies especially through intelligence gathering as well as community involvement.

¹¹⁶ Europol, “*TE-SAT 2014 : European Union Terrorism Situation and Trend Report 2014*, Europol, The Hague, Netherlands,” 2014

¹¹⁷ Harper, E., “Reconceptualising the drivers of violent extremism: An agenda for child and youth resilience.” (WANA Institute 2018).

¹¹⁸ Ibid.

However, the terrorist group still adapted these strategies.¹¹⁹ The Al-Shabaab utilized the funds received through online and social media platforms to pay for recruitment process and traveling costs to Somalia. The funds were also used to launch terror attacks in Kenyan regions such as Northern area, Mombasa and Nairobi. Secondly, the Al-Shabaab aimed at converting youths who were Christians in Central and Western regions as opposed to its earlier objective of targeting the Muslims who were against the government. Finally, the terrorist group avoided problems at the coasts of Kenya by crossing into Tanzania where they assimilated well owing to the culture and ethnic similarities.¹²⁰ The Al-Shabaab have been silent recently. However, their operations have been focused at the border of Somalia. Unlike her neighbors such as Uganda and Tanzania, Kenyan- Somalia border so long and this increases her vulnerability to attacks by Al-Shabaab. Several soldiers and security officers have been killed by the Al-Shabaab at the Somalia border during their patrols five years after the terror attack at Westgate mall. These killings have mostly occurred from ambush and powerful explosives. The government's effort to prevent the killings of soldiers have not succeeded like those used to thwart terrorism in urban regions.¹²¹

Towards the end of 2011, Al-Shabaab begun using the slogan that holy war could establish Islamic rule in lost lands of the Muslims and, as a corollary, restore inhabitants' political, economic and social rights to enable them achieve more recruitments at the coast.¹²² The terrorist group got funding from Jihadists groups such as the ones that supported the AL-Qaeda in 2002 in carrying out terror assault in hotel owned by an Israeli in Malindi Town. At the

¹¹⁹ Cohen-Almagor, R. (2017). "Jihad online: How do terrorists use the Internet?" *Media Metamedia Management*, 55-66

¹²⁰ Botha, Anneli. 2014. "Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya." *Studies in Conflict and Terrorism* 37 (11): 895–919.

¹²¹ Ibid.

¹²² Anderson, David M., & Jacob McKnight. 2015. "Understanding Al-Shabaab: Clan, Islam and Insurgency in Kenya." *Journal of Eastern African Studies* 9 (3): 536–57.

formerly coastal province, Al-Shabaab group recruited large number of people from Lamu, Mombasa, Kilifi and Kwale counties, as compared to small number recruited from Tana River County. In Kwale County which lies on the inland of Kenya. According to an estimation by the soldiers, about 150 youths were recruited and taken to Somalia in a period ranging from 2012 to 2015. This represents the largest number from a Kenyan region.¹²³

Just like any part of the country, the Kenyan coastal authorities have taken different military strategies.¹²⁴ When the Al-Shabaab terrorists started creating ties with local militants, the government did not respond to the issue. However, after the 2012 attack, it responded with heavy attacks for instance various leaders were reportedly assassinated. The security officers shut down at least 4 mosques allegedly linked with the recruitment activities by Jihadists. These mosques were later allowed to open with new leadership. Even though it worked within a short time, the strategy increased the grievances by the Muslims against the government of Kenya.¹²⁵

From 2015 onward, Kenya desisted from its previous tactic of mass arrests and intimidations, which was not working to stop Al-Shaaab, especially in their funding schemes. Instead, they adopted a new strategy that involved deeper engagements with the Muslims from the coastal region their participation in matters pertaining security and the involvement of civil society and local political leaders and civil organizations were critical to the reduction of recruitments by the militants. The National Counter-Terrorism Centre and the regional security officers have engaged and consulted regional leaders with an aim to create the best way of handling the terrorist attacks. Political leaders, Kenyan Muslim leaders, and academics have lauded the approach as it has established cooperation and trust between the government bodies and the

¹²³ Ibid.

¹²⁴ Botha, Anneli. 2014. "Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya." *Studies in Conflict and Terrorism* 37 (11): 895–919.

