CYBERSPACE ANARCHY AS AN EMERGING THREAT TO SECURITY OF MOBILE MONEY SERVICES: THE CASE OF M-PESA

BY:

TIKWANG IRIALE FABIANO

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A MASTER OF ARTS DEGREE IN STRATEGIC AND SECURITY STUDIES AT THE DEPARTMENT OF POLITICAL SCIENCE AND PUBLIC ADMINISTRATION, UNIVERSITY OF NAIROBI.

15th October, 2019

DECLARATION

Declaration by Candidate

This research thesis is my original work and has not been presented for any academic award in any other University.

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

TIKWANG IRIALE FABIANO

C50/5215/2017

Declaration by Supervisor

This research work has been submitted for examination with my approval as the University Supervisor

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

DR. PETERSON MAGUTU, PhD

School of Business

University of Nairobi

DEDICATION

I would like to dedicate this work to my family members: My Wife, Nelly Cheposepoi and entire AkÖcho family for their understanding and support during the course of writing this research.

ACKNOWLEDGEMENT

I would like to express my special acknowledgement and thanks to my supervisor Dr. Peterson Magutu for his diligent guidance, encouragement and advice while writing this research. Much appreciation to my friends for their advice and moral support when I needed and more so to Dr. Jennifer Wangari for proof reading and giving guidance my work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS/ACRONYMS

ACS	Australian Computer Society
CBK	Central Bank of Kenya
DBIR	Data Breach Investigations Reports
GDP	Gross domestic product
GSMA	Global System for Mobile Communications Association
IBM	International Business Machines
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IP	Internet Protocol
IoT	Internet of Things
ITU	International Telecommunication Union
KShs	Kenya Shillings
MITM	Man-in-the Middle
OHRP	Office of Human Research Protections
P2P	Persons-to-Persons
SLR	Systematic Literature Review
SMS	Short Message Service
SPSS	Statistical Package for the Social Sciences
STK	Systems Tool Kit (formerly Satellite Tool Kit)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
Tbps	Tetrabits per second
TLS	Transport Layer Security
UNICEF	United Nations International Children's Emergency Fund
US	United States of America

ABSTRACT

Cyberspace anarchy is emerging as a threat to proper utilization of internet despite of numerous benefits it offers. Security has been a contentious issue in the cyberspace because of dominance of non-state actors. Despite security threats creeping into Mobile money services, citizens' reliance on this front is gaining ground since it is driving financial inclusion. Gaps highlighted include: Mobile money service apps had SMS flaws and weak cryptography that allowed spoofing and eavesdropping respectively, in 46 Android Mobile money service apps used by 246 Mobile money providers the apps failed reliable security testing. Despite the deployment of measures to minimize the threat, cyber criminals have been utilizing various security flaws within deployed systems to carry out their crimes on Mobile money services. These flaws inform the basis of this research, which is to determine why the number of cyber-attacks directed at Mobile money services increase with increase in users. Qualitative method especially descriptive techniques as well as quantitative tools were used to adequately analyze data and threats. The research found that Mobile money services like deposits, withdrawals among others were disrupted by the various forms of cyberspace threats. Similarly, the research concluded that perceiving cyberspace anarchy in the lenses of game theory, the security and insecurity nexus within Mobile money services would increase and decrease in pursuit of balance that unfold infinitely, that only requires containment. Therefore, containment measures would include: threats driven solutions and legislations, the creation of multilateral regimes among others.

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

Cyberspace is a boundary-less ecosystem, where no strict lines are defined or enforced, hence, some countries are capable of crossing them thus violating the cyber sovereignty of others (Waldemar, 2017). Similarly, Deibert (2013) defines cyberspace as global communications and data system which is entrenched in all aspects of society, with security of the sphere becoming greatly disputed among countries, the private sector and non-state actors. From the above definitions, Deibert and Waldemar looks at the global nature of shared cyberspace and its contested nature, Waldemar goes further to highlight its borderless aspect.

Waltz (1979) define anarchy as lack of overarching authority to police the international system, which instills a sense of distrust among states, implying, therefore, that the international system is a devolved rivalry among sovereign equals. Similarly, Robert and Jervis (2015) looked at anarchy as the lack of absolute authority within the globe to make laws and settle disputes. From the above authors, the relations of states should be perceived through anarchic lenses. Therefore, the marriage of the two concepts creates cyberspace anarchy, which can be defined as perpetual pursuit of interests online by states or non-state actors with little or no accountability which yields competition and conflict. Although realism as a school of thought emphasizes the competitive and conflictual side of international relations (Sandrina & Isabel, 2017), it fell short to give prescriptions on how to tackle cyberspace threats because it is a new domain of warfare.

Nye (2011) observed that cyber-attacks have low impact, but a successful one on key infrastructure, can have substantial effects ranging from crippling national security to the livelihood and safety of individual citizens, adding that if a country discovers weakness in another state’s information system and only uses it to snoop on classified data of that country, it is espionage that is acknowledged by states as a fair game. Gueldry, Gokcek and Hebron (2019) observed that despite traditional state-centered threats remain of a concern, with espionage, territorial challenges and persistent regional tensions among others being key; the new threats like: climate change, disease and food insecurity among others combine and interact to create intertwining puzzles to state security. A cyber-attack arise when a vulnerability that is yet unknown is exploited. Cybersecurity is not about attaining ideal security but is about curtailing vulnerabilities (Alexander, Seychelle & Alan, 2015). According to Arnold Wolfers, security in objective sense, measures the absence threats to acquired values, in subjective sense, absence of fear that such values would be attacked (Wolfers, 1962). Similarly, Ullman (1983) observes that we may not understand what security is or how important it is until we are endangered with losing it. Thus, cyber security is a loosely idea which is perceived when lost through fraud on Mobile money services.

The extensive adoption of mobile phones in contrast to computers has led to a new age of data exchange (Feizollah, Anuar, Salleh & Wahab, 2015). Kearns (2016) observed that the use of mobile phones in business has been growing as employees use them for communications, creating and editing documents, storage and retrieval of files, and browsing the internet. Despite, the usefulness of mobile phones in carrying out Mobile money services among others, they have created new attack fronts. For instance, Karim, et al. (2015) state that the mobile botnet attacks have been discovered through various malicious activities, like: distributed denial of service (DDoS), theft of corporate data, phishing and designing mobile phones for the illegal transmission of data. Similarly, Cheng (2007) points that the more the functionalities a mobile handset has, the greater vulnerable the mobile handsets becomes to the same types of risks that plague laptops and computers. From the above perspectives, the authors agree on the vulnerability of Mobile money service to attacks which they link to the flaws within Android operating system. In addition, the anarchic nature of cyberspace has enabled threats to evolve unchecked, becoming key tools of settling differences within the international system, hence, this therefore has created insecurity within Mobile money system.

In summary, therefore, emphasizing security at the expense of freedom can suppress innovative potential, since freedom in cyberspace domain without appreciating of cyber threats lead to unacceptable threats to national security. This is because, freedom of the internet and cyber threats arise together in an endless continuum, one cannot exist without the other. Thus, despite its weakness, the cyber domain is a centre for innovation with Mobile money service being one of its outcrops, hence, how can cyberspace anarchy as emerging threats be minimized while at the same time its usefulness being enjoyed.

1.2 Research Problem

Mobile money service transactions have grown due to ease of use and limited banking services to a majority of people. The unbanked populace cites high fees associated with opening bank accounts, compared to nil charges for opening or maintaining mobile accounts, in addition to its availability in inaccessible regions (ITU, 2013). Similarly, Xan (2007) observed that the M-Pesa is in much demand due to the number of Kenyans supporting relatives in rural areas. Elsewhere, Buku and Mazer (2017) observed that Mobile money services like M-Pesa in Kenya and Tanzania have developed into main payments systems that are moving billions of dollars yearly, adding that despite its increasing usage this has also been a channel for fraud and criminality. Therefore, looking at the above perceptive, the authors agree that Mobile money service has been critical in not only facilitating inclusion of the poor into financial system but also it is enabling social support, Buku and Mazer go further to show that criminals have used the same platform for ulterior motives.

Frankline (2019) observed that in Kenya and Niger, Airtel Money service lost KShs. 670 million and KShs. 67 million respectively through insider breaches of Mobile money system which was attributed to technical and administrative weaknesses in Airtel money payment systems, in similar incident, according to Byrone (2019) a Kisumu businessman lost KShs. 229,894 to bank and Mobile phone fraudsters, after making four successive withdrawals via M-Pesa after sending several codes to his Mobile Money phone. Elsewhere, Banzi (2017) pointed that Tanzania government through media outlets has urged its citizens to beware of fraudsters targeting Mobile Money services like Airtel, Tigo, M-Pesa among others, adding that Police are investigating a number of cases across the Country. Looking at the above observations, whie Frankline and Byrone give the dark side of insider breaches, where employees use company weaknesses to perpetuate fraud; Banzi, on the other hand highlight the threats disregard of territoriality. Therefore, the growth of cyberspace threats has increased integrity issues due to challenges of identification and verification of Mobile money users, thus, this research is geared towards minimizing fraud.

Deibert (2013) argued that cyberspace is a complex environment, which becomes more intricate with each passing day. This complexity is attributed to cyberspace anarchy, which is the lawlessness that encourages misuse of virtual resources with no authority to hold actors to account, hence, cyber threats have become form of tools to perpetuate anarchy online.

Kozuch (2018) observed that there has been a twenty four percent rise in banking Trojan infections from mobile apps like the Android/Marcher malware that use automatic installation susceptibilities in Android devices by mimicking genuine applications by issuing fake updates or targeted email/SMS phishing. Similarly, Symantec (2018) argued that risks in the mobile space continue with new malware increasing by 54% in 2017, as compared to 2016, which is worsened by the sustained use of older operating system. From the above outlook, while Deibert highlight the complex nature of cyberspace, Kozuch and Symantec on their part agree on the rising cyberspace threats which they attribute to the design flaws found on applications, hence, attest to uncertainty of security within this domain.

Thus, in view of the challenges above, the dependency levels of Mobile money services by individuals, corporations and e-government services would continue to be a gap that can be exploited by criminals to disrupt, including stealing from customers. Therefore, the aim of the study is to understand the effects of cyberspace threats on security of Mobile money services before proposing on how to minimize such threats through incorporation of security during the design and development of Mobile money applications in order to reduce fraud online.

1.3 Objectives of the Study

The key objective of the research was to determine whether the number of cyber-attacks directed at Mobile money services increase with increase in the number of Mobile money service users. The specific objectives of this research include:

i. To establish what are the forms of threats used to perpetuate cyberspace anarchy within Mobile money service in Kenya.

ii. To analyze the impact of fraud on Mobile money services among users in Kenya.

iii. To establish whether cyber-attacks directed at Mobile money services increase with the increase of Mobile money service users in Kenya.

1.4 Research Questions

i. What are the different forms of threats used to perpetuate cyberspace anarchy within Mobile money service in Kenya?

ii. What is the impact of fraud on Mobile money services among users in Kenya?

iii. Does cyber-attacks directed at Mobile money services increase with the increase of Mobile money service users in Kenya?

1.5 Hypothesis of the Research

In order to achieve research objective, it was hypothesized that due to cyberspace anarchy does the number of cyber-attacks directed at Mobile money services increases with the increase in the number of Mobile money service users. Thus, are cyber threats directed to Mobile money services a function of the number of customers using it?

1.6 Justification of the Research Problem

Mobile phones penetration especially in developing countries has been rising rapidly in comparison to landline phone usage. The entry of Mobile money service has been a game changer for the poor, enabling financial inclusion in developing countries (ITU, 2013). The cyberspace anarchy has been a hindrance to the fully realization of Mobile money service potential in Kenya. Various cyber threats have been used to perpetuate anarchic conditions within cyberspace, for instance, according to Trend Micro (2015) in the previous years, cyber criminals have used ransomware to trick online customers, but with rising trend, attacks have been targeting victim's psyche to make each attack 'personal', either for user or an enterprise, adding that the users' behaviour malware growth is projected to reach 20 Million mark by the end of 2016. This is because the entire cyberspace is envisioned as borderless and states are no longer able to adapt to the so-called Westphalian state system to this domain (Nocetti, 2015). Therefore, this research aims at establishing the various forms of cyber threats used to unleash cyberspace anarchy within Mobile money services within Kenya.

Similarly, the study seeks to understand the extent and nature of challenges affecting Mobile money transfer services, on one hand, and the nexus between the impacts of the cyber threats on these services in Kenya, on the other. Using game theory, proposed countermeasures would be highlighted in order to help in enhancing cyber security. This is because cyber threats and solutions arise together in an endless continuum; one cannot exist without the other. Thus, cyberspace vulnerabilities create a need to patch the software, which give assurance of security until a new vulnerability is discovered. Therefore, forming a chain of security and insecurity, that shows the mutual interdependence of cyber threats and solutions, hence, creating a cyberspace security circle which unfolds infinitely within cyberspace domain. The findings of this research would contribute to the debates in this area as well as adding to the existing literature.

1.7 Theoretical Foundation

This research was approached from the lenses of game theory as espoused by scholars like John Von Neumann and Oscar Morgenstern. John Von Neumann introduced game theory in 1928 for the first time as a mathematical tool, used to define and solve games (Neumann, 1928). Similarly, Neumann and Morgenstern defined a game as a circumstance where two or more participants are in pursuit of certain conflicting objectives (Neumann & Morgenstern, 1953). Thus, the conflicting objectives are induced by the frustration brought about by anarchy within the international system, which encourages state's self-interests in total disregards of others. Therefore, to the authors, if such frustrations are sufficiently felt, states or non-state actors are likely to express their anger using any method including cyberspace threats.

Game theory according to Neumann and Morgenstern (1953) is whereby every player acts in sensible way to resolve a conflicting situation in his own favour. It is thus, the gap between what an actor perceives they are entitled to and that which they are capable of getting, that breeds cyberspace anarchy, which is becoming a challenge for states. Moreover, as Thucydides (1972) argued that in an international politics, the strong do what they can and the weak suffer what they must. Thus, such is the current situation of the cyberspace. For instance, states or individual want to have a secure cyberspace where communications and Mobile money service transactions go without any challenges, but when a cyber-attack occurs it disrupt the ecosystem causing severe damages to those concerned, but in game theory such need to be perceived as a game.

Denis (n.d.) observed that despite aiding in perceiving some game like circumstances and to guide in coming up with strategies for making real decisions, it also clarify why some actions happen in some situations. Similarly, Mihai (2016) argued that in a tactical situation the actions of numerous agents are interdependent. Thus, each agent's outcome hinge on not simply on his actions, but also on the actions of other agents. Elsewhere, Dipak, Prajakta and Yogesh (2016) state that hackers activities have been increasing, thus need for developing detection mechanisms but also ability to prevent it. This theory, therefore, can be used to examine possible scenarios, before taking the best action; thus, aiding in the decision process of the players (Kandethody & Zheni, 2016). This is due to the theory ability to depicts the multi-agent decision situations as games where a player is considered as an entity which take a move with best possible benefit for self (Sheila, Jeff, David, Cristina & Radu, n.d.). Thus, the theory illustrates scenarios by considering it as game which consists of players, where self-interests is key, therefore, as a consequence, anarchy prevails.

Neumann and Morgenstern’s theory rests on the following assumptions: finite number of players, players acts rationally and intelligently, every actor has a specific plan of action, the interests are conflicting among the players and the rules of game are known by the actors, which if questioned collapses. There in lays the Achilles’ heel of the theory since while states may cause cyberspace anarchy at a times due to conflicting interests, some of the cyberspace threats can also be attributed to non-state actors who might not have the enthusiasm to operate as a rational state. For instance, if a non-state actor causes a cyberspace attack due differences in a state policy causing disruption of critical services within another state, it may be hard to identify and prosecute if the targeted state is not in good relation with the country of attack origin. In addition, if there is increase in the number of actors’ as in an actual cyberspace, the theory falls apart; similarly, it simply offers a common rule of logic but not the winning strategy. Similarly, uncertainty within cyberspace being an actual field of contention makes the theory fall apart.