¹²⁵ Ibid.

public. The fact is that as from 2015, the recruitment by the Al-Shabaab has declined. Security staffs have reported that Al-Shabaab militants have either escaped to neighboring states especially Tanzania or gone underground. Moreover, the security has also been increased. The reduction of tension has enhanced lifting of travel restrictions in 2015 by foreign countries to various Kenyan coastal regions such as Mombasa.¹²⁶

3.3 Increased Radicalization

Kenyan youth are coerced by their religious, social and economic status to join the extremist groups. They chose to join the militant groups as their only option. Coastal religious leaders indicate that most youth are converted to Islam by promises of food or some economic advantages.¹²⁷ One of the reasons for Christian youth conversion to Islam was economic opportunities. This is according to PeaceTech Lab's report of June 2018. As the Alshabaab militants increase in Somalia, Kenya has turned into the main recruitment grounds as well as the main targets for terror attacks. Reports show that several Kenyans were convinced by the Al-Shabaab to convert to Islam as early as the year 2012. By around December of 2014, reports estimate that about 25% of the Al-Shabaab's ranks were Kenyans.¹²⁸

Basically, Al-Shabaab has carried out recruitments on Muslims living in Coastal regions of Kenya.¹²⁹ According to School administrators in these regions, the Alshabaab group has destroyed the schools since they influence and recruit youth to join their militant group. Kenyan security forces invaded Muslims' school at Likoni, in Mombasa county in December 2017. In the raid, about four teachers were arrested and at least a hundred students were taken to safety.

¹²⁶ Seth G. Jones, Andrew Liepman, and Nathan Chandler, "Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab," *Rand Corporation*, 2016.

¹²⁷ Prestholdt, J., "Kenya, the United States, and Counterterrorism." *Africa Today*, Vol. 57(4), 2011, pp. 3-27.

¹²⁸ Ibid.

¹²⁹ Coning, Cedric. 2017. "Peace Enforcement in Africa: Doctrinal Distinctions Between the African Union and United Nations. *Contemporary Security Policy*" 38 (1): 145-160.

According to the police officers, were being introduced to extremist Islamic narratives.¹³⁰ Al-Shabaab who carry out recruitments and have both Somalia and Kenyan links remains a danger to Kenyan security. Abdukadir Mohamed Abdukadir, a popular al-Shabaab militant is a Kenyan by nationality but of Somali origin. He therefore creates a medium and proper link between the terrorists in Kenya and Somalia.¹³¹ Commonly referred to as Ikrima, Abdukadir, is free to travel in the two countries and use his linguistic and cultural advantage attract youths into Al-Shabaab group. According to a study carried out in 2018 by PeaceTech Lab, an N.G.O based in U.S, the alshabaab had increased the recruitments in Kenya and the recruits includes both Somali diaspora and Muslims from Kenya.¹³²

The activities carried out by the Al-Shabaab vividly shows how much they require proper funding. Despite the fact that Alshbaab has been tactically suffering some defeats in Somalia, its operations remains efficient with an expanding operation to raise funds. ` From a financial point of view, the Al-Shabaab talks to local individuals more convincingly, more forcibly, and more effectively for many years even though life in regions under Al-Shabaab control lacking democracy and freedom, with extremely dangerous ways of maintaining discipline¹³³

3.4 Conclusion

This section has looked at how Al-Shabaab's mobile and online funding schemes are affecting Kenya's counterterrorism measures. While the Kenyan government is trying to rehabilitate youth from violent extremism, Al-Shabaab is using economic incentives to recruit them.

¹³⁰ Ibid.

¹³¹ Botha, Anneli. 2014. "Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya." *Studies in Conflict and Terrorism* 37 (11): 895–919.

¹³² Harper, E., "Reconceptualising the drivers of violent extremism: An agenda for child and youth resilience." (WANA Institute 2018).

¹³³ Ibid.

CHAPTER FOUR

COUNTER-TERRORISM STRATEGIES THAT CAN BE USED TO PREVENT AL-SHABAAB'S MOBILE AND ONLINE MONEY FUNDING SCHEMES IN KENYA

4.0 Introduction

Al-Shabaab's mobile and online money funding schemes in Kenya can only be overcome through effective counter-terrorism strategies. While Kenya has developed a number of counter-terrorism measures to prevent terrorism activities, there is scarcity of measures to deal with the promotion of terrorism through the Internet, including mobile and online money funding schemes. This section provides measures that can be used to overcome internet-based terrorist activities. It is through such measures that Al-Shabaab's mobile and online money funding schemes in Kenya can be overcome.

4.1 Introducing Legal Measures to Guide Online Financial Companies

Following the terrorist events that have recently been reported around the world especially in Kenya, there have been a call by policymakers for social media companies to remove or block the extremist or terrorist linked contents whenever such contents appear in their platforms. Furthermore, there is a developing body which involves proposed, forthcoming and existing local and worldwide regulations which includes the European Commission proposal on the distribution of the online terrorist content, that will pose financial penalties if content is not

taken down within a short, specified period of time.¹³⁴ In turn, online companies are developing proper means of doing away with terrorist contents as well as persons who tend to violate their conditions and terms of service.¹³⁵

Social media platforms usually coordinate with the security departments by giving more information on or help stopping terrorist accounts even though they don't participate in financing of terrorism.¹³⁶ Payment processors and Crowdfunding platforms play a major role in providing useful information required for investigating a suspected misconduct or terrorism content. Such valuable information that may be required by the authorities for investigative purposes include the account details, transactional information, personal identity and IP address.¹³⁷ Many different terrorist groups have also been attracted in virtual currencies including bitcoin, which represents an important innovation in the financial sector and this may bring about Terrorism financing. The bitcoin technology enables international transfer of funds in anonymous manner.¹³⁸ Despite the fact that the original currency purchases like via banking system maybe visible the detection of the rest of the procedures followed in virtual transfers is very difficult. It is very important therefore, for Kenya to create regulations to effectively monitor payments made through the online platforms which has become a common source of terror financing for Al-Shabaab.

¹³⁴ Seth G. Jones, Andrew Liepman, and Nathan Chandler, "Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab," *Rand Corporation*, 2016.

¹³⁵ Ibid.

¹³⁶ United Nations Security Council (2012), "*First report of the analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban and associated individuals and entities*," S/2012/683, 5 September 2012.

¹³⁷ Ibid.

¹³⁸ UNEP (2014), "The Environmental Crime Crisis – Threats to Sustainable Development from Illegal Exploitation and Trade in Wildlife and Forest Resources. A UNEP Rapid Response Assessment," United Nations Environment Programme, Nairobi, Kenya, www.unep.org/unea/docs/RRACrimecrisis.pdf

4.2 Uses of the Internet to Counter Terrorist Activity

The spreading of terrorism propaganda through social media platforms is among the ways through which terrorist groups gain sympathizers, who then start to support them financially. Despite the fact that terror groups use the internet to facilitate their assaults, their availability in the social media platforms helps provide information about them and their illicit plans. The evidence gotten through their internet accounts can be used for investigation and prosecution of the terrorists by the authorities and hence prevent further terror activities.¹³⁹ The Kenyan counter-terrorism agencies can gather relevant information about the activities, targets as well as functioning terror groups from the internet, chatroom and website. In addition, increased use of Internet by terrorists makes it possible to find their electronic data which may be processed for circumvention of terrorist activities.¹⁴⁰

Security departments, relevant authorities and Kenyan intelligence need to come up with more improved means for detecting and preventing terrorist acts through the internet. There is an expansive application of traditional methods of investigation including dedicated translation resources for prompt identification of possible terrorism. Conducting constructive discussions and debates through online platforms may bring about contradicting point of view. This may play a vital role of discouraging potential terrorist supporters¹⁴¹

Counter-narratives information with factual and reliable foundation may be distributed via the online forums through proper discussion, videos and images and videos. Proper conveyance of the messages may bring clear understanding of the grievances such as social and political

¹³⁹Telegraph (2014), "How ISIL is funded, trained and operating in Iraq and Syria (Harriet Alexander and Alistair Beach)," August 23, 2014.

¹⁴⁰ Ibid.

¹⁴¹ Seth G. Jones, Andrew Liepman, and Nathan Chandler, "Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab," *Rand Corporation*, 2016.

situations that lead to radicalization. It will also provide possible alternatives of satisfying various needs rather than through violence.¹⁴² .

An example of such initiative is the Center for Strategic Counter-terrorism Communications which is a US's inter-agency whose aim is to reduce violent extremists by timely identifying the propaganda narratives the online platforms respond with counter-narratives through various digital communications technologies.¹⁴³ In May 2012, for example, this Center reportedly responded within 48 hours to an advertisement on a banner that was distributed by Al-Qaida in the Arabian Peninsula on certain websites promoting terror violence. The center responded by providing a counter-advertisement via the same website and featured the altered version of message that aimed at conveying that Yemen citizens were the victims of the activities of the extremist organization.¹⁴⁴ This counter-narrative campaign incorporated the intelligence unit, the military, the Department of State of the US. For counter-narrative communications, the Center uses social media forums like YouTube and Facebook which helped limit the spread of propaganda.¹⁴⁵ If Kenya can adopt such measures, it will help reduce the number of sympathizers who might be used to offer financial support to the terrorist groups.