In spite of the shortcomings inherent in Neumann and Morgenstern’s theory, it provides the most useful guidelines to examine the impacts of cyberspace anarchy on Mobile money service through a qualitative and quantitative methodology in order to achieve the best approach in conflictual domain such as the case of cyberspace. This is because theory can be used to explain cyberspace conflict when it involves strategic interactions among rational actors, just like a play, relations among states through trade agreements, electoral campaigns, Mobile money service, cyber threats among others, can be viewed as a game. In addition, it offers a scheme for player’s responses to another player’s actions and is a tool for making reasonable decisions. This would explain for instance why incidences of cyberspace anarchy on Mobile money service are usually preceded by loss of huge sums of money by clients/mobile banks. Therefore, looking from the above view, everything is a game. Thus, the theory is useful in helping in understanding interactions within the international system in which tactics are established by one side to counter the actions and tactics of others.

In conclusion, a game implies interactions among contesting parties with each looking for rewards for actions within an anarchic world. Therefore, this provides a measure by which policies are looked according to their ability to aid in the maximization of one's interests, hence, reinforcing the application of anarchy within the cyberspace domain.

1.8 Definition of Significant Terms

Operational definition of anarchy – Is the number of disruptions on Mobile money services attributed to cyberspace threat(s) with an aim to cause harm, defraud or alter behavior. This definition has been chosen despite realist outlook; to guide this research in understanding the drivers of actions of countries and non-state players within cyberspace domain since the pursuit of interests sometimes becomes conflictual especially where interests of other actors come into play within this space.

Operational definition of cyberspace threats – Is measure(s) deployed to alter the proper functioning of Mobile money service by criminals, non-state actors or states with intent to harm.

Malware – Applications programmed to gain access to and impair a computer without the customers consent (BullGuard, 2018).

Mobile money service transfer - Is whereby client's mobile phone is used for transmission of money by electronic means from one individual to another (Janine, 2009).

Mobile banking - Is whereby phones using text messages transfer funds to other mobile devices within and outside their network (Janine, 2009).

Ransomware – It is a malware that stops or restricts clients from using their systems, either by locking the system's screen or clients' files unless a payment is made (Trend Micro, 2017).

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

The study used a combination of thematic and author approaches in reviewing the literature and is divided into nine sections. The first section delves into the traditional and the rise of new security threats, while the second section looks at conceptualization of cyberspace anarchy. Similarly, the third section discusses security of Mobile money services. In addition, the fourth section looked at Mobile money transfer services in Kenya, while the fifth section traces the origin of the concept of anarchy within the international system before examining the reasons behind its use by states. On the other hand, the sixth section entails forms of cyber threats contributing to cyberspace anarchy and its threat to Mobile money service system. Moreover, the seventh section illustrates cyberspace anarchy as an emerging threat to Mobile money services. Furthermore, the eighth section gives a summary of the empirical review and finally, the ninth section proposes a conceptual framework.

2.2 Traditional and the Rise of New Security Threats

Security is a contested concept with no universally accepted meaning. Security being a contested concept can be looked at from three major different perspectives, which are: realism or traditional, liberalism and Copenhagen school. Realism focuses on the state as the most important and referent object of security, while others sees security going beyond the state. Walt (2002) looks at security from military power standpoint being of central focus. Similarly, Booth (2007) looks at security as ability to pursue cherished political and social values, with freedom from life threats. Elsewhere, Lippmann (1943) argued that a nation has security when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war. Therefore, while Booth, perceived security from threats to values and freedoms, Walt and Lippmann on the other hand looked at security from the standpoint of analysis of threat and the application of military tactics to diminish it. Thus, despite being different in outlook, they are various strands of realism with one underlying theme that ties them all together that is state-centric view of security.

Gueldry, Gokcek and Hebron (2019) observes that despite traditional state-centered threats remain of a concern, with espionage, territorial challenges and persistent regional tensions among others being key; the new threats like: climate change, disease and food insecurity among others combine and interact to create intertwining puzzles to state security. Similarly, Liberalism theory emphasis that: human nature is good and capable of collaboration, evil people are a product of evil institutions and structural arrangements that motivate people to be selfish, war can be reduced by eradicating anarchy that encourage it and war requires collective effort to eliminate it (Keohane, 1988). Therefore, authors look at collaboration and cooperation as tools for addressing anarchy within the international system, since it is the one driving states and individual to be selfish especially when interests intertwine.

Copenhagen school of security proposed by Buzan, Waever and Jaap (1991) challenged the realist state-centric view of security by advocating for its widening, where they looked at security as a particular type of politics applicable to a wide range of issues, with emphasis on how to identify, what is and what is not a security issue. The authors' perceived security depending upon prevailing practices, with a basic idea being a social category that arises out of, and is constituted in, political practice, which is constructivism view, since they believed that social relations make or construct people into the kind of beings they are. Similarly, Wendt (1995) being the main proponent of constructivism theory looked at it as a cognitive, intersubjective process in which identities and interests are endogenous to interaction, rather than a rationalist-behavioural one in which they are exogenous. Thus, while Buzan, Waever and Jaap took a constructivist lens to understand the securitization of threats, Wendt, on the other hand, viewed it as relation between what actors do and what they are.

Although liberalism and Copenhagen school of security look as if they are different, they appreciate that security can better be conceptualized if it is widened to include more actors and referent objects, that is security should embrace people outlook. In a nutshell, therefore, looking at the three conceptualization of security attest to its contested nature, hence, framing it to the emerging cyberspace threats being in a new domain of warfare creates even more confusion because of its disregard of territoriality and the dominance of non-state actors, since territoriality was the key premise of state formation in Westphalia model.

2.3 Cyberspace Anarchy

In understanding the cyber risks, it is critical to remember how cyberspace anarchy is. The internet initial conceptualization was not built for security, because its design and architecture was meant to be free and open for all the humanity. Therefore, the conceptualization and design of the internet and by extension cyberspace did not factor assumption of realism theory that is: the world is anarchic where moralities are not considered and each state is anarchic and thus would protect its self-interest over those around them (Morgenthau, 1985). Realism according to Morgenthau's perception is where state's actions are directed towards keeping, increasing and demonstrating power, which in the era of cyberspace falls short because of its borderless nature. Thus, failure to incorporate man's and societal inherent nature to be selfish in the design creates vulnerabilities which threatens utilization of cyberspace through Mobile money services, hence, despite original assurances and benefits that come with cyberspace, there are those who utilize such trust to advance their interests which are harmful to the greater public using cyberspace threats. Therefore, the use of cyberspace to achieve ulterior motives because of man's inherent nature to be selfish causes insecurity which hinders users' utilization of this domain.

According to Industrial Control Systems (2017) cyber threats are people who attempts illegal access to a control system device or network using an information infrastructure pathway, while Kenya Cyber Security Bill (2016) defines cybersecurity threat as an illegal effort to harmfully impact the security, availability, confidentiality, or integrity of data that is stored on, processed by, or transiting a data system. Similarly, Waldemar (2017) argues that cyberspace has become a boundary-less ecosystem, where no strict lines are defined or enforced, hence, some countries are capable of crossing them thus violating the cyber sovereignty of others. Therefore, from the above definitions', while Alessandro is emphasizing on lack of order, the Cyber Security Bill and Industrial Control, on the other hand agree on the issue of unauthorized access to confidential data, with Industrial Control going further to specify on the intruder to be a person.

Meanwhile, Alessandro (2017) observed that cyberspace is an immaterial realm, where geography and laws do not matter, adding that it is only an extension of telecommunication networks, a matter for inter-governmental fora. Elsewhere, Deibert (2013) defines cyberspace as global communications and data system which is intensely entrenched in all aspects of society, with security of the sphere becoming greatly disputed among countries, the private sector and non-state actors, therefore, clashes with Barry Buzan thought who observed security as the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change which they see as hostile (Buzan, 1991). From the above definitions, cyberspace usefulness is not in question, what is contested is framing it for securitization. While Deibert and Waldemar looks at the global nature of shared cyberspace and its contested nature, Alessandro and Waldemar, on the other hand, agree on its borderless aspect, which is against the perception by Buzan which is based on Westphalian model which is realist in outlook, thus, takes territoriality as key, hence, any challenge to security should be from states and not non-state actors. Thus, cybersecurity, just like other concepts in social sciences, is still contentious term, lacking universally accepted definition.

The concept of anarchy as coined by Thomas Hobbes, some centuries ago, has been utilized by realists in explaining the various actions of states (Waltz, 1979). The author goes to define anarchy as lack of overarching authority to police the international system, which instills a sense of distrust among states, implying, therefore, that the international system is a devolved rivalry among sovereign equals. Similarly, Robert and Jervis (2015) looks at anarchy as the lack of absolute authority within the globe to make laws and settle disputes, while, Arthur Stein looks at anarchy as a trait of global politics where relationships amongst sovereign states are aimed at own self-preservation, with ability to use force if required (Stein, 1982). From the above perspectives, Waltz, Stein, Roberts and Jervis looks at anarchy from the point of lack of international body to make actors accountable in their pursuits and therefore no one to police external coercion.

Elsewhere, Grieco (1988) defines anarchy as the principle power determining the motives and actions of countries, with main focus being power and security, hence, conflictual, even where shared interests are concerned. On the other hand, Powell (1994) looks at anarchy as implying certain behavior where power tends to form in system whether it is made up of tribes, nations, companies or criminal gangs, on the other hand, Helen Milner, for example, asserts that anarchy is a vague concept and that dangers exist since it is an essential fact of world politics (Milner, 1991). While Grieco and Powell, points to factors that shape behavior of the actors within any setting where humans are involved, on the other hand, Milner brings the ambiguity of anarchy in world politics, hence, showing how it is contentious concept. From the above authors, the conception of international politics should be perceived through anarchic lenses, hence, the application of game theory, since states pursue interests in disregard of others. Therefore, the marriage of the two concepts creates cyberspace anarchy, which can be defined as perpetual pursuit of interests online by states or non-state actors with little or no accountability which yields competition and conflict. Although realism as a school of thought emphasizes the competitive and conflictual side of international relations (Sandrina & Isabel, 2017), it fell short to give prescriptions on how to tackle cyberspace threats because it is a new domain of warfare.

The continually developing cyber domain and the increasing connection of devices within different aspects of life have increased threat vectors to users. This is because of the anarchic nature of cyberspace, which has enabled threats to evolve unchecked, becoming key faces of anarchy within the international system. Therefore, due to lack of measures to contain threats, cyberspace risks becoming a Hobbesian state of nature in which those targeted engage in self-help and cyber vigilantism (Alexandra, 2017). Similarly, cyberspace creates the sense that it has become an anarchic playground where users can compete for power over its use with no restraints (Waldemar, 2017). Meanwhile, Elizabeth (2017) observes that Cyber threats have become recognized as global security issues, emanating within a lawless, anarchic cyberspace, adding that cyberspace has challenged the concept of territoriality and given non-state actors dominance. Elsewhere, Myriam (2008) argues that cyberspace is now accepted as a fifth domain of warfare and cyber threats are seen to be of national security concern by states. Therefore, these threats affect the delivery of basic services including Mobile money service, thus, impacting on national security. From the above observations, Alexandra, Waldemar, Elizabeth and Myriam agree on threats emanating from the contested domain of cyberspace, however, Elizabeth goes further to illustrate the challenge to territoriality as conceived in the Westphalian model of the state as well as civil society dominance.

In a nutshell, therefore, the inconvertibility of interests would remain the key factor encouraging states or non-state actors to rely on anarchy as a principle applicable to cyberspace. Therefore, game theory comes handy whereby contesting actors would be looking for rewards for their actions at the expense of other players. Thus, in essence game theory perceives players from the lenses of realism theory, but the theory fall short to specify who the players are?, while on the other hand, realism theory look at competitive and conflict nature of national interest from states perspective. This is because the peeling off of the cyberspace is when you relies its underlying complexity, which is behind the mistrust states or non-state actors have on this new domain. This mistrust emanate from the mutual coexistence of security and insecurity within cyberspace domain with no authority to police it.

2.4 Security of Mobile money Services

Mobile money services have been a key tool in reducing financial exclusion of the majority. According to Claire, Arunjay, Jennifer, Alix and Nika (2014) about two and half billion people globally lack access to recognized financial services, with Mobile money services now offered in 61% of the developing states, with Sub-Saharan Africa accounting for 53% globally, mobile devices are used to: make payments, transfers and savings, hence, devices have aided unbanked. The less developed countries have seen an increasing use of mobile phones more quickly than any other technology in human history (Bossi, 2014). Nielsen (2016) observe that Worldwide, 38% of survey respondents used a mobile application to purchase a product or service online within the past half a year, with Asia-Pacific having the highest rates of mobile purchasing, whereby fifty percent of Chinese, forty nine percent of Indians, forty seven percent of South Koreans and forty six percent of Vietnamese interviewed disclosed that they purchased online within the past six months. Elsewhere, GSMA (2016) affirm that in 2015, 46% of the people in Africa had mobile services, equivalent to more than half a billion people, in 2018 there were 272 Mobile money services distributed in 90 states with a recorded Mobile money accounts rising to 866 million an increase of 20% from 2017, with Mobile money services moving US$ 1.3 billion daily (GSMA, 2019). For instance, Mobile money in Uganda has increased payments and money transfer, with over 30% of the population actively using it and over 200,000 jobs created directly (GSMA, 2019). From the above observations, it can be concluded that the demand for Mobile money service is on upward trajectory, thus, enabling financial inclusivity. However, despite high reception by customers of Mobile money services, the cyberspace threats normally found within laptops and desktop computers would eventually shift to the mobile front.

The benefits of Mobile money service do not end with money transfers. GSMA (2016) observe that in 2015, mobile technologies generated 6.7% of GDP in Africa, an input equally around $150 billion, adding that by 2020, it is expected to generate 7.6% of African GDP amounting to about US$ 210 billion due to expanded usage of mobile services. Similarly, Nielsen (2016) observe that mobile to banking services, for instance: gain access to account data and bills payments, were done with mobile, adding that 47% of global respondents surveyed said they accessed their account balances, among other services through their mobile phones. Therefore, from the above scenarios, although mobile phones come with benefits to states and regions, there are also inherent threats that come with such advancements. For instance, Australian Computer Society (ACS) observes that ten million Android devices have seemingly been infected by Chinese malware (ACS, 2016). Similarly, Buku and Mazer (2017) points that Mobile money service have traits that make them easy to use thus making them to be favoured in developing states, therefore same elements, for instance in carrying out: payments, mobile savings, cross-border and international money transfer services among others make it a favoured conduit for easily perpetrated fraud and scam. From the above outlook, while Buku and Mazer highlight easiness of transacting using Mobile money service, the same traits are what fraudsters utilize in achieving their desired goal, ACS, on the other hand, point to design flaws that come with Android phones especially since most mobile phones used in developing world run on this operating system.