4.3 Developing Operational Cybercrime units

One of the best ways through which Kenya can prevent or control Al-Shabaab's mobile and online funding schemes is by developing effective cybercrime units. Increased dependency on

¹⁴² Neumann, P. (2015). "*Remarks on Terror on the Internet*. The White House Summit to Counter Violent Extremism," Washington DC (February 19).

¹⁴³ Keatinge, Tom (2015), "*Identifying Foreign Terrorist Fighters : the role of public-private partnership, information sharing and financial intelligence*," Royal United Services Institute (RUSI).

¹⁴⁴ FATF (2013a), FATF Guidance, "*National Money Laundering and Terrorist Financing Risk Assessment*," FATF, Paris,

¹⁴⁵ Ibid.

computer technologies suddenly raised the “demand for dedicated cybercrime units to respond to forensic retrieval requests for computer-based evidence, rather than just terrorist activities done through the Internet.” The most prevalent cases in which terrorists use the internet include carrying out criminal activities such as human trafficking and drug trafficking. However, in current years there have been an increased case that involve the use of electronic or computer mediums.¹⁴⁶ The operational capability of a state to support such demands can be improved by establishing a national cybercrime unit with sufficient knowledge on investigation of cybercrime. This national units can also gain support from other smaller local units to respond to some regional needs depending on resource and geographical requirements.¹⁴⁷

The roles played by the Kenya’s national cybercrime units includes: (a) collecting intelligence by using specialized techniques for online investigations from social media platforms, internet bulletin board, website and chat rooms in order to identify terrorist and criminal activities. Considering terrorists, this function may be incorporated within the remit of counter-terrorism units where the staff has adequate training to execute the work, but specialist training within a cybercrime environment is regarded very important to play the role. In order to support the strategy development in countering threats from terrorist group’s use of the Internet, the function of gathering intelligence needs proper analysis and evaluation. Even though national intelligence units may have conflicting objectives or roles that may negatively affect harmonization, effective plans of operation can be achieved through translation of the intelligence;¹⁴⁸ (b) carrying out special investigations on cybercrime both in international and national criminal cases related to

¹⁴⁶ Europol (2014), *TE-SAT 2014: “European Union Terrorism Situation and Trend Report 2014,”* Europol, The Hague, Netherlands, www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014

¹⁴⁷ Ibid.

¹⁴⁸ Cohen-Almagor, R. (2017). “Jihad online: How do terrorists use the Internet? *Media Metamedia Management,*” 55-66

technology, including those that involve theft of data or Internet fraud and other cases that involve complex technological applications, law or procedures emerge; (c) providing services as an international linkage and industry such as learning institutions, international and national organizations, government authorities, computer industry, and the telecommunication industry in order to forge strong bonds with the key stakeholders in the war against cybercrime; (d) Maintaining assessment unit to assess national and international cybercrime cases for prioritized investigation by regional and national cybercrime units. This unit may as well be used to maintain statistical data on cybercrime incidences; (e) establishing research, development and training, as the evolving and complexity of cybercrimes require scientific assistance from specialist academic institutions to ensure that regional and national units are sufficiently equipped with required skills, resources, tools, technology, and trainings necessary to perform forensic examination on computerized media and investigating cybercrime.¹⁴⁹

4.4 Establishing Computer forensic triage units

Kenya needs to develop computer forensic triage units that will support national cybercrime units. The staff of these units would require proper training to enable them forensically analyse items in the computer by use of special software applications at the sites where the search is done. A member of a triage team can initially examine the site to either eliminate computers or other computer tools from investigation as lacking in terms of evidence or may seize computer related evidence by use of forensic tools to assist the investigation team in examining the suspects based on the evidence gotten through the computer.¹⁵⁰ If necessity arises, the items

¹⁴⁹ Botha, Anneli. 2014. "Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya. *Studies in Conflict and Terrorism*" 37 (11): 895–919.

¹⁵⁰ Ball, N., "The Evolution of Security Sector Reform Agenda". In Sedra, M. (Ed.), *The Future of Security Sector Reform,*" (Ontario: Canada, CIGI, 2010). Pp. 29-44

seized by triage units may be subjected to full forensic examination by the national cybercrime unit or regional cybercrime unit.

In addition, this unit can help in intelligence-gathering, which is a very important component of counter-terrorism activities. These channels provide information that may be used as evidence during trial or may trigger investigations and hence the suspects' prosecution. There is a need to carefully balance the striking interests between different purposes for gathering intelligence and the different agencies that may use the information.¹⁵¹ For instance, the law enforcement or intelligence services that gathered the intelligence information may need to maintain confidentiality by protecting the source of the information acquired, whereas the court judges may need the information in regard to defendant's right to a fair trial as well as equal access to the evidence presented against him or her. There is need to take cautious measures to ensure that sufficient checks and balances are executed to protect the basic human rights as stipulated in all international accords.¹⁵²

The University College Dublin researchers are trying to develop a variety of forensic software applications that would support preliminary analysis, and will be available free of charge to security officers. The University College Dublin Centre for Cyber security and Cybercrime Investigation and the Computer Crime Investigation Unit has launched these tools as part of its wider strategy meant for assisting underfunded cybercrime units whose budgets are limited and inadequate staff to successfully manage their cybercrime cases.¹⁵³ The main goal of the initiative will be to establish a forensics lab with a totally open source. The investigators taking part in the

¹⁵¹ AUSTRAC (2014), "*Terrorism financing in Australia 2014*, Commonwealth of Australia, West Chatswood, Australia."

¹⁵² UNODC. *The use of the Internet for terrorist purposes*. New York, 2012.

¹⁵³ US Department of State (2015), "*Counter-ISIL Finance Group Kidnapping for Ransom Communiqué*," US Department of State, Washington.

activity will be instructed on how to develop computer processing equipment that that will help in evidence storage as well as receive training on the application of forensic gadgets. The Kenyan security intelligence and counterterrorism units can also borrow such tools to help in thwarting Al-Shabaab's online funding schemes.

4.5 Training Counter-Terrorism Units

Kenyan law enforcement officials who carry out investigations on how internet is used to involved for terrorist activities need special technical training on how criminals utilize the internet for illegal purpose as well as how the internet can be effectively used by law enforcement can to monitor the terrorist activities. Either private sector, public sector or both sectors can collectively be used provide training. Organizations like INTERPOL and Europol can be used to offer programs on cybercrime investigations and IT forensics at the international or regional level.¹⁵⁴ Additionally, some of countries have created their own training programmes on law enforcement cybercrime. These countries have achieved this either on their own or with support from academic entities. Ad hoc courses, conferences and seminars may also be used to provide training in the specific industry or in the public sector.¹⁵⁵

Futhermore, various academic institutions including KU, UoN and JKUAT have begun providing special trainings on Cybercrime. Courses provided by these universities include master's degree in law enforcement forensic computing and cybercrime investigation. Many other courses also help first responders with operational skills in regard to the cases of

¹⁵⁴ Ottawa Citizen (2014), "ISIL using social media to lure young teenagers, accountants, engineers to its cause" (David Pugliese), Ottawa Citizen, Ottawa, December 16, 2014

¹⁵⁵ Ibid.

cybercrime¹⁵⁶ Counterterrorism officers can also be trained through online counter-terrorism programs through platforms such as the UNODC's 2011 Counter-Terrorism Learning Platform. While this platform aims at training practitioners of criminal justice to fight terrorist activities, it creates an interactive environment for the practitioners where they can virtually share their perspectives and experiences to successfully fight terrorism. The platform not only allows practitioners who have trained UNODC to connect and create networks with their counterparts but it also provides them with further learning activities, updates them with legal trends in the field as well as informing them about training opportunities.¹⁵⁷

4.6 International cooperation

Due to the fact that online and mobile terrorism funding schemes are a global phenomenon, Kenya needs to cooperate and seek for cooperation from the regional and international intelligence units to be able to control Al-Shabaab's funding. The relative anonymity, the speed and global reach with which terrorists use the Internet to carry out terrorism, as well as the complexities of the production, retention, seizure and location of Internet data, makes effective and timely international cooperation between intelligence agencies and law enforcement officers a very critical factor in several terrorism cases regarding a successful investigation and prosecution. The relevant resolutions of the Security Council and the international conventions and protocols are the universally used instruments to fight terrorism and have measures that promote international collaboration in prosecuting terrorists.¹⁵⁸ These measures help to ensure that there is mutual legal assistance for extradition, "transfer of criminal proceedings and convicted persons,

¹⁵⁶ Seth G. Jones, Andrew Liepman, and Nathan Chandler, "Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab," *Rand Corporation*, 2016.