Despite the benefits brought about by Mobile money services, criminals have also exploited some weaknesses within this domain to perpetrate fraud, for instance, Buku and Mazer (2017) have observed that Mobile money has numerous forms of fraud that like: consumer-facing scam perpetrated by agents and scam executed against agents, adding that occurrences of internal scam have led to substantial financial loss to Mobile money providers and users. Elsewhere, Mahlangu (2018) has pointed that MTN warned of SIM swap fraud, urging its customers that they should not to share their security credentials like passwords to anyone in order to process a SIM swap request, adding that one customer so far has lost funds from Mobile money account after fraudulent agents asked for her personal information. Six ex-employees of MTN were charged by Anti-Corruption Court in Kampala for Mobile money fraud where the company lost US$ 3.4 million (Morawcznski, 2015). Similarly, in Rwanda, Tigo lost over US$ 170,000 through an insider breach which utilized a weak Mobile money system. Elsewhere, Communication Authority of Kenya (CA) observed that the National Cybersecurity Centre (NCC) detected cyber threats ranging from denial-of-service (DOS), brute force attacks, malware including phishing attacks; online abuse including fraud and system misconfigurations among others, adding that in the quarter ending September 2018, the NCC detected over 3.8 million cyber threats which was an increase of about 3,789,448 threats from the last quarter (CA, 2018). From the above authors, while Buku and Mazer looked at the two angles in which fraud happens in Mobile money, Mahlangu and Morawcznski, on the other hand, pointed to insider breaches and customer-facing fraud as where money was lost. Similarly, CA highlighted the different forms of cyberspace threats that were employed to perpetuate anarchy and fraud online. The table 2-1 below illustrates.

Table 2-1: Cyber Threats Detected (Communications Authority of Kenya, 2018)

Cyber Threats Detected No.	**Cyber Attack Vector**	**Jul -Sep 18**	**Apr-Jun 18**
1.	Malware attacks	1,844,897	1,665,961
2.	Web application attacks	1,064,971	771,518
3.	Botnet/DDOS	911,298	1,023,388
4.	System Misconfiguration	2,548	932
5.	Online Abuse	158	647
6.	Online Impersonation	196	34
Total Cyber Threats		**3,824,068**	**3,462,480**

Elsewhere, Serianu (2017) observed that in 2017, Kaspersky blocked 51 million attempts to open a phishing page, with over 20% of these attacks targeted banks among other financial organizations, adding that with the evolution of phishing, basic awareness training may not be sufficient to safeguard your organization. The author goes to point that in March, 2017 a man was charged with hacking Kenya Revenue Authority (KRA) system and causing a loss of KShs. 4 billion, in addition, the man was suspected of hacking into Safaricom's systems. Similarly, Akomea, Andoh, Frimpong and Dwomoh (2019) in their study Control of Fraud on Mobile Money Services in Ghana, found that in Mobile money services fraud is caused by: weak internal controls and systems, lack of sophisticated technology tools to detect the menace, inadequate education and training and the poor remuneration of employees, thus, proposed legal code and internal fraud policy to be used by Mobile money service providers and partner banks. Elsewhere, in 2017, 86% of all vulnerabilities had a patch available on the day of disclosure that is slightly higher compared to 81% in 2016 (GSMA, 2019). From the observations above, while Serianu highlight how cyberspace threats can be used to defraud companies, Akomea, et al. on their part points to common weaknesses encouraging fraud within Mobile money services, despite GSMA pointing out that such challenges are addressed as they are discovered.

According to ITU (2013) Mobile money service transfers require client to give the money to a remittance centre on a fee, and then centre transmits the money through the phone service provider network to the receiver's mobile. In addition, mobile banking is whereby phones using text messages transfer funds to other mobile devices within and outside their network. Interoperability is seen as the capacity aimed at transferring money between different Mobile money service accounts and across different Mobile money service providers and as well as from and to banks accounts (Marc & Steffen, 2016). Looking at the above perspective, mobile has been a critical element in the growth of economies around the globe.

In addition, therefore, the growing calls for interoperability by Mobile money service providers have caught banks off guard due to stringent measures associated with banking institution. Thus, Mobile money services have been a technological gift to the underprivileged that were left out of recognized financial systems. However, despite its enormous possibility of offering financial inclusion through the mobile front, cyberspace anarchy continuous to emerge as a threat to Mobile money services through shared technology vulnerabilities since it widens attack space, giving criminals a broader attack vector for launching cyber-attacks.

2.5 Mobile money Transfer Service Providers in Kenya

William and Claudia (2017) observed that there are about seven Mobile money service transfer systems in Kenya, which include: M-Pesa, Airtel Money, Equitel, Mobi Cash, Orange Money, M-Coop Cash and Yu Cash. Similarly, Alliance for Financial Inclusion (2010) note that the M-Pesa Mobile money service transfer was conceptualized in 2005 by Safaricom and started operations in March, 2007. Despite, being the first in Kenya, Xan (2007) point that Globe Telecom and Smart communications have been transferring money in the Philippines since 2005. William and Claudia (2017) goes to state that Safaricom has partnered with some banks to allow clients access their accounts, in addition to making transactions, citing that M-Shwari, a platform for saving and borrowing money as an outcrop of such partnership. In addition, Airtel Money has strived to increase its client base by offering cheaper rates. Similarly, Equitel transfer service was launched by Equity Bank with key intent of serving more Kenyans who are tired of the idea of waiting in line in banks to access their cash (William & Claudia, 2016). On the other hand, Mobi Cash is a transfer service offered by Kenya Commercial Bank, with various agents across the country to enable its clients get the services that they need. M-Coop is a money transfer service operated by Co-Operative Bank using Safaricom network. Elsewhere, Orange Money and Yu Cash despite their affordability rates to Kenyans, they closed their services after Orange pulled out of their partnership with Telkom Kenya and Yu was sold. The table 1 below illustrates Mobile money service transfer services showing key indicators.

Table 2-2: Mobile money Transfer Services per Operator (Communications Authority of Kenya, 2017)

Service	July – September, 2017						
	Agents	**Subscriptions**	**Number of transactions**	**Value of transactions (Kshs)**	**Mobile commerce transaction**	**Value of mobile commerce (Kshs)**	**Person to Person transfers (Kshs)**
M-Pesa	148,107	22,790,752	428,766,641	1,334,737,016,674	295,298,839	478,403,156,750	448,148,241,300
Airtel Money	14,038	1,632,580	2,468,625	1,151,036,654	2,572,199	2,283,774,337	862,755,908
Equitel Money	-	1,908,083	104,794,588	322,416,284,883	54,552,342	233,627,382,789	94,380,691,295
Mobikash*	16,749	1,772,696	815,881	127,032,829	6,430	9,227,168	22,876,608
Mobile Pay	5,643	88,883	397,080	1,458,055,912	-	-	767,174,277
Total	184,537	28,192,994	537,242,815	1,659,889,426,952	352,429,810	714,323,541,044	544,181,739,388

Looking at the above data M-Pesa with 22.8 million subscribers, or 80 per cent market share, with a total of 428.8 million transactions (sending and withdrawals) valued at KShs. 1.33 trillion. Equitel, run by Equity Bank's Finserve has 6.8 per cent share (1.9 million), while Mobikash has a 6.3 per cent share (1.77 million). Airtel money has dropped to a share of 5.8 per cent as of September, with 1.6 million customers. Telkom Kenya has just introduced it's T-cash which is yet to shape the Mobile money service market. Thus, from the above observations, the continued growth of Mobile money service is closely linked to allowing interoperability as well as a good formal financial system, hence, bank branches are a critical part of the Mobile money service ecosystem.

In summary, Mobile money service interoperability if implemented successful will enhance financial inclusivity since monopoly of Mobile money services will cease to exist. Therefore, Mobile money service transfer progress in Kenya, as in the continent, has been notable, even amongst the rural poor, since financial inclusion has always been a mirage for most households, despite being majority of the population

2.6 Origin of Anarchy within International System

Flint (2017) observes that starting in the 17th century, anarchy begun to get the attention of philosophers. They talked about anarchy, what it was and what it meant. Thomas Hobbes understanding of it as human's natural state where each man could pursue its interest in disregard of others, including taking of other human being's life (Flint, 2017). Thus, total chaos, therefore, the interpretation is still a general view of anarchy to date. Similarly, Waltz (1979) observes that in a state of anarchy within an international system, defining feature is a self-help system: as a last resort, a state has to rely on itself to promote its security and welfare. From the above view of anarchy, therefore, states had no choice but to constitute and enforce some order, which is famously understood as Westphalia order. Despite this order, game theory came into play in each action by states, whereby actors within the international system resolved conflicting situations in their own favour as stipulated by Neumann and Morgenstern (1953).

In order to best understand factors that fuel use of anarchy by states, the conceptualization of state formation during Westphalia treaty is critical. The Peace of Westphalia treaty had ended the thirty years' (1618-1648) war in Europe (Flint, 2017). The author goes to state that the first treaty was an accord among the Roman Emperor and the King of France signed in Münster city; while the second, involved the Emperor and the King of Sweden signed in Osnabrück city. Thus, Westphalia treaties aim was to cure the problem of anarchy brought by the conflicts over religion, hence, became the first diplomatic discourse which initiated a new order in central Europe based on state sovereignty. The sovereignty conceived at Westphalia is based on: territoriality and the elimination of external actors from internal control of a state. Therefore, this sovereignty was conceived from realist dimension, in which the state is key entity, thus, would perceive the international relations from anarchic lenses, hence, would protect its self-interest over those of other states (Morgenthau, 1985). Consequently, the principle of treaty, of non-intervention in the national affairs of a state is being challenged by cyberspace anarchy. This is because, cyberspace domain not only disregards territoriality but also its control is beyond the state since its continued growth is initiated more by individuals and non-state actors than by states, thus, in such scenario of conflicting interests by states, non-state actors and individuals, game theory is best placed to explain the actions of actors.

Although Westphalia brought some form of order among people within states, anarchy continued to be exploited by states. This is because, states' pursuit of their national interests at the expense of others, make international system very conflictual, due to lack of an overarching authority to make states comply with what is agreed. Eriksson and Giacomello (2006) define state sovereignty as adequate control of the national territory and of the population living within it. Similarly, Scott (2014) argues that state sovereignty should be conceived not as an application of state control but of state authority. These two different interpretations of state sovereignty show the distinctness in the focus of the two major schools of thought in international relations and thus, embody the intricacy of the debate. As Waltz (1979) argue that the idea of anarchy within the international system forces states to arm themselves and seek allies, in readiness to thwart threats instead of collaboration. Thus, in a state of anarchy within global affairs, commitment to cooperate is not guaranteed. Therefore, while the liberalists put emphasis on the aspect of state control as indicator of state sovereignty, realists focus on the aspect of state authority. Thus, from the two schools of thought, the view of state sovereignty becomes conflicting, therefore, making interstate relations to be based on anarchy which is present within the cyberspace domain. Although elite theory can also explain dominance of elites in a state, such theory envisioned only elites and masses, hence, falls short of envisioning elites in terms of cyberspace domain, therefore, game theory comes at handy.

2.7 Forms of Cyber Threats Contributing to Cyberspace Anarchy

Mobile phones are becoming key within a firm since they deliver incredible business value through effectiveness and improved communications (Kearns, 2016). Similarly, Feizollah, et al. (2015) observe that the pervasiveness of mobile phones is proven since they have ushered new possibilities in people's life, adding that, the current mobile phones are more powerful than computers used a decade ago. Thus, with increase of mobile phones usage so is the increase in threats directed at them. According to Secureworks (2017) the major security problem is understanding, since the risks businesses consider they face are frequently very different than the risks that pose extreme threat, saying that, occasionally firms call for the deployment of public key infrastructure (PKI) or an enterprise-wide intrusion detection system though what is needed is better patching. Thus, while Kearns and Feizollah, et al. agree on the benefits of mobile revolution, Secureworks , on the other hand, identify lack of clarity on cyber threats by companies to be a big challenge. Therefore, as Wolfers (1962) observed security in an objective sense measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values would be attacked. In this sense therefore, the presence of cyberspace threats curtailing the smooth usage of Mobile money service is a challenge to states.

Despite various cyber threats, this research would discuss seven types: distributed denial of service (DDOS), ransomware, socially engineered malware, password phishing attacks, unpatched software, social media threats and Advanced Persistent Threats (APT).

2.7.1 Distributed Denial of Service attacks (DDOS)

It is whereby devices send enormous amount of packets beyond network capacity and causing congestion and losses, thus disrupting genuine traffic (Geva, Herzberg & Yehoshua, 2014). Similarly, Australian Computer Society (ACS) points out that DDOS attack took down United States Congress website for three days (ACS, 2016). The author went further to state that in August, 2016 the world witnessed the largest DDOS attack which knocked down OVH, French Internet Service Provider, suffering an attack that transmitted a record of 1 Tbps, enough to disrupt businesses anywhere globally. Thus, looking at the above perspectives, Geva, et al. highlight the attack aim of exhausting the resources (CPU power, memory and bandwidth) of the target, in order to deny legitimate clients access, ACS on their part gives instances where such attacks have been demonstrated successfully.

2.7.2 Ransomware

It is where resources are locked by denying clients' access. Symantec (2015) observe that two forms of ransomware circulating are: crypto and locker, adding that, crypto purpose is to encrypt data and files; while locker is intended to lock a computer, inhibiting users from using it. According to Kaspersky they protected 35,413 Android clients from mobile ransomware in April 2014 to March 2015, adding that, a year later it increased to 136,532 users (Kaspersky, 2016). Similarly, Skybox Security (2018) points out that traditionally, malware have fallen into distinct categories: ransomware, banking Trojans, worms among others, but now those divisions are disappearing and attacks are using multiple elements to evade detection, spread and to reach their goal, giving an example were both WannaCry and NotPetya started ransomware attacks before graduating to worms. Therefore, from the above discussion, Symantec gives the common forms of ransomware in circulation, Kaspersky on their part highlight the number of customers that have been targeted by ransomware in a year, while Skybox security looks at evolution of ransomware until now there is a blurring distinction between worms, Trojan horses and ransomware and its capacity to evade detections.

2.7.3 Socially Engineered Malware

It is software that urges the customer to install some application in order to have access to site, run bogus antivirus application, or run some "critical" program that is mischievous (Secureworks , 2017). Skybox security (2018) observes that in 2017 social engineering have risen with spear phishing being the favoured method, where communication is tailored to each victim: for instance, human resource professionals may receive a malicious file that appears like a resume. Thus, while Secureworks gives what socially engineered malware can do, Skybox security on their part points to how such malware have risen and have become client specific.

2.7.4 Password phishing attacks

It is sending emails to many people requesting for sensitive information (like bank details) or encouraging them to visit a bogus website (National Cyber Security Centre, 2015). Australian Computer Society (ACS) observe that 63% of breaches are caused by weak, default, or stolen passwords (ACS, 2016). While National Cyber Security centre looks at definition, ACS on their part observes how the attacks have been perpetuated.

2.7.5 Unpatched software

A flaw is unintended functionality (Cert-UK, 2015). Similarly, National Cyber Security Centre (2015) observes that a flaw is unforeseen functionality, this may either be a result of poor design or through errors made during implementation. The author goes further to state that in the last one year nearly 8000 unique and confirmed program vulnerabilities were revealed in the United States National vulnerability database.

Similarly, Secunia (2015) observes that 2014 saw a dramatic increase in the number of discovered zero-day vulnerabilities, 25 zero-day vulnerabilities in all products, compared to 14 the year before. Zero-day vulnerability is a vulnerability that is being actively exploited by hackers before it is publicly known. Therefore, Cert-UK and National Cyber Security Centre agree on the definition of the unpatched software, Secunia on their part points to the drastic increase of zero-day vulnerabilities and subsequent exploitation by criminals.

2.7.6 Social media threats

This happens through a rogue friend or program that set up request, thus, enabling the rogue friend more access to your social account than you wanted (Secureworks , 2017). ACS (2016) points out that even the most hardened system can be breached through social engineering, the 'hacking' of people. The author goes to state that no amount of secure network topologies and firewalls or security software can withstand a user innocently clicking on an email link. While, Secureworks highlight how clients end up being persuaded through social media, ACS on the other hand, points to the client being the weakest link within cyberspace domain.

2.7.7 Advanced Persistent Threats

This happens after a successful socially engineered Trojans or phishing attacks (Secureworks , 2017). The author further observes that a common means is when a Trojan attachment in the email is opened, its execution aid infection of the first computer, enabling the infection of all of the devices within that network.