¹⁵⁷ Europol (2015), "*EU Terrorism Situation & Trend Report (TE-SAT) 2015*," Europol, The Hague, Netherlands, www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015

¹⁵⁸ Drazen Jorgic, "Kenya suspends bank accounts of suspected funders of terrorism," *Reuters*, April 8, 2015.

reciprocal enforcement of judgements, freezing and seizure of assets and exchange of information between law enforcement Agencies.”¹⁵⁹ The main components that embody international cooperation against terrorism include the responsibility to ensure that terrorism perpetrators face justice; the duty to prosecute or extradite; the responsibility to come up with legal stipulations in defined conditions; the duty to respect human rights and the rule of law; and the duty to respect special rules and international accords.¹⁶⁰

The commonly applicable principles for extradition and mutual legal assistance in terrorism cases or internationally coordinated “crime are part of the universal counter-terrorism instruments and other instruments dealing with transnational organized crime like the United Nations Convention against Transnational Organized Crime.”¹⁶¹ When implemented fully, the mechanism of international cooperation in the universal instruments against terrorism, may create a legal foundation for cooperation in many Internet-related cases. Without the counter-terrorism instrument specifically dealing with terrorism-related issues in the Internet, security officers, when carrying out investigation and prosecution on these cases, will rely on the available regional or international arrangements or treaties developed to facilitate successful cooperation among nations in the investigation and prosecution of transnational criminal offences and terrorism. International cooperation in the investigation and prosecution of internet-related terrorism cases hindered by the lack of specific tools that can deal with internet related issues. The fundamental instrument that deals with adverse trans-national organized crimes among the states is UNCATOC - United Nations Convention against Transnational Organized Crime. International cooperation between states is covered in articles 16 - extradition, 18 -

¹⁵⁹ Ibid.

¹⁶⁰ Botha, Anneli. 2014. “Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya.” *Studies in Conflict and Terrorism* 37 (11): 895–919.

¹⁶¹ Ibid.

mutual legal assistance, 19 - joint investigations and article 27- “law enforcement cooperation of the Organized Crime Convention. Though the criminal acts contained in the Organized Crime Convention only concerns transnational organized crime and not terrorism, its international cooperation principles are similar to those in the universal counter-terrorism instruments.”¹⁶²

4.7 Conclusion

This chapter has looked at the counter-terrorism strategies that can be used to prevent Al-Shabaab’s mobile and online money funding schemes in Kenya. From this, the study found that some of the major strategies employed by the Kenyan security agencies include introducing legal measures to guide online financial companies, use of Internet to counter terrorist activities, and developing operational cyber-crime units. Other strategies include establishing computer forensic units, training counter-terrorism units and international cooperation.

¹⁶² Ibid.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

The previous section has presented counter-terrorism strategies that can be used to prevent Al-Shabaab's mobile and online money funding schemes in Kenya. This section presents the summary of the key findings. It also infers conclusions, which are key in forming study recommendations.

5.1 Summary of Key Findings

This study sought to examine the effects of the Al-Shabaab mobile and online funding on Kenya's counterterrorism measures. The specific objectives included: To examine Al-Shabaab's mobile and online funding schemes in Kenya; To evaluate the impact of Al-Shabaab's mobile and online money funding schemes on counterterrorism measures in Kenya, and; To assess the counter-terrorism strategies that can be used to prevent Al-Shabaab's mobile and online money funding schemes in Kenya.

From the first objective, the study found that Al-Shabaab's funding schemes include online fundraising mechanisms. Methods used by Al-Shabaab to sustain funding schemes include rent collection, siphoning of money meant for mosques construction, appealing to its sympathizers through advanced online communication, especially in Kenya where there is open access to information. Al-Shabaab also derive their finances through trade-based money-laundering from Somali business people in the Gulf. Through Twitter, Al-Shabaab normally find sympathizers in

Kenya through the general population, terrorist sympathizers and the West. Through social media, Al-Shabaab normally create a sense of community or for one-on-one conversations between terrorists and interested parties. Through ICT, Al-Shabbab finds it easier to make payment incentives to potential recruits, besides sourcing for funds. Al-Shabaab notably use Ushahidi and Mpesa for crowd sourcing and mobile payments respectively.

From the second objective, Al-Shabaab's mobile and online money funding schemes impacts Kenya's counterterrorism measures by weakening the "Anti-Money Laundering and Combating the Financing of Terrorism (AML and CFT)" mechanisms. While most African countries, including Kenya, are trying to abide by the international financial regulation measures, they have not managed to contain money-laundering, which Al-Shabaab uses frequently to maintain its financial stability. Al-Shabaab also uses economic incentives to beat Kenya's efforts to rehabilitate youths from violent extremism. While the Kenyan security forces have boosted their counterterrorism measures to reduce radicalization, Al-Shabaab still lure youth into its cause through monetary incentives and other economic benefits.