Despite, the constant evolution of cyber threats, the source of the threats remains the human element. This is because either somebody has a motive of attacking a system while another falls to his/her tricks.

2.8 Cyberspace Anarchy, an Emerging Threat to Mobile money service

Cyberspace has political, legal and social dimensions and implications. Despite, the various dimensions, Arunesh, et al. (2015) assert that security is a key concern around the globe since protecting cyber domain from threats by other nation-states and criminals like terrorists is of essence. Similarly, Joubert (2010) notes that cyber-attacks are emerging as new type of threats which nations would face going forward, adding that conflicts within cyber domain are becoming part of more traditional battles, and thus, nations require strategies to protect their networks against growing cyber threat. On the other hand, World Economic Forum (2016) observed that cyber risks remain difficult to measure in spite of over a decade of effort to know and craft suitable response to them, adding that the threat actors vary as do their motives, making it a challenge to predict and quantify the effects of these threats that are getting stealthier and more continuous. This trend is also observed by Sassen (1998) who asserts that the internet is a medium for non-elites to link, support each other's fights and form insider groups at levels going from local to global. From the above outlook, Arunesh et al and Joubert points to the emerging security implications brought about by the persistent cyberspace threats, Sassen, on the other hand, points to the borderless nature of the domain to be key advantage utilized by non-state actors. Similarly, World Economic Forum looks at the difficulty of crafting an adequate response to cyberspace threats. Therefore, perceiving the cyberspace threats from the outlook of the game theory as Neumann and Morgenstern (1953) envisioned, the self-interest is key. Thus, as a consequence anarchy is likely to prevail.

Castle, Pervaiz, Weld, Roesner and Anderson (2016) in their study looked at 197 Android apps and 71 products to assess specific organizational practices to examine security challenges facing Mobile money services, in which they concluded that although attack vectors are present in many apps, service providers were making intentional, security-conscious design decisions. Similarly, the authors argued that an in-depth analysis of Mobile money service apps uncovered the most alarming threats include Short Message Service (SMS) spoofing, SMS interceptions on the network, man-in-the-middle (MITM) attacks and external libraries, which track users within a context where privacy, perceptions are not well understood, adding that other concerns were unauthorized access from stolen devices. The authors went to state that the vulnerabilities may arise due to unique regional factors, that is the servers and specifications may be managed by multiple stakeholders with different requirements, resulting in restricted coverage of the threat model. While the study revealed that the developers of the applications had limited threat model since they only considered protecting the organization from fraud rather than protecting the customers, the study fails to address security threats from client perspective side since they are the most affected in case of a breach. Thus, this research, however, makes the customer key center of Mobile money service security provisions, hence, it looks at how online fraud can be minimized if not completely eliminated.

Butler (2017) looked at Security and Privacy Challenges for Mobile money service Applications uncovered significant security problems like eavesdropping and weak cryptography on mobile phones and 2G cellular networks, arguing that the movement to modern data networks and smartphones offer tremendous opportunities for improvement. The author goes to observe that in an automated analysis they performed almost 50% of apps had a critical Transport Layer Security (TLS) vulnerability, while in 2015, only 9.3% of all the 46 Mobile money service apps analyzed had problems discovered statistically. Further the author looked at the manual analysis in which 6 out of 7 Mobile money service apps had easily exploited critical vulnerabilities which resulted in 28 vulnerabilities that could be exploited to steal money, with a conclusion that Mobile money service systems fail to safeguard user data confidentiality and integrity. Like Castle, et al. (2016), Butler seems to agree on the increasing cyberspace threats directed at Mobile money service users through a variety of ways, the key among them is through Mobile money service apps, but the authors fall short of addressing fraud brought about by anarchic conditions within cyberspace.

Kozuch (2018) in his study looked at Android/Lokibot malware, which takes all the functions of Android/Marcher and adds crypto-ransomware capabilities, including crypting files, locking devices, impersonation of the victim’s IP address and sending notifications to trick users. The author observed that Android/Lokibot has targeted more than 100 financial institutions around the world, adding that they estimated Lokibot has generated close to US$ 2 million, in addition, another increasing tendency is counterfeit mobile banking applications, intended to steal account credentials and login details from customers when mistakenly download the application. Despite, the in-depth analysis of the threat environment, the author highlighted: use of threat intelligence in taking proactive approach, evaluation of risks, leveraging of automation tools, tracking threats specific to the organization and offering cybersecurity training as ways of enhancing security. Thus, the author failed to explicitly look at cyberspace anarchy as an emerging threat to Mobile money service. Therefore, this research looks at how cyberspace anarchy can contribute to insecurity facing Mobile money services around the country as well as globally.

Reaves, Scaife, Bates, Traynor and Butler (2015) on the other hand looked at Mobile money service, mobile problems, in their studies they focused on claims that Mobile money service is a more secure option to cash with first emphasis being on an in-depth analysis of 46

Android Mobile money service apps across 246 Mobile money service providers and they demonstrated that their findings failed to provide reliable insights into its security. Secondly, the authors looked at the design of the registration, login and transaction measures of 15% of these applications and uncovered weaknesses spanning from botched certification validation, do-it-yourself cryptography among others, that allow an attacker to imitate genuine customers, modify transactions inflight including getting financial records. This observation above suggests that despite the alleged claims of a secure Mobile money service environment, there is still vulnerabilities which can be attributed to anarchic nature of cyberspace which makes identification and verification of clients a difficult endeavour, which this research looks at addressing.

Masamila (2014) looked at the explosion of mobile banking technologies that has led to absence of unified protocols that can be responsible for a worldwide mode of mobile banking, adding that the mobile payments applications are intricate in nature, hence, creating complexity especially with the involvement of multiple players. In bold contribution to this debate, Masamila argued that interoperability of mobile banking systems would hasten financial inclusion by permitting clients to use the deployed systems from multiple service providers to access their account, despite, Mobile money service threats. Therefore, this research aims at giving an illustrative account on how cyberspace as a source of threats to Mobile money services continues to evolve because of the anarchic nature of the domain, since as observed by Mihai (2016) in a game theory, actions of numerous agents are interdependent, thus, one actor action informs the course the other would take.

Due to the above scenario, cybersecurity has become a pressing policy issue, with national security community focusing more closely. The economic espionage has existed at least since the industrial uprising, but the scale of modern cyber-enabled aggressive data theft is an unparalleled (Friedman, Austen, & Ross, 2013). Nye (2016) observed that maintaining security is a responsibility of government, and increasing cyberspace threats would lead to more enlarged role of governments in the domain, adding that states and non-state actors collaborate and contest for control in this intricate arena of cyberspace urging for global collaboration in the area of cybercrime, since the likelihood of unified governance on cyberspace regime would continue to remain a mirage. Looking at the above arguments, Friedman, Austen and Ross points to the data theft that has being part of human nature from the beginning, Similarly, Nye perceived cyber security from the lenses of Westphalian model, which is a realist perspective to security, which cyberspace through its borderless nature has challenged. Thus, he goes further to suggest the incorporation of liberal theory ideas, for instance, those that calls for everybody to be brought on board (Meiser, 2017). Therefore, despite difference on agreement on how to govern cyberspace, this research would look at how and in what ways can secure Mobile money services be implemented, since cyber threats would continue to persist going forward due to anarchic cyberspace which is encouraged by its borderless nature.

In financial world, market liquidity is seriously reliant on certainty of the security and reliability of clearing and settlement plans for funds and financial instruments. World Economic Forum (2016) observed that if not handled securely, the legal and financial operational risks intrinsic in payment, clearing and settlement actions have the probability to cause interference in the financial system within an economy. For instance, Masamila (2014) observed that in 2013 there were 219 Mobile money service distributions worldwide with 203 million subscribers in 84 countries, saying that Africa was leading with over 123 mobile banking deployments, representing 52%. Thus, cyber threats to mobile financial transactions can shatter its reliability; hence, becoming a national security risk, therefore, the reliability of mobile financial systems is key to their ease of use and acceptability. From the above observations, while Masamila highlights mobile banking growth, World Economic Forum, on the other hand, looks at the evolving cyberspace threats and its implications on the economy of states. Thus, for the reliability of financial systems including Mobile money services to be effective, the ideas of idealism theory needs to come into play since it seeks to transcend anarchy by, for example, looking at cooperation as key and the believe that you cannot resolves conflict without having other states (Vitor, 2017).

The research above examined the short falls in addressing the cyberspace anarchy on Mobile money service. This research therefore, seeks to establish how cyberspace anarchy as an emerging threat on Mobile money service can address fraud wrought by this condition and as such it aims at filing the gap in knowledge by incorporating the game theory examined in the previous chapter. This would guide in understanding cyberspace anarchy as an emerging threat to Mobile money services and as such the game theory involves actors who chooses actions and outcomes with best probable reward for self (Sheila, et al., n.d), in order to come up with policy prescriptions to address the problem of cyberspace anarchy within the domain.

2.9 Summary of Empirical Review

This chapter has traced the origin of anarchy within the international system as well as drivers of state cyberspace anarchy which is attributed to deeply held differences on how national interests are approached. The pursuit of national interests, informs the sectors to which security is applicable and the possibility of moving from realist logic of security, which is mostly apprised by anarchy to a more cooperative one having liberal theory ideas. As this chapter shows, there is need to identify the most valuable information assets and prioritize protection of this high-value data and improve processes for earlier detection, reduce the time from detection to respond. In addition, there is a quite strong evidence for seeing states converging in defending cyberspace if cyber-attacks due to its anarchic nature, threaten the very existence of freedom across the globe, despite their obvious political differences on the concept of cyberspace. There are certainly disagreements, bordering at times on preferred priorities and policies by states and non-state actors; although at the extremes there are different views of how to define the problem.

2.10 Conceptual Framework

The proposed conceptual framework was meant to map cyber threats to increase of Mobile money service users.

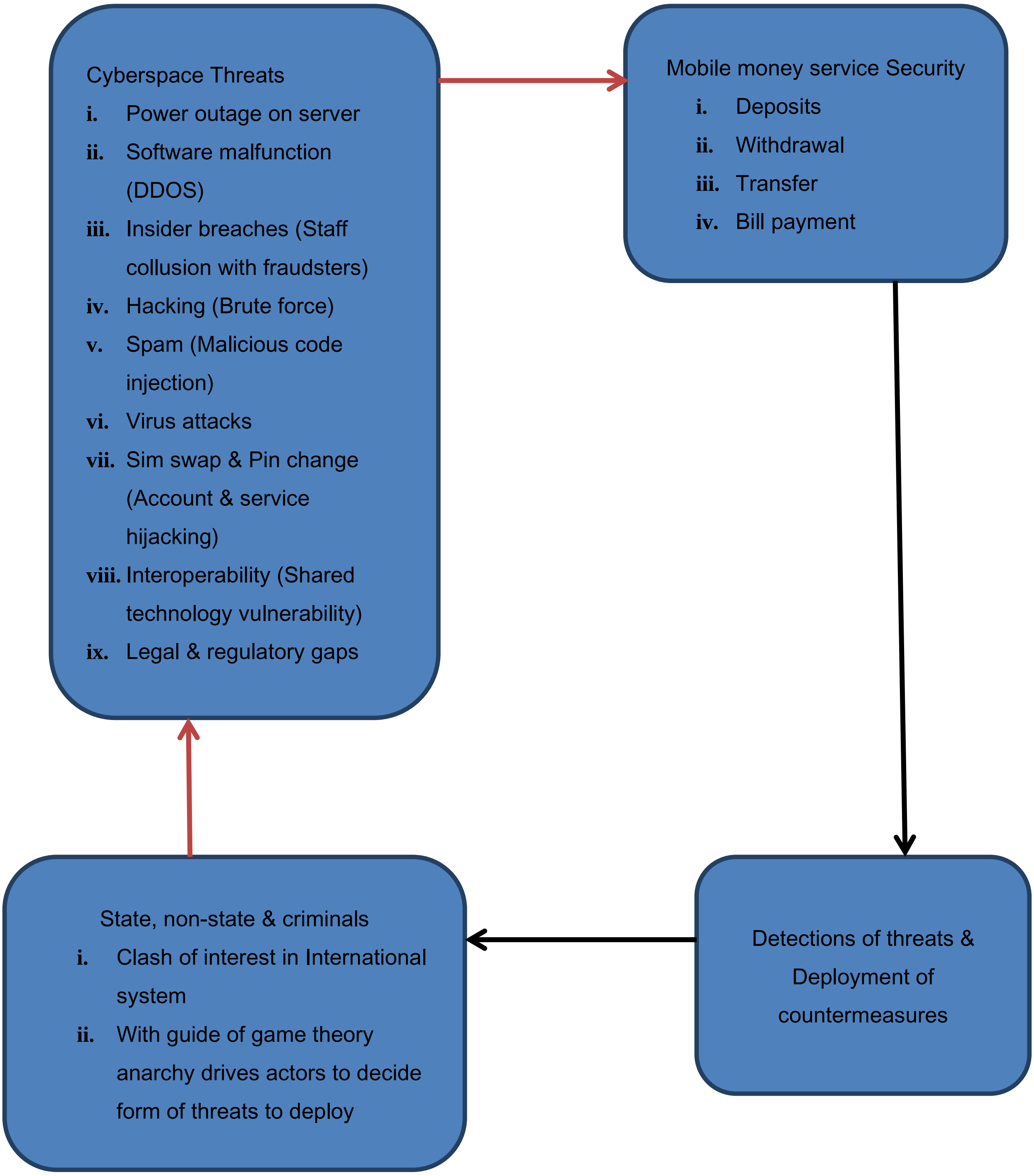
Cyberspace Threats
i. Power outage on server
ii. Software malfunction (DDOS)
iii. Insider breaches (Staff collusion with fraudsters)
iv. Hacking (Brute force)
v. Spam (Malicious code injection)
vi. Virus attacks
vii. Sim swap & Pin change (Account & service hijacking)
viii. Interoperability (Shared technology vulnerability)
ix. Legal & regulatory gaps
Mobile money service Security
i. Deposits
ii. Withdrawal
iii. Transfer
iv. Bill payment
Detections of threats & Deployment of countermeasures
State, non-state & criminals
i. Clash of interest in International system
ii. With guide of game theory anarchy drives actors to decide form of threats to deploy

Figure 2-1: Proposed cyberspace security circle

Taking from the observation of conceptual framework, a secure Mobile money service transfer service is envisioned, but because of clash of interest within international system (IS), actors are forced to use cyberspace to settle differences. This is because the mistrust within the international system makes cyberspace anarchy the only option available for states to rely upon. Thus, cyberspace anarchy drives actors to decide the form of attacks to use and with help of game theory, design of cyberspace threats and subsequent launching. The detection of Mobile money service threats compels the organization to seek for countermeasures including prosecution of the individual involved in collaboration with other states. Therefore, cyberspace anarchy creates insecurity, which with a few patches of the systems (software or hardware) guarantees security, hence, they mutually coexist, thus, cyberspace security creates cyberspace insecurity and vice versa, therefore, creating cyberspace security circle.

Consequently, through this chain of security we can be able to have a predictive outlook, hence, have readiness to minimize the circumstances of the attack. Therefore, in cyberspace security, the game theory envisage that there is an interplay of skill and chance, whereby so much reliance on skill makes it tiresome for actors, while on the other hand, exploitation of only chance makes the game to be boring to the actors. Thus, there is need for intermix between skill and chance; this is because cyberspace geometry keeps changing with each new security solution that is deployed, thus, security and insecurity nexus in cyberspace increase and decrease in pursuit of balance that unfolds infinitely, hence, need for a contained anarchy within this domain.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This section is divided into five parts: the first section would delve on research design methods and why they have been chosen. The second section dwells on population sampling, while the third part would involve data collection methods. The fourth section entails data analysis while the fifth section gives a summary of the chapter.

3.2 Research Design

The research design used both descriptive as well as explanatory research aspects. The descriptive study was essential in understanding of the context and how it informed in the filling of existing gaps. Thus, answering the question “what is” and “what was”. Descriptive aspect provided the frequencies of the use of cyberspace threats as forms of creating anarchic conditions within M-Pesa platform. The research used descriptive method to understand the facts and dimensions of the phenomenon of increasing use of anarchy within cyberspace especially to disrupt or defraud users of Mobile money services within the international system. Similarly, explanatory study focused on why cyberspace anarchy? Therefore, it helped in examining the trends within the international system and how this informed in the answering of the research objectives. In essence, the ‘why’ in cyberspace anarchy guided in the development of casual interpretation on why cyberspace threats are gaining attention among states and non-state actors more so in the past few years than during the last two decades since internet inception. Thus, giving insight on the reasons that may have fueled this trend hence provoking action. In addition, this study adopted both the qualitative and the quantitative techniques in guiding the research, because each used different aspects in addressing the research objectives.

The use of Systematic Literature Review (SLR) as well as survey methods was also employed in this research. This was because SLR assisted in giving a summary of the literature related to the study questions in order to determine the key words that formed the basis of the study topic. These words were used in Google Scholar among other University online resources to identify papers related to the research questions. The analyzed literature guided in answering the study questions. The literature reviewed was on published Journals, books as well as other research papers on the study topic.

Survey method was critical in designing questionnaires that were distributed to M-Pesa dealers in this changing world where cyberspace threats have been used to extend anarchy online. Thus, the sliding scale was used to get the quantitative aspects of research, while the 'yes/no' questions gave the descriptive dimensions of the research. This, therefore, involved the use of random sampling in the identification of various dealers of M-Pesa who have different levels of access and who have worked at least for one year.

3.3 Population Sampling

Population consists of all members that meet a set of specifications. When a small set is selected from population it is called a sample. Corinna (2014) defines a sample as a subgroup of the whole population that would provide data for the research. According to Singh and Masuku (2014) sampling can fall into the following categories: random, purposive, cluster, quota, spatial and independent sampling among others. This study used random sampling because each elementary unit in the population was given equal chance of being selected.

A questionnaire was administered to 50 dealers of M-Pesa transfer service, who have diverse levels of access to M-Pesa platform infrastructure, because this gives insights into challenges that dealers experience in day to day work, thus, guaranteed correctness of the findings since they have different experiences over time. Level of access is where Safaricom gives some of its dealers authority to access M-Pesa platform infrastructure in order to address daily challenges experienced by users either from cyber threats or otherwise, without company involvement. In addition to random sampling, stratified sampling also guided in identifying of the respondents. From the above view, the sample was seen to be adequate for inference purpose, in addition it guided in attaining precision in research among other considerations.

3.4 Data collection methods

The researcher got the main parameters of the study through random and stratified sampling units which consist of dealers with diverse levels of access to M-Pesa that are conversant with use of cyberspace threats to perpetuate anarchic conditions, especially how its applications is used in cyberspace exhortation or fraud within Mobile money service by criminals. The questionnaire (See Appendix A) was the key technique of data collection. A sample of various dealers of Mobile money service transfer services were provided with questionnaires on the various cyberspace threats especially use of anarchy by states or non-state actors within the international system to achieve their objectives. The questionnaire was designed using Google forms and forwarded through e-mails and in some instances given physically to the M-Pesa dealers. The collected data assisted in identifying kinds of cyberspace threats that have been used to perpetuate anarchy within the international system that has slowly crypt into Mobile money service transfer services through the internet. The questionnaires were collected after an agreed time with each dealer and its data was interpreted through frequency tables, percentages and graphs using Google forms.

3.5 Data analysis and Validity

UNICEF (2014) observed that data analysis techniques should be chosen to match the particular evaluation in terms of its main evaluation questions and the resources available. It goes further to state that the methods should be able to complement each other's strength and weaknesses, in order to fill the existing gaps with the existing data. Therefore, since resources and other factors influence the choice of methods to analyze data, the study concentrated on utilizing less resources as well as meeting the intended objectives of the research. Data was analyzed after the all the questionnaires were received from the various dealers of Mobile money service. The choice of dealers with diverse levels of access to M-Pesa was in order to guarantee that the data collected was reliable, the use of a phone call was also considered in order to urge respondents to give their honest input to assure precision of the study. In addition, they were not required to put their names to ensure they gave right information without fear.

Francis Galton and Karl Pearson multiple linear regression (Stanton, 2001) formula was used:

$$\mathbf{Y = A_{0} + A_{1}X_{1} + A_{2}X_{2} + \ldots + A_{n}X_{n} + \varepsilon}$$

Where:

A_0 = constant (y-intercept in a graph)

A_1 to A_n = Coefficients relating to cyberspace threats

X_1 to X_n = Cyberspace threats

Y = Security of the Mobile money services.

ε – Residual of dealers' responses

The choice of multiple linear regressions was because the security of M-Pesa was directly related to a set of explanatory threat variables within cyberspace domain that is security of the Mobile money service is a function of various cyberspace threats. The study analyzed data using frequency tables, means, standard deviations and percentages which were obtained by the use of Microsoft excel, Google forms and IBM SPSS software platform.

3.6 Summary

In summary, the study designs and methods highlighted in this section guided how the study was conducted since one complement the other, in answering the research objectives, especially the use of cyber threats as form of creating cyberspace anarchy and its relationship to power polarity within the international system. This was because the riddle of insecurity within the international system has slowly crypt into the Mobile money services through cyberspace anarchy. Therefore, descriptive and explanatory as well as qualitative and the quantitative aspects are different dimensions of the same coin, hence, enables the research to unravel this riddle, thus, limiting its impact.

CHAPTER FOUR

RESEARCH ANALYSIS, FINDINGS AND DISCUSSION

4.1 Introduction

This chapter focused on presentation of data analysis and interpretation of results in accordance to the objectives of this study. The general objective of the study was to determine whether the number of cyber-attacks directed at Mobile money services increase with increase in the number of Mobile money service users. The specific objectives were to: establish what form of threats are used to perpetuate cyberspace anarchy within Mobile money services, analyse the impact of fraud on Mobile money service transactions among users and to establish whether cyber-attacks directed at Mobile money services increase with the increase of Mobile money service users.

This section was divided into eight parts: response rate, demographic information, forms of threats used to perpetuate cyberspace anarchy, factors influencing Mobile money service security, impact of fraud on Mobile money service transactions, cyber-attacks directed at Mobile money service, discussion of the findings and the summary of the chapter. The results were presented in tables and figures especially bar graphs.

4.2 Response Rate

The sample size of the study comprised of 50 dealers of M-Pesa transfer service platform with different levels of access to M-Pesa infrastructure. Fifty questionnaires were distributed among the participants. Out of the total, 32 respondents filled their questionnaires and returned them to the researcher on time. The response rate of the study was 64%. According to Kothari (2012), a response rate above 50% is appropriate for inference making. Therefore, the response rate of the study was within acceptable limit.

4.3 Demographic Information

Demographic information of the participants focused on duration of provision of Mobile money services, the type of Mobile money services offered by the dealership and how they learned about the Mobile money service security. The results were presented in figures (bar graphs) and tables.

4.3.1. Duration of Provision of Mobile money Services

The dealers of M-Pesa transfer service were requested to indicate for how long they have been offering Mobile money services. The results were as shown in figure 4.1.

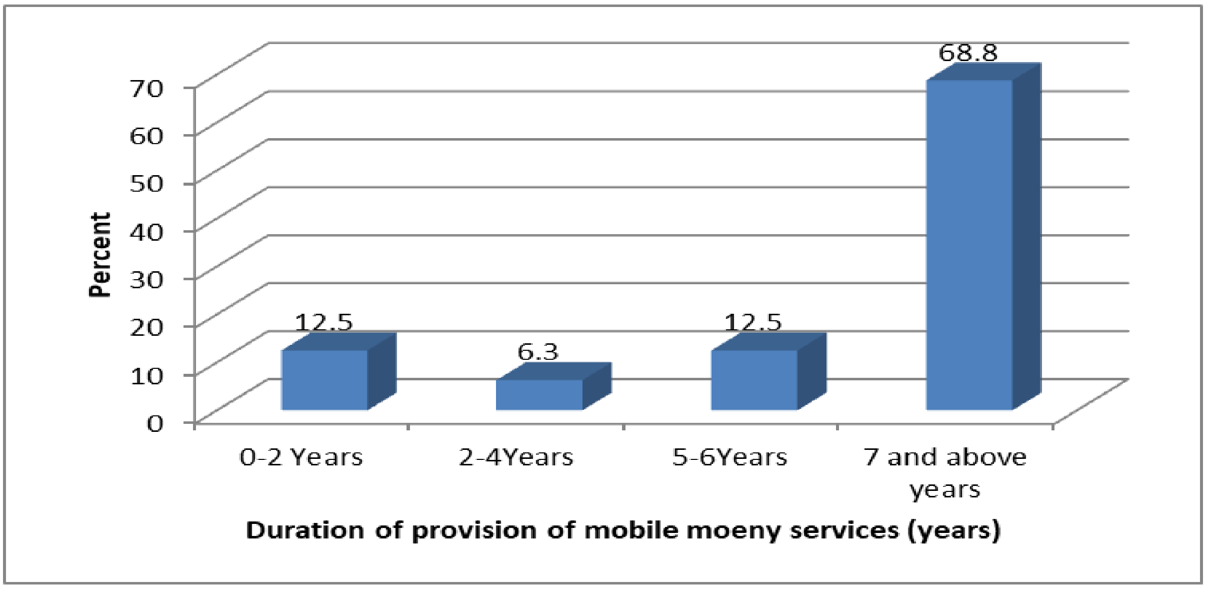

Figure 4-1: Duration of Provision of Mobile money Services

According to the results, 68.8% of the dealers of M-Pesa transfer service indicated that they have been offering Mobile money services for more than 7 years. Similarly, 12.5% of the dealers specified between 5 and 6 years, the same percentage indicated not more than 2 years, while 6.3% pointed out that they have been offering Mobile money services between 2 and 4 years. Thus, this implied that most of the dealers have been providing Mobile money service services for more than 7 years.

4.3.2 Type of Mobile money Services Offered by the Dealership

The dealers of M-Pesa transfer service were asked to indicate what kind of Mobile money services were offered by the dealership. The results were as shown in table 4.1.

Table 4-1: Type of Mobile money Services Offered by the Dealership

	Frequency		**Percent**	
	Yes	**No**	**Yes**	**No**
Deposit	32	0.0	100	0.0
Withdrawal	32	0.0	100	0.0
Transfer	32	0.0	100	0.0
Bill payment	6	26	18.8	81.3

From the above results, 100% of the dealers of M-Pesa transfer service specified that they offered: depositing, withdrawal and money transfer services. Similarly, 18.8% of the dealers specified that they offered bill payment services. Therefore, this implied that most of the dealers of M-Pesa transfer services offered depositing, withdrawal and transfers services to the customers.

4.3.3 Training on Mobile money Security

The dealers of M-Pesa transfer service were requested to specify how they learnt about the Mobile money service security. The results were as shown in table 4.2.

Table 4-2: Training on Mobile money Security

	Frequency		**Percent**	
	Yes	**No**	**Yes**	**No**
Workplace training	24	8	75.0	25.0
Mobile phone company training	10	22	31.3	68.8
Personal initiative	8	24	25	75

According to the results, 75.0% of the dealers of M-Pesa transfer service pointed out that they learnt about Mobile money service security through workplace training, another 31.4% specified through mobile phone company training, while 25% indicated personal initiatives. This implied that most of the dealers of M-Pesa transfer service learnt about Mobile money service security through workplace training.

4.4 Forms of Threats Used to Perpetuate Cyberspace Anarchy

The first objective of this study was to establish the forms of threats used to perpetuate cyberspace anarchy within Mobile money service. Therefore, in this section the researcher wants to find out dealers attitude towards Mobile money service security, disruption of Mobile money service services and what services were disrupted by what forms of cyberspace threats.

4.4.1 Attitude towards Mobile money service Security

The dealers of M-Pesa transfer service were asked to indicate their attitude towards Mobile money service security. The results were as shown in table 4.3.

Table 4-3: Attitude towards Mobile money Security

	1	**2**	**3**	**4**	**5**	**Mean**	**Std. Deviation**

Clients to receive education on Mobile money service security	0.0	0.0	0.0	37.5	62.5	4.625	0.491
Dealers to be taught about Mobile money service security	0.0	0.0	6.3	37.5	56.3	4.500	0.622
Mobile money service security be taught in schools	6.3	18.8	31.3	31.3	12.5	3.250	1.107
companies to offer opportunities for Mobile money service training	0.0	6.3	6.3	25.0	62.5	4.437	0.877
Individuals to teach themselves about Mobile money service security	25.0	12.5	18.8	25.0	18.8	3.000	1.481
Mobile money service security is unnecessary if security software is used	31.3	43.8	6.3	6.3	12.5	2.250	1.319

From the above observations, with a mean of 4.625 (Std. dv = 0.491) and a mean of 4.500 (Std. dv = 0.622) the dealers of M-Pesa Mobile money service strongly agreed that: clients ought to receive education on Mobile money service security and they ought to be taught about Mobile money service security respectively. Similarly, they agreed that Mobile money service providers ought to offer opportunities for Mobile money service training as shown by a mean of 4.437 (Std. dv = 0.877). In addition, they moderately agreed that: Mobile money service security ought to be taught in schools as shown by a mean of 3.250 (Std. dv = 1.107) and individuals to teach themselves about Mobile money service security as shown by a mean of 3.000 (Std. dv = 1.481). Furthermore, they disagreed that Mobile money service security was unnecessary if security software was used as shown by a mean of 2.250 (Std. dv = 1.319).

4.4.2 Disruption of Mobile money Services by Cyberspace Threats

The respondents were requested to indicate the extent to which M-Pesa services have been disrupted by cyberspace threats in any form on their dealership. The choices given were 1=Very frequent, 2= Frequent, 3== Moderately Frequent, 4=Less Frequent and 5=Not at all. The results were as shown in table 4.4.

Table 4-4: Disruption of Mobile money Services by Cyberspace Threats

	1	2	3	4	5	Mean	Std. Deviation
Power outage on server	12.5	43.8	6.3	18.8	18.8	2.875	1.385

Software malfunction(dedicated denial of service attacks)	18.8	50.0	6.3	12.5	12.5	2.500	1.295
Staff collusion with fraudsters (insider breaches)	56.3	18.8	6.3	6.3	12.5	2.000	1.436
Hacking(brute force attacks)	56.3	12.5	0.0	6.3	25.0	2.312	1.749
Spams (Malicious code injections)	68.8	0.0	6.3	6.3	18.8	2.062	1.664
Virus attacks	62.5	12.5	0.0	0.0	25.0	2.125	1.718
Sim swaps and pin change (account and service traffic hijacking)	62.5	12.5	6.3	12.5	6.3	1.875	1.338
Inter-operability (shared technology vulnerabilities)	50.0	6.3	0.0	12.5	31.3	2.750	1.849
Legal and regulatory gaps	56.3	6.3	0.0	12.5	25.0	2.500	1.796

Looking at the above data, with a mean of 2.875 (Std. dv = 1.385), 2.750 (Std. dv = 1.849), 2.500 (Std. dv = 1.295) and 2.500 (Std. dv = 1.796) the dealers of M-Pesa Mobile money service moderately agreed that: power outage on server, interoperability (shared technology vulnerabilities), software malfunction (dedicated denial of service attacks) and legal and regulatory gaps were forms of cyberspace threats used to disrupt Mobile money services. Similarly, they specified that: hacking (brute force attacks), virus attacks, staff collusion with fraudsters (insider breaches), spams (Malicious code injections), and Sim swaps and Pin change (account and service traffic hijacking) frequently disrupted Mobile money services as shown by a mean of 2.312 (Std. dv = 1.749), 2.125 (Std. dv = 1.718), 2.000 (Std. dv = 1.436), 2.062 (Std. dv = 1.664) and 1.875 (Std. dv = 1.338) respectively.

4.4.3 Mobile money service Disrupted at the Dealership

The dealers of M-Pesa transfer service were asked to point out which of the Mobile money services were disrupted by cyber threats. The results were as shown in table 4.5.

Table 4-5: Mobile money service Disrupted at the Dealership

	Frequency		Percent	
	Yes	**No**	**Yes**	**No**
Deposit	22	10	68.8	31.3
Withdrawal	20	12	62.5	37.5
Transfers	10	22	31.3	68.8

Bill payment	8	24	25.0	75.0

According to the results, 68.8% of the dealers of M-Pesa transfer service indicated that depositing services were disrupted by cyberspace threats. Similarly, 62.5% specified that withdrawal were disrupted by cyberspace threats, while 25.0% indicated that bill payment were disrupted by these threats and another 22% pointed out that transfer services were disrupted by cyberspace threats. Therefore, this implied that depositing services were adversely affected by cyberspace threats.

4.4. Factors Influencing Mobile money Security

The dealers of M-Pesa transfer service were also requested to indicate the agreement level on various factors influencing Mobile money service security services in their dealership. The results were as shown in table 4.6.

Table 4-6: Factors Influencing Mobile money Security

	1	**2**	**3**	**4**	**5**	**Mean**	**Std. Deviation**
Cost	18.8	6.3	6.3	56.3	18.8	3.562	1.342
Scalability	6.3	12.5	18.8	62.5	0.0	3.375	0.941
Availability	0.0	0.0	6.3	68.8	25.0	4.187	0.535
enabling environment	6.3	6.3	6.3	62.5	18.8	3.812	1.029
Digital registration of subscribers	6.3	18.8	31.3	43.8	0.0	3.875	1.338
Legal and regulatory gaps	6.3	12.5	12.5	37.5	31.3	3.750	1.218
Customer awareness	0.0	12.5	6.3	37.5	43.8	4.125	1.008

From the above data, with a mean of 4.187 (Std. dv = 0.535), 4.125 (Std. dv = 1.008), 3.875 (Std. dv = 1.338), 3.812 (Std. dv = 1.029), 3.750 (Std. dv = 1.218) and 3.562 (Std. dv = 1.342) the dealers of M-Pesa Mobile money services agreed that availability, customer awareness, digital registration of subscribers, enabling environment, legal and regulatory gaps and cost respectively influence Mobile money service security. Similarly, they were undecided on whether scalability influenced Mobile money service security as shown by a mean of 3.375 (Std. dv = 0.941).

4.5 Impact of Fraud on Mobile money services

The second objective of this study was to analyze the impact of fraud on Mobile money services among users.

4.5.1 Impacts of Mobile money Security on Dealership

The respondents were asked to indicate the impacts of Mobile money service security on their dealership. The results were as shown in table 4.7.

Table 4-7: Impacts of Mobile money Security on Dealership

	1	2	3	4	5	Mean	Std. Deviation
Offer more services to the business	0.0	12.5	0.0	81.3	6.3	3.812	0.737
Reduced cost on security training	6.3	18.8	6.3	62.5	6.3	3.437	1.075
Mobile money service becoming more strategic	12.5	12.5	12.5	56.3	6.3	3.312	1.176
Reduced outsourcing of Mobile money service security	12.5	12.5	0.0	68.8	6.3	3.437	1.189
Less time in updating Mobile money service infrastructure	6.3	6.3	6.3	68.8	12.5	3.750	0.983
Reduced staff	12.5	31.3	6.3	43.8	6.3	3.000	1.244

Looking at above data, with a mean of 3.812 (Std. dv = 0.737) and 3.750 (Std. dv = 0.983), the dealers of M-Pesa Mobile money service agreed that Mobile money service security enabled them to: offer more services on their businesses and spent less time updating Mobile money service infrastructure respectively. In addition, they moderately agreed that Mobile money service security: reduced outsourcing of Mobile money service security, reduced cost on security training, Mobile money service to become more strategic and reduced staffing as shown by a mean of 3.437 (Std. dv = 1.189), 3.437 (Std. dv = 1.075), 3.312 (Std. dv = 1.176) and 3.000 (Std. dv = 1.244) respectively.

4.5.2 Trust in Data Security Offered by Mobile money service Provider

The dealers of M-Pesa transfer service were requested to indicate their level of trust in data security offered by Mobile money service providers. The results were as shown in figure 4.2.

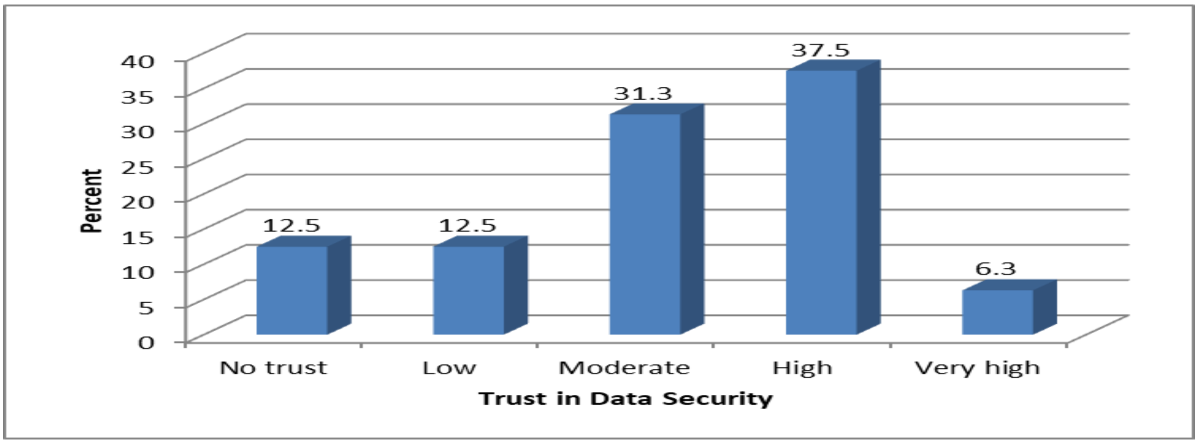

Figure 4-2: Trust in Data Security Offered by Mobile money service Provider:

According to the results, 37.5% of the dealers of M-Pesa transfer service specified that they have high trust in data security offered by Mobile money service provider, with 31.3% pointing out that they have moderate trust of the same. Similarly, 12.5% indicated that they have no trust of data security offered; the same percentage also specified to have low trust. In addition, 6.3% specified very high trust on data security provided by Mobile money service Provider. Therefore, this implied that most of the dealers of M-Pesa services had trust in the data security services offered by the mobile service provider.

4.5.3 Losses Incurred due to Problems with Mobile money Security

The respondents were asked to specify if they have ever incurred losses attributed to problems in Mobile money service security. The results were as shown in table 4-8.

Table 4-8: Losses Incurred due to Problems with Mobile money Security

	Frequency		**Percent**	
	Yes	**No**	**Yes**	**No**
Accidental leakage of Mobile money service number	2	30	6.3	93.8
Leakage of your own personal information	4	28	12.5	87.5
Unauthorized access	2	30	6.3	93.8
Phishing	3	29	9.4	90.6
Password sniffing	2	30	6.3	93.8
Theft of data or information on Mobile money service	4	28	12.5	87.5

From the above observations, 12.5% of the dealers of M-Pesa transfer service specified that theft of data or information on Mobile money service had made them to incur losses; also the same percentage indicated that leakage of their own personal information led to losses.

Similarly, 9.4% specified phishing, with 6.3% pointing at unauthorized access which led them to incur losses. In addition, another 6.3% specified password sniffing. Looking at data above, theft of data or information on Mobile money service and leakage of personal information were the leading sources of incurring losses according the dealers as far as Mobile money service security is concerned.

4.6 Cyber-attack Directed at Mobile money Services

The third objective of this study was to establish whether cyber-attacks directed at Mobile money services increase with the increase of Mobile money service users.

4.6.1 Greatest Barriers to adoption of Mobile money Services

The respondents were asked to indicate the greatest barriers to adoption of Mobile money services in their dealership. The results were as shown in table 4.9.

Table 4-9: Barriers to adoption of Mobile money Services

	Frequency		**Percent**	
	Yes	**No**	**Yes**	**No**
Legal and regulatory gaps	16	16	50.0	50.0
Data security and privacy	18	14	56.3	43.8
Cyber extortionist	16	16	50.0	50.0
Staff collusion with fraudsters	18	14	56.3	43.8
Sim swaps and Pin change	18	14	56.3	43.8
Virus attacks	6	26	18.8	81.3
Vendor lock in	6	26	18.8	81.3
Spams(malicious code injections)	10	22	31.3	68.8
Customer awareness	24	8	75.0	25.0
Digital registration of customers	20	12	62.5	37.5

According to the results, 75.0% of the dealers of M-Pesa transfer service specified that the greatest barriers to adoption of Mobile money service was lack of customer awareness, with 62.5% citing lack of digital registration of customers. Similarly, 56.3% of the dealers specified staff collusion with fraudsters was the greatest barrier to the adoption of Mobile money services, with also the same percentage indicating that Sim swaps and Pin change being the greatest barriers. In addition, another 56.3% indicated data security and privacy being the greatest barriers, with 50% indicated legal and regulatory gaps contributing to the same. In the meantime, 50% specified cyber extortionist being the greatest barriers, with 31.3% pointing at malicious code injection and another 18% indicated Virus attacks and the same percentage blaming vendor lock was the greatest barriers to the adoption of Mobile money services. Therefore, this implied that lack of customer awareness was the greatest barrier to adoption of Mobile money services.

4.6.2 Inferential Statistics

In the research, inferential statistics focused on multivariate regression analysis. Regression analysis was used to determine whether cyberspace threats (power outage on server, software malfunction, staff collusion with fraudsters, hacking, malicious code injections, Sim swaps and Pin change, interoperability, legal and regulatory gaps) increases with increase in the number of Mobile money users, thus, affecting the security of the Mobile money service transfer transactions.

4.6.2.1 Regression Analysis

The study used multivariate regression analysis to determine the relationship between cyberspace threats and security of the Mobile money service transfer transactions especially its link with the increase of users within Mobile money payment system.

Table 4-10: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.961	0.923	0.901	0.10217

From the above data, the R squared was used to determine the variation in the dependent variable (security of the increased users of Mobile money service transfer transactions) that could be explained by independent variables (cyberspace threats). The R squared was 0.923. Therefore, this implied that 92.3% of the variation in the dependent variable (security of the increased users of Mobile money service transfer transactions) could be explained by independent variables (cyberspace threats). In other words, the larger the R^2, the better the regression model fits dealers' response returns.

Table 4-11: Analysis of Variance

	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	314.213	8	39.276	2618.400	.000[b]

Residual	3.581	23	.015
Total	317.794	31	

Looking at data above, the ANOVA was used to determine whether the model was a good fit for the data. The F – calculated was 2618.400. The F critical was 2.1802. Since the F calculated was greater than the F critical and the p value 0.000 was less than the significant level, the model was considered a good fit for the data. Henceforth, the model was used to predict the effect of cyberspace threats on security of the Mobile money service transfer transactions when users increase.

Table 4-12: Regression Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.217	0.075		2.899	0.004
	Power outage on server	0.135	0.05	0.184	2.732	0.028
	Software malfunction	0.172	0.073	0.139	2.353	0.019
	Staff collusion with fraudsters	0.188	0.061	0.187	3.086	0.013
	Hacking	0.241	0.057	0.299	4.217	0.010
	Spams (Malicious code injections)	0.335	0.047	0.403	7.141	0.009
	Sim swaps and Pin change (Account and service traffic hijacking)	0.356	0.056	0.296	6.333	0.008
	Interoperability (Shared technology vulnerabilities)	0.385	0.063	0.32	6.095	0.001
	Legal & regulatory gaps	0.906	0.068	0.879	13.316	0.000

The regression equation was follows:

$$Y = -0.217+ 0. 135 X_1 + 0. 172 X_2 + 0. 188 X_3 + 0. 241X_4 + 0. 335X_5+ 0. 356X_6+ 0. 385X_7+ 0. 906X_8+ \varepsilon$$

From the results, it revealed that power outage on server has significant effect on security of the Mobile money service transfer transactions when users increase (β_1=0.135, p value= 0.028). Similarly, the relationship was considered significant since the p value 0.028 was less than the significant level (0.05). In addition, the results also revealed that software malfunction has significant effect on security of the Mobile money service transfer transactions when users increase (β_2=0.172, p value= 0.019). In the meantime, the relationship was considered significant since the p value 0.019 was less than the significant level (0.05). In addition, the results showed staff collusion with fraudsters has significant effect on security of the Mobile money service transfer transactions when users increase (β_3= 0.188, p value= 0.013). The relationship was considered significant since the p value 0.013 was less than the significant level (0.05). Moreover, the results revealed that hacking has significant effect on security of the Mobile money service transfer transactions when users increase (β_4= 0.241, p value= 0.010). Therefore, the relationship was considered significant since the p value 0.010 was less than the significant level (0.05).

Besides that, the results revealed that spams (Malicious code injections) has significant effect on security of the Mobile money service transfer transactions when users increase (β_5= 0.335, p value= 0.009). The relationship was considered significant since the p value 0.009 was less than the significant level (0.05). The results also revealed that Sim swaps and Pin change has significant effect on security of the Mobile money service transfer transactions when users increase (β_6= 0.356, p value= 0.008). The relationship was considered significant since the p value 0.0008 was less than the significant level (0.05). Further, the results showed that interoperability has significant effect on security of the Mobile money service transfer transactions when users increase (β_7= 0.385, p value= 0.001). The relationship was considered significant since the p value 0.001 was less than the significant level (0.05). Furthermore, the results revealed that legal and regulatory gaps have significant effect on security of the Mobile money service transfer transactions when users increase (β_8= 0.906, p value= 0.000). Thus, the relationship was considered significant since the p value 0.000 was less than the significant level (0.05).

In summary, therefore, with the above data it can be inferred that cyber-attacks directed at Mobile money services increased with the increase of Mobile money service users, thus, validating the research hypothesis.

4.7 Discussion of the Findings

4.7.1 Forms of Threats Used to Perpetuate Cyberspace Anarchy

The study found that dealers of M-Pesa transfer services ought to: receive education on Mobile money service security, be educated on Mobile money service security, offer opportunities for Mobile money service training, be taught in schools and use security software in improving security of Mobile money services. Therefore, the findings are line with the findings of Feizollah, et al. (2015) that training and education on cyberspace security improve Mobile money service security.

In addition, the study found that: power outage on server, software malfunction (dedicated denial of service attacks), staff collusion with fraudsters (insider breaches), spams (malicious code injections), virus attacks, Sim swaps and Pin change (account and service traffic hijacking), inter-operability (shared technology vulnerabilities) and legal and regulatory gaps are forms of threats used to perpetuate cyberspace anarchy among the Mobile money service providers. Thus, the findings concur with the findings of Geva, et al. (2014) that the main threats to cyberspace security include: virus attack, power outage on server, software malfunction and staff collusion with fraudsters. Similarly, the findings were in line with the findings of Kaspersky (2016) that sharing technological vulnerabilities perpetuate cyberspace anarchy.

The study found that cyber threats disrupted: depositing, withdrawal and transfer of cash of cash among the dealers of M-Pesa transfer service. Similarly, the study also established that cyber threats also disrupted bill payment among the dealers of M-Pesa transfer service. Thus, the findings conform with the findings of Feizollah, et al. (2015) that fraudulent activities tend to disrupt withdrawal, transfer, bill payment and depositing of cash among dealer of Mobile money service providers.

4.7.2 Impact of Fraud on Mobile money service Transactions

The Study found that Mobile money service security enabled them to: offer more services to the business, reduced the time spent in updating Mobile money service infrastructure, reduced outsourcing of Mobile money service security, reduced cost on security training, made Mobile money service to become more strategic and reduced staffing. Therefore, the findings are in agreement with the findings of Arunesh, et al. (2015) that improving on Mobile money service security reduced cost and time spent in updating Mobile money service infrastructure, outsourcing of Mobile money service security experts and reduce staffing cost.

In addition, the study also established that cyber threats lead to: accidental leakage of Mobile money service number of clients, leakage of personal information, unauthorized access to information and theft of information on Mobile money service transactions. Thus, the findings conform with the findings of Reaves, et al. (2015) that fraud result to leakage of information to unauthorized persons and theft of information relating to financial transactions consequently affecting performance of Mobile money service providers.

4.7.3 Cyber-attack Directed at Mobile money Services

The study found that: data security and privacy, cyber extortion, Sim swaps and Pin change increased with increase of Mobile money service users. Therefore, the findings are in line with the findings of Castle, et al. (2016) that the cyber extortion and virus attack are the main forms of cyber-attack directed at Mobile money service services. Similarly, the study found that virus attacks, vendor lock in, spams (malicious code injections) and digital registration of customers increased with the increase of Mobile money service users. Therefore, the finding is in line with the finding of Masamila (2014) that cyber-attack through vendor lock in and malicious code injections have negative influence on delivery of services among the Mobile money service providers.

4.8 Summary

This chapter has analyzed the questionnaires which were returned and found that cyberspace anarchy was ripe within this domain and would continue to be utilized by states as well as non-state actors going forward. The fraud perpetuated in this domain was more, despite two dealers stating to have incurred losses amounting to Kshs. 176,000 upon encountering accidental leakage of mobile phone number in 2013, some agree that they have incurred losses despite their failure to mention the amount involved. Similarly, various Mobile money services have been disrupted by cyberspace threats to various degrees as shown from the analysis with deposits, withdrawals, transfers, Sim swap, bill payment, buying goods and services in that order of importance being disrupted. In addition, dealers agreed on various factors influencing the provision of security within Mobile money services, these factors on the other hand fueled cyberspace anarchy, since provision of adequate security within this domain was a big challenge not only to states but also non-state actors. This was because enforcement of order within this realm is a great challenge due to its borderless nature as well as the dominance of non-state actors in this domain.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter entailed presentation of: summary of the study’s findings, conclusions that were drawn, recommendation that were made and suggestion for further research. The key objective of the study was to determine whether the number of cyber-attacks directed at Mobile money services increase with increase in the number of Mobile money service users. The specific objectives were to: establish the forms of threats, impact of fraud and why cyber-attacks directed at Mobile money services increase with the increase of Mobile money service users.

5.2 Summary

The cyberspace has been interwoven into the operations of: financial system especially Mobile money service as well as Mobile banking among others, intelligence/military logistics system and aspects of every day communication. Therefore, this critical role is increasingly be threatened not only by states but also non-state actors, who despite being a great source of innovations are also a source of tools for developing both the offensive and defensive capabilities within this domain. As this research have shown, cyberspace threats directed at Mobile money services increase with the increase of users, in addition, cyberspace extortion increase with increase of Mobile money service users. This research was centered on two arguments: Mobile money service security within cyberspace is a function of its insecurity or in essence cyberspace threats directed to Mobile money service is the basis of its security and the cyberspace geometry keeps changing with each new security solution, hence, need for a contain anarchy within it.

Cyberspace anarchy is evolving with constant evolution of the internet in its various forms, for instance, Mobile money service, Internet of Things (IoT) to them but a few. Thus, this evolution carries with it threats which in one way or another threaten Mobile money service systems. These threats requires collaborations from state and non-state actors, this is because these threats sometimes are borderless in nature due to cyberspace disregard of territoriality. In addition, the difficulty of addressing cyberspace threats is because there are no clearly spelt out objectives to be attained while tackling these challenges as well as lack of specific targets to be taken.

Similarly, the power polarities within the international system is or may be of no significance because cyberspace domain requires less resources for one to master it, hence, even countries with less resources can be high in terms of power polarity in cyberspace as a domain of warfare or even non-state actors with less resources can threaten states which have far more resources and military power in traditional sense of power polarity within the international system. Therefore, humanity needs to understand that there is more to gain in cyberspace through collaboration than the continued application of anarchy since the Westphalia model of state rules to this domain is obsolete.

5.3 Conclusions

The study concludes that: training on Mobile money service security, power outage on server, software malfunction (dedicated denial of service attacks), staff collusion with fraudsters (insider breaches), spams (malicious code injections), Sim swaps and Pin change and shared technology vulnerabilities were forms used to perpetuate cyberspace anarchy among the Mobile money service providers.

Moreover, the study concluded that Mobile money service security: reduced the time spent in updating Mobile money service infrastructure, cost incurred in outsourcing services and training. The study also concluded that fraud disrupted depositing, withdrawal, transfer and bill payment among the dealers of M-Pesa transfer service. Besides that the study established that fraud lead to: accidental leakage of Mobile money service number of clients, leakage of personal information, unauthorized access to information and theft of information on Mobile money service transactions.

Further, the study concluded that: data security and privacy, cyber extortion, Sim swaps and Pin change, spams (malicious code injections), vendor lock in and virus attacks are the greatest barriers to the adoption of Mobile money services by users.

In a nutshell, perceiving the anarchic conditions within the cyberspace in the outlook of the game theory as shown by the research that virus attacks directed at Mobile money service increase with the increase of users, the evolution of anarchy should be looked at not as something to be completely wiped but as a necessary incentive encouraging innovation of solutions to address the cyberspace threats going forward, and as such parts of the mutually coexistence of threats and solutions.

5.4 Recommendations

The study found that power outage on server as a form of threat was used to perpetuate cyberspace anarchy among the Mobile money service providers. Therefore, the study recommends that the dealers of M-Pesa transfer services should install standby generators, install fire walls and encrypt data so as to prevent threats due to cyberspace anarchy.

The study also established that fraud lead to unauthorized access to information. Therefore, the study recommends that the dealers of M-Pesa transfer services should enhance identification and verification using biometric methods like fingerprint, facial among others in addition to password/pin to protect files, bugler proof computer rooms and utilize IP Whitelisting to prevent unauthorized access to information by fraudsters.

Further, the study established that virus attacks increase with increase of Mobile money service users which were carried using these forms of cyberspace threats: software malfunction, spams (malicious code injections) and shared technology vulnerabilities. Therefore, the study recommends that the dealers of M-Pesa transfer services should install advanced and quality antivirus, perform daily scans and isolate affected drives so as prevent virus attacks. Similarly, security should be incorporated during the design and development of the Mobile money service applications since most flaws are attributed to failure to incorporate it from the beginning

Therefore, since these cyberspace threats cannot be adequately be addressed because they outgrow each solution deployed, hence, there is need for its management in order to enable utilization of the benefits which comes from this domain. Thus, contained anarchy within cyberspace domain is what this research recommends through: continued development of tools to contain threats within cyberspace and continued legislation that is threats driven to tackle cyberspace challenges as they emerge.

Therefore, despite anarchy creating a devolved rivalry among sovereign states as coined by Kenneth Waltz (Waltz, 1979), it is worsened by the involvement of non-state actors, making it difficult for any one or more tools/measures of national security to effectively contain cyberspace threats, since, threats and solutions evolve infinitely, thus, need for a multilateral as well as multi-agency approach in order to tackle it through creation of a regime among states.

5.5 Suggestion for further research

The key objective of the study was to determine why the number of cyber-attacks directed at Mobile money services increase with increase in the number of Mobile money service users in Kenya. Therefore, the study recommends that further studies should be conducted in other countries to determine why the number of cyber-attacks directed at Mobile money services increase with increase in the number of Mobile money service users. The study also established that 92.3% of the variation in security of the Mobile money services could be explained by cyberspace threats. Hence, the study recommends that further studies should be conducted to determine other factors affecting security of the Mobile money services outside anarchy within cyberspace.

Reference

Akomea, F. I., Andoh, C., Frimpong, A. A. & Dwomoh, O. Y. (2019). Control of Fraud on

Mobile Money Services in Ghana: an Exploratory Study. Journal of Money Laundering Control May 2019. DOI: 10.1108/JMLC-03-2018-0023 https://www.researchgate.net/publication/323907528 [Accessed on: 13.08.2019].

Alliance for Financial Inclusion (2016). Policy Frameworks to Support Women's Financial Inclusion. https://www.afi-global.org/sites/default/files/publications/2016-08/2016-02-womenfi.1_0.pdf [Accessed on: 07.07.2018].

Australian Computer Society (ACS). (2016). Cybersecurity: Threats, Challenges and Opportunities. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf [Accessed on: 13.07.2019].

Alessandro, G. (2017). Imposing and Evading Cyber Borders: The Dilemma of Sovereignty. 2017 Pirate Security Conference, Munich 16/2/2017.

Alexander, M., Seychelle, C. & Alan, W. D. (2015). Cybersecurity Challenges for Canada and United States. Fraser Institute. https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf [Accessed on: 8.2.2018].

Alexandra, P. (2017). A Problem Without a Passport: Overcoming Jurisdictional Challenges for Transnational Cyber Aggressions.

Arunesh, S., Thanh, H. N., Debarun, K., Mathew, B., Milind, T. & Albert, X. J. (2015). From Physical Security to Cybersecurity. Journal of Cybersecurity. Doi: 10.1093/cybsec/tyv007.

Banzi, A. (2017, February 10th). Fraud Hits Tanzania's Mobile Money Transfer. The EastAfrican Digital. https://www.theeastafrican.co.ke/business/Fraud-hits-Tanzania-mobile-money-transfer-/2560-3807992-jihx3c/index.html [Accessed on: 13.08.2019].

Booth, K. (2007). Theory of World Security. Cambridge University Press. https://pdfs.semanticscholar.org/aefa/2613b3277b1f6f5c973cc46111fc42a1ad4d.pdf [Accessed on: 21.09.2019].

Bossi, M. (2014). State of Mobile Banking in Tanzania and Security Issues. *International Journal of Network Security & Its Application (IJNSA), Vol.6, No. 4, July, 2014*.

Buku, M. W. & Mazer, R. (2017). Fraud in Mobile Financial Services: Protecting Consumers, Providers and the System. https://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf [Accessed on: 13.08.2019].

BullGuard (2018). A definition of malware. https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/m alware-definition,-history-and-classification.aspx [Accessed on: 25.01.2018].

Butler, K. (2017). Security and Privacy Challenges for Mobile money service Applications. ITU Digital Financial Services Workshop. Port of Spain, Trinidad & Tobago, 28th April, 2017.

Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. *International Affairs (Royal Institute of International Affairs 1944-),* Vol. 67, No. 3 (July, 1991), pp. 431-451. http://home.sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/10/New%20Patterns%20of%20Global%20Security%20in%20the%20TwentyFirst%20Century_Buzan.pdf [Accessed on: 13.08.2019].

Byrone, R. (2019, August 11th). Sh 230,000 Stolen as Fraudsters Clean Kisumu Man's Bank Savings. Standard Newspaper Digital. https://www.standardmedia.co.ke/article/2001337714/kisumu-man-loses-sh230-000-in-m-pesa-withdrawal-fraud [Access on: 11.08.2019].

Castle, S., Pervaiz, F., Weld, G., Roesner, F. & Anderson, R. (2016). Let's Talk Money: Evaluating the Security Challenges of Mobile money service in the DeveloPing World. 2016 ACM Symposium on Computing for Development.

Cert-UK (2015). Common Cyber Attacks: Reducing the Impact. CESG, the Information Security Arm of GCHQ. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf [Accessed on: 16.07.2019].

Communications Authority of Kenya (CA) (2018). First Quarter Sector Statistics Report for the Financial Year 2018/2019 (July/September, 2018). https://ca.go.ke/wp-content/uploads/2018/12/Sector-Statistics-Report-Q1-2018-2019.pdf [Accessed on: 12.08.2019].

Communications Authority of Kenya (2017). First Quarter Sector Statistics Report for the Financial Year 2016/2017 (July – September, 2017). http://www.ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%2 0Q1%20%202017-18.pdf [Accessed on: 12.2.2018].

Corinna, F. (2014). Sampling and its Relevance for Sound Data Collection. Data Network for Better European Organic Market Information. University of Kasel.

Cheng, Z. (2007). Mobile Malware: Threats and Prevention. McAfee Avert.

Claire, S., Arunjay, K., Jennifer, F., Alix, M. & Nika, N. (2014). 2014 State of the Industry: Mobile Financial Services for the Unbanked. https://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2015/03/SOTIR_2014.pdf [Accessed on: 08.08.2018].

Cyber Security and Protection Bill (2016). Kenya Gazette Supplement No.110, Senate Bills No. 12, 2016. Nairobi: The Government Printer.

Deibert, R. J. (2013). Black Code: Inside the Battle for Cyberspace, in International Journal of Communication 7, Book review 2730 – 2732 by Sarah Myers, University of Southern California. http://ijoc.org. [Accessed on: 2.2.2018].

Denis, B. (n.d.). Game Theory & Deterrence Theory. Ch. 9: What Causes War? International Interactions.

Dipak,V. B., Prajakta, K. M. & Yogesh, S. L. (2016). Cyber Security Using Game Theory. *International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue* 1, January 2016. http://www.ijiset.com.

Elizabeth, T. (2017). Taming the ‘Wild West’: The Role of International Norms in Cyberspace. http://www.e-ir.info/2017/11/13/taming-the-wild-west-the-role-of- international-norms-in-cyberspace/ [Accessed on 2.2.2018].

Eriksson, J. & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? International Political Science Review 2006, Vol. 27, No. 3, 221-244.

Feizollah, A., Anuar, N. B., Salleh, R. & Wahab, A. W. A. (2015). A Review on Feature Selection in Mobile Malware Detection.

Flint, J. (2017). What is Anarchy – Definition & Examples. Philosophers on Anarchy. http://study.com/academy/lesson/what-is-anarchy-definition-examples.html [Accessed on: 24.11.2017]

Frankline, S. (2019, June 28th). Airtel Money Loses Kshs. 670 Million to Staff Fraud. The Standard Digital. https://www.standardmedia.co.ke/business/article/2001331718/airtel-money-loses-sh670-million-to-staff-fraud [Accessed on: 20.07.2019].

Friedman, A. A., Austen, M. C. & Ross, A. H. (2013). Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences. *Center for Technology Innovation at Brookings.*

Geva, M., Herzberg, A. & Yehoshua, G. (2014). Bandwidth Distributed Denial of Service:

Attacks and Defenses. IEEE Security & Privacy, Volume 12, Issue 1, Jan – Feb. 2014. [Accessed on 28.06.2019].

Gueldry, M., Gokcek, G. & Hebron, L. (2019). Understanding new security threats. 1st ed. Abingdon: Routledge. https://www.amazon.com/Understanding-Security-Threats-Michel-Gueldry/dp/1138104728 [Accessed on: 21.09.2019].

GSMA (2019). State of the Industry Report on Mobile Money 2018 https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018-1.pdf [Accessed on: 12.08.2019].

GSMA (2016). State of the Industry Report on Mobile Money 2015 https://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2015.pdf [Accessed on: 12.08.2019].

Grieco, J. M. (1988). Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism. Published online by Cambridge University Press: 22 May 2009
DOI: https://doi.org/10.1017/S0020818300027715
https://www.cambridge.org/core/journals/international-organization/article/anarchy-and-the-limits-of-cooperation-a-realist-critique-of-the-newest-liberal-institutionalism/B15341ABF136D039DBC1D99A4179A64E [Accessed on: 11.08.2019].

Industrial Control Systems (2017). Cyber Threats Source Descriptions. United States, Department of Homeland Security: Industrial Control Systems Cyber Emergence

International Telecommunication Union (ITU) (2013). The Mobile Money Revolution. Part 2: Financial Inclusion Enabler. ITU-T Technology Watch Report, May, 2013. https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200002PDFE.pdf [Accessed on: 08.08.2018].

Janine, F. (2009). E-Money-Mobile money service-Mobile Banking-What’s the Difference. http://blogs.worldbank.org/psd/health/e-money-mobile-money-mobile-banking-what-s-the-difference [Accessed on 8.2.2018].

Joubert, V. (2010). Getting the Essence of Cyberspace; a Theoretical Framework to Face Cyber Issues. Conference on Cyber Conflict, Tallinn, Estonia.

Kandethody, R. & Zheni, S. (2016). Dynamic Game Theories in Cyber Security. Proceedings of Dynamic Systems and Applications (2016). Interdisciplinary Data Sciences Consortium (IDSC), University of Florida. Florida: Dynamic Publishers, Inc.

Karim, A., Shah, S. A. A., Salleh, R. B., Arif, M., Noor, R. M. D. & Shamshirband, S. (2015). Mobile Botnet Attacks, an Emerging Threat: Classification, Review and Open Issues. *KSII Transactions on Internet and Information Systems, Vol. 9, No.4, April, 2015.*

Kaspersky (2016). Kaspersky Security Bulletin 2016. https://media.kasperskycontenthub.com/wpcontent/uploads/sites/43/2018/03/07182317/ KASPERSKY_SECURITY_BULLETIN_2016.pdf [Accessed on: 08.07.2018].

Kearns, G. S. (2016). Countering Mobile Device Threats: A Mobile Device Security Model. In *Journal of Forensic & Investigative Accounting, Volume 8: Issue 1, January – June, 2016.*

Keohane, R. (1988). International Institutions: Two Approaches, *International Studies Quarterly*, Vol.32, No.4, 1988, pp.379-396.

Kothari, C. R. (2012). Research Methodology: Methods and Techniques. New Age International Pvt Ltd Publishers. New Delhi, India.

Kozuch, I. (2018). Financial Services Threat Landscape Report: The Dark Web Perspective. https://cdn2.hubspot.net/hubfs/3699194/Content/Research%20Reports/IntSights_ Financial_Services_Landscape-Final.pdf [Accessed on 20.08.2018].

Lippmann, W. (1943). U.S. Foreign Policy: Shield of the Republic in Bailey, Thomas, A. *Political Science Quarterly*, Vol. 58, No. 3 (September, 1943), pp. 429 – 431. The Academy of Political Science. DOI: 10.2307/2144495 https://www.jstor.org/stable/2144495 [Accessed on: 21.09.2019].

Mahlangu, T. (2018). MTN Warns of SIM Swap Fraud. https://rekordeast.co.za/170608/mtn- warns-of-sim-swap-fraud/ [Accessed on: 13.08.2019].

Masamila, B. (2014). State of Mobile Banking in Tanzania and Security Issues. International Journal of Network Security & Its Applications (IJNSA), Vol. 6, No. 4. Doi: 10.5121/ijnsa.2014.6405.

Marc, B. & Steffen, H. (2016). Interoperability of Mobile Money: International Experience and Recommendations for Mozambique. International Growth Centre. https://www.theigc.org/wp-content/uploads/2017/01/Hoernig-et-al-2016-Final-Report.pdf [Accessed on: 08.07.2018].

Meiser, J. W. (2017). Liberalism. In McGlinchey, S. , Walters, R. & Scheinpflus, C.

(Eds.), *International Relations Theory* (pp. 22 – 27). Bristol England: E-International Relations Publishing https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/ [Accessed on: 12.08.2019].

Mihai, M. (2016). Game Theory. MIT.

Milner, H. (1991). The Assumption of Anarchy in International Relations Theory: A Critique. *Review of International Studies, Vol. 17, Issue 1, Pg. 67-85.* http://toprovenothing.blogspot.co.ke/2008/09/milner-assumption-of-anarchy-in.html [Accessed on: 8.2.2018].

Morawczynski, O. (2015). Fraud in Uganda: How Millions Were Lost to Internal Collusion https://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion [Accessed on: 12.08.2019].

Morgenthau, H. J. (1985). Politics Among Nations: The Struggle for Power and Peace (7th Edition). New York: McGraw-Hill. http://saldanha.pbworks.com/f/Morgenthau.Politics+Among+Nations.pdf [Accessed on: 16.08.2019].

Myriam, D. C. (2008). Cyber-Terror: Looming Threat or Phantom Menace? The Framing of The US Cyber Threat Debate. *Journal of Information Technology and Politics* 4:1 (2008): Pg: 19-36.

National Cyber Security Centre (2015). National Cyber Security Strategy 2016 – 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf [Accessed on: 07.07.2018].

Neumann, J. V. (1928). Essay "The Mathematician" in *The Works of the Mind* Chicago 1947, pp. 180-196 in *The World of Mathematics* (J. R. Newman, ed.) New York, 1956, pp. 2053-2063. https://pdfs.semanticscholar.org/711b/7d142764484b29119f9b6c2222ea81756f4d.pdf [Accessed on: 8.2.2018].

Neumann, J. V. & Morgenstern, O. (1953). Theory of Games and Economic Behaviour. Princeton University Press, Princeton. https://pdfs.semanticscholar.org/0375/379194a6f34b818962ea947bff153adf621c.pdf [Accessed on: 28.08.2018].

Nielsen (2016). Mobile Money: From Shopping to Banking to Payments, How Mobile is Transforming Commerce Around the World, October, 2016. https://www.nielsen.com/wp-content/uploads/sites/3/2019/04/nielsen-global-mobile-money-report-oct-2016.pdf [Accessed on: 08.08.2018].

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, vol. 91, no. 1, pp. 111-130, 2015.

Nye, J. S., Jr. (2016). The Regime Complex for Managing Global Cyber Activities. In Laura, D. (Eds.), *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance.* Global Commission on Internet Governance, Research Volume Two.

Nye, Jr. J. S. (2011). Nuclear Lessons for Cyber Security*?* In *Strategic Studies Quarterly* 5 (4): 18 - 38. http://www.au.af.mil/au/ssq/2011/winter/nye.pdf [Accessed on: 06.11.2017]

Powell, R. (1994). Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate. *International Organization*, Vol. 48, No. 2 (Spring, 1994), pp. 313-344. The MIT Press. http://www.jstor.org/stable/2706934[Accessed on: 11.08.2019].

Reaves, B., Scaife, N., Bates, A., Traynor, P. & Butler, K. R. B. (2015). Mobile money service, Mobile Problems: Analysis of Branchless Banking Applications in the Developing World. The Proceedings of the 24th USENIX Security Symposium, August 12 – 14, 2015, Washington, D. C. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/reaves [Accessed on: 27.08.2018].

Robert, A. & Jervis, R. (2015). International Politics: Enduring Concepts and Contemporary Issues (Twelfth Edition). Boston Pearson, 2015. https://trove.nla.gov.au/version/206743168 [Accessed on: 11.08.2019].

Secunia (2015). Secunia Vulnerability Review 2015: Key Figures and Facts on Vulnerabilities from a Global Information Security Perspective. https://www.alpha-gen.co.uk/wp-content/uploads/2015/07/secunia-vulnerability-review-2015.pdf [Accessed on: 13.07.2019].

Sandrina, A. & Isabel, C. (2017). Realism. In McGlinchey, S. , Walters, R. & Scheinpflus, C. (Eds.), *International Relations Theory* (pp. 5 – 15). Bristol England: E-International Relations Publishing https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/ [Accessed on: 12.08.2019].

Secureworks (2017). Cyber Threats Basics, Types of Threats, Intelligence and Best Practices. https://www.secureworks.com/blog/cyber-threat-basics [Accessed on: 08.07.2018].

Serianu (2017). Africa Cyber Security Report 2017: Demystifying Africa’s Cyber Security Poverty Line. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf [Accessed on: 12.08.2019].

Sassen, S. (1998). On the Internet and Sovereignty. *Indiana Journal of Global Legal Studies*: Vol. 5: Iss. 2, Article 9. http://www.repository.law.indiana.edu/ijgls/vol5/iss2/9 [Accessed on: 23.01.2018].

Singh, A. S. & Masuku, M. B. (2014). Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. *International Journal of Economics, Commerce and Management*, United Kingdom. Vol. 11, Issue 11, Nov, 2014 ISSN 2348 0386.

Scott, J. S. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. http://www.cambridge.org/9781 1004375 [Accessed on 20.01.2018].

Sheila, B., Jeff, S., David, Z., Cristina, N. R. & Radu, S. (n.d.). “Applying Game Theory to Analyze Attacks and Defenses in Virtual Coordinate Systems”.

Skybox Security (2018). Vulnerability and Threat: Trends Report 2018, Analysis of Vulnerabilities, Exploits and Threats in Play. https://lp.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox_Report_Vulnerability_Threat_Trends_18.pdf [Accessed on: 14.07.2019].

Stanton, J. M. (2001). Galton, Pearson and the Peas: A Brief History of Linear Regression for Statistics Instructors Education, https://www.tandfonline.com/doi/pdf/10.1080/10691898.2001.11910537 [Accessed on: 04.05.2018]

Stein, A. (1982). Coordination and Collaboration: Regimes in an Anarchic World. *International Organization*, Vol. 36, No. 2, *International Regimes* (Spring (1982). Pp. 299-324. The MIT Press. https://www.jstor.org/stable/2706524 [Accessed on: 11.08.2019].

Symantec Corporation (2018). Internet Security Threat Report, Vol. 23, March 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf [Accessed on: 08.08.2018].

Symantec Corporation (2015). 2015 Internet Security Threat Report, April, 2015, Vol. 20. https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf [Accessed on: 08.07.2018].

Thucydides. (1972). History of the Peloponnesian War. Harmondsworth, England Baltimore, MD: Penguin Books.

Trend Micro, Inc. (2017). Definition: Ransomware https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Trend Micro, Inc. (2015). The Fine Line: 2016 Trend Micro Security Predictions. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2016 [Accessed on: 8.2.2018].

Ulman, R. H. (1983). *Redefining Security*, in International Security 8 (1983): 129 – 153).

United Nations Children's Fund (UNICEF). (2014). Overview: Data Collection and Analysis Methods in Impact Evaluation. UNICEF Office of Research, Methodological Briefs. Impact Evaluation No. 10.

Vitor, R. F. (2017). Idealism and Realism in International Relations: An Ontological Debate. Janus.net, e-journal of International Relations, Vol. 7, No. 2 (April, 2017), pp. 14 – 25 http://www.redalyc.org/pdf/4135/413548516002.pdf [Accessed on: 16.08.2019].

Waldemar, P. (2017). The Anarchy of Cyberspace: How the Adaptation of the Westphalia Model can help provide accountability. https://www.linkedin.com/pulse/anarchy-cyberspace- how-adaptation-westphalia-model-can-waldemar-pabon [Accessed on: 2.2.2018].

Walt, S. M. (1991). 'The Renaissance of Security Studies', *International Studies Quarterly*, 35, 1991, pp.211-239.

Walt, S. M. (2002). The Enduring Relevance of the Realist Tradition, in Ira Katznelson & Helen V.Milner, ed. *Political Science: State of the Discipline* (New York & London: W.W.Norton & Company, 2002), pp.197- 230.

Waltz, K. N. (1979). Theory of International Politics. Reading, Mass: Addison-Wesley Public ation Company

Wendt, A. (1995). Anarchy is What States Make of It: The Social Construction of World Politics in James Der Derian ed. *International Theory: Critical Investigations* (London: Macmillan, 1995), pp.129-177.

William, C. & Claudia, M. (2017). Banking in the M-Pesa Age: Lessons from Kenya. CGAP Working Paper, September, 2017. https://www.cgap.org/sites/default/files/Working-Paper-Banking-in-the-M-PESA-Age-Sep-2017.pdf [Accessed on: 05.05.2018].

Wolfers, A. (1962). National Security as an Ambiguous Symbol, in *Discord and Collaboration: Essays on International Politics.* John Hopkins University Press: Baltimore, pp. 147 – 165.

World Economic Forum (2016). Understanding Systemic Cyber Risk. Global Agenda Council on Risk & Resilience. White Paper, October, 2016.

Xan, R. (2007). Kenya sets world first with money transfers by mobile. https://www.theguardian.com/money/2007/mar/20/kenya.mobilephones [Accessed on 17.11.2017]

Appendix A: Questionnaire

Kindly answer the following questions as honestly and accurately as possible. Confidentiality would be observed with any information given. Please do not write your name anywhere on this questionnaire.

Survey to determine Mobile money Services security within Safaricom M-Pesa

1. Name of your dealership (Optional)……………………………………………………

2. How long have your dealership been offering Mobile money services?

   i. 0 – 2 years ( )
   ii. 2 – 4 years ( )
   iii. 5 – 6 years ( )
   iv. 7 and above years ( )

3. What kind of Mobile money services are offered by your dealership? Please tick all that apply

   i. Deposit ( )
   ii. Withdrawal ( )
   iii. Transfers ( )
   iv. Bill Payment ( )
   v. Others, name them………………………………………

4. How did you learn about Mobile money service security?

   i. Workplace training ( )
   ii. Mobile phone Company training ( )
   iii. Personal Initiative ( )
   iv. Others, Name them...

5. In your perception what is your attitude towards Mobile money service security?

Statement	**Disagree Strongly**	**Disagree**	**Difficult to say**	**Agree**	**Agree Strongly**
Clients to receive education on Mobile money service security					

Dealers be taught about Mobile money service security					
Mobile money service security be taught in schools					
Companies to offer opportunities for Mobile money service security training					
Individuals to teach themselves about Mobile money service security					
Mobile money service security education is unnecessary if security software is used					

Disruption of Mobile money services by cyberspace threats

6. This Section is concerned with assessing the extent on whether M-Pesa services have been disrupted by cyberspace threats in any form in your dealership. Please mark (x) in the box which best describes your oPinion on each of the following statements. The choices given are: 1=Very frequent, 2= Frequent, 3== Moderately Frequent, 4=Less Frequent and 5=Not at all

Statement	**Very Frequent**	**Frequent**	**Moderate frequent**	**Less Frequent**	**Not at all**
Power outage on server					
Software malfunction (Dedicated Denial of service attacks)					
Staff collusion with fraudsters (Insider breaches)					
Hacking (Brute force attacks)					
Spams (Malicious code injections)					
Virus attacks					
Sim swaps and Pin change (Account and service traffic hijacking)					
Interoperability (Shared technology vulnerabilities)					
Legal & regulatory gaps					

7. Which of these Mobile money services in your dealership was disrupted? Please tick all that are applicable

i. Deposit (   )

ii. Withdrawal (   )

iii. Transfers (   )

iv. Bill Payment (   )

v. Others, name them……………………………………….

8. To what extent do you agree that the following factors influence the Mobile money service security in your dealership? Use the following Likert scale to rate your level of agreement on the following factors.

Factors	**Strongly agree(5)**	**Agree(4)**	**Undecided(3)**	**Disagree(2)**	**Strongly disagree(1)**
Cost					
Scalability					
Availability					
Enabling environment					
Digital registration of subscribers					
Legal & regulatory gaps					
Customer awareness					

9. What impacts does Mobile money service security have on the following in your dealership? Use the Likert scale to rate your agreement.

Statement	**Strongly Disagree**	**Disagree**	**Moderately Agree**	**Agree**	**Strongly Agree**
Offer more services to the business					
Reduced cost on security training					
Mobile money service becoming more strategic					
Reduced outsourcing of Mobile money service security					
Less time in updating Mobile