From the last objective, the study found that while Kenya has developed a number of counterterrorism measures to prevent terrorism activities, there is scarcity of measures to deal with the promotion of terrorism through the Internet, including mobile and online money funding schemes. To fill this gap, Kenya needs to introduce legal measures to guide online financial companies; use the internet to counter terrorist activities, especially fund sourcing through online means; develop operational cybercrime units; establish computer triage units; training counterterrorism units; and initiating international cooperation measures.

5.2 Conclusions

From the study, the following conclusions can be made. First, Al-Shabaab draws their resources from unconventional mechanisms, which include rent collection, siphoning off money meant for mosques construction, appealing to its sympathizers through advanced online communication. While most of their conventional fundraising mechanisms were thwarted, Al-Shabaab find strength in online platforms, which are not easy to detect. Therefore, they can still fund their activities, which include recruiting, radicalization and sponsoring terrorist activities. Second, Kenya's counterterrorism measures are weakened by Al-Shabaab's mobile and online money funding schemes. While Kenya is a signatory to a number of anti-money laundering treaties and online financial control treaties, it has not put enough mitigation measures in place to thwart online money fundraising schemes by the terrorists. Lastly, the study can also conclude that Kenya needs to upgrade its counterterrorism strategies to be able to deal with the online terrorism threat.

5.3 Recommendations

From the findings, the relevant stakeholders in the security sector need to consider the following recommendations:

- a. There is need to solidify the legal framework guiding online financial money transfers. While the Central Bank of Kenya restricts companies that have not registered with it to transact money online, there is need to increase strict measures against companies found contravening this regulation.

- b. There is need for Kenya to develop operational cybercrime units. While cybercrime is still a new phenomenon in Kenya, it has done much damage to the country's socioeconomic fabric. Specifically, the increased rate at which Al-Shabaab is employing online platforms to raise funds is alarming. With active and operational cybercrime units, the Kenyan security sector will be able to nab the online networks involved in raising funds towards Al-Shabaab's activities.
- c. There is need for the Kenyan government to upgrade its security forces training facilities to encompass training on emerging threats or new wars. With the advancement of technology, Al-Shabaab has advanced its tactics, especially adopting online forums to propagate fear and extremism messages. When the relevant security forces are well-trained on how to deal with such, it will become easier to deal with their online fundraising schemes.
- d. Lastly, there is need for the Kenyan security sector to bolster its cooperation with the international community. With strengthened cooperation, Kenya will be able to share and receive crucial information regarding Al-Shabaab activities.

REFERENCES

- Anderson, David M., & Jacob McKnight. 2015. 'Understanding Al-Shabaab: Clan, Islam and Insurgency in Kenya.' *Journal of Eastern African Studies* 9 (3): 536–57.
- Anzalone, Christopher (2016). 2016a. *Continuity and Change: The Evolution and Resilience of Al-Shabab's Media Insurgency, 2006–2016*. Hate Speech International.
- AUSTRAC (2014), *Terrorism financing in Australia 2014*, Commonwealth of Australia, West Chatswood, Australia, www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf.
- Ball, N., "The Evolution of Security Sector Reform Agenda". In Sedra, M. (Ed.), *The Future of Security Sector Reform*, (Ontario: Canada, CIGI, 2010). Pp. 29-44
- Baro, Ebikabowei Emmanuel, & Benake-ebide Christy Endouware. 2013. 'The Effects of Mobile Phone on the Socio-Economic Life of the Rural Dwellers in the Niger Delta Region of Nigeria.' *Information Technology for Development* 19 (3): 249–63.
- Botha, Anneli. 2014. 'Political Socialization and Terrorist Radicalization Among Individuals Who Joined al-Shabaab in Kenya.' *Studies in Conflict and Terrorism* 37 (11): 895–919.
- Carter, J.A., Maher, S. and Neumann, P.R. (2014), *Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, International Centre for the Study of Radicalisation and Political Violence (ICSR), London, United Kingdom ”
- Carmody, Pádraig. 2013. 'A Knowledge Economy or an Information Society in Africa? Thintegration and the Mobile Phone Revolution.' *Information Technology for Development Journal* 19 (1): 24–39.

Coning, Cedric. 2017. Peace Enforcement in Africa: Doctrinal Distinctions Between the African Union and United Nations. *Contemporary Security Policy* 38 (1): 145–160.

Daniel Runde, “M-Pesa And The Rise Of The Global Mobile Money Market,” *Forbes*, August 12, 2015

CGTF (nd), Algiers Memorandum on Good Practices on Preventing and Denying the Benefits of Kidnapping for Ransom by Terrorists, CGTF, <https://www.thegctf.org/documents/10162/159874/Algiers+Memorandum-English.pdf>

Cohen-Almagor, R. (2017). Jihad online: How do terrorists use the Internet? *Media Metamedia Management*, 55-66

Drazen Jorgic, “Kenya suspends bank accounts of suspected funders of terrorism,” *Reuters*, April 8, 2015.

Europol (2015), *EU Terrorism Situation & Trend Report (TE-SAT) 2015*, Europol, The Hague, Netherlands, www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015

Europol (2014), *TE-SAT 2014 : European Union Terrorism Situation and Trend Report 2014*, Europol, The Hague, Netherlands, www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014

FATF (2015a), *Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL)*, (the ‘FATF ISIL report’), FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

FATF (2015b), *Guidance to a Risk-Based Approach to Virtual Currencies*, FATF, Paris, France, www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF (2014a), *Risk of terrorist abuse in non-profit organisations* (the “NPO report”), FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

FATF (2014b), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

FATF (2013a), FATF Guidance, *National Money Laundering and Terrorist Financing Risk Assessment*, FATF, Paris,

Harper, E., “Reconceptualising the drivers of violent extremism: An agenda for child and youth resilience.” (WANA Institute 2018).

Keatinge, Tom (2014), “The Role of Finance in Defeating Al-Shabaab”, *Whitehall Report 2-14*, Royal United Services Institute (RUSI), United Kingdom, December 2014,

Keatinge, Tom (2015), *Identifying Foreign Terrorist Fighters : the role of public-private partnership, information sharing and financial intelligence*, Royal United Services Institute (RUSI).

Neumann, P. (2015). *Remarks on Terror on the Internet*. The White House Summit to Counter Violent Extremism, Washington DC (February 19).

John Cassara, *Trade-Based Money Laundering*, (New Jersey: John Wiley & Sons, Inc., 2016).

Kathleen Caulderwood, “Al-Shabab’s Finances: The Militant Group Gets Funding From Local Businesses, Sources Abroad,” *International Business Times*, September 4, 2014.

Prestholdt, J., “Kenya, the United States, and Counterterrorism.” *Africa Today*, Vol. 57(4), 2011, pp. 3-27.

Sanchez-Franco, M. J. (2010). WebCT—The quasimoderating effect of perceived affective quality on an extending Technology Acceptance Model. *Computers & Education*, 54(1), 37-46.

Seth G. Jones, Andrew Liepman, and Nathan Chandler, “Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab,” *Rand Corporation*, 2016.

Telegraph (2014), “How ISIL is funded, trained and operating in Iraq and Syria” (Harriet Alexander and Alistair Beach), August 23, 2014, www.telegraph.co.uk/news/worldnews/middleeast/iraq/11052919/How-Isil-is-funded-trained-and-operating-in-Iraq-and-Syria.html.

Oftedal, Emilie (2015), *The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment (FFI), Norway, 6 January, 2015, www.ffi.no/no/Rapporter/14-02234.pdf

Ottawa Citizen (2014), “ISIL using social media to lure young teenagers, accountants, engineers to its cause” (David Pugliese), Ottawa Citizen, Ottawa, December 16, 2014 <http://ottawacitizen.com/news/national/defence-watch/isil-using-social-media-to-lure-young-teenagers-accountants-engineers-to-its-cause>.

Scott Baldauf and Ali Mohamed, “Somalia’s Al Shabab recruits ‘holy warriors’ with \$400 bonus,” *Christian Science Monitor*, April 15, 2010

United Nations Al-Qaeda & Taliban Sanctions Monitoring Team, First report of the Analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban and associated individuals and entities.

UNEP (2014), *The Environmental Crime Crisis – Threats to Sustainable Development from Illegal Exploitation and Trade in Wildlife and Forest Resources. A UNEP Rapid Response Assessment*,

United Nations Environment Programme, Nairobi, Kenya,
www.unep.org/unea/docs/RRAcimecrisis.pdf.

United Nations Security Council (2012), *First report of the analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1988 (2011) concerning the Taliban and associated individuals and entities*, S/2012/683, 5 September 2012.

UNODC. *The use of the Internet for terrorist purposes*. New York, 2012.

US Department of Treasury (2015), *United States National Terrorist financing risk assessment*, US Department of Treasury, Washington, United States.

US Department of State (2015), *Counter-ISIL Finance Group Kidnapping for Ransom Communiqué*, US Department of State, Washington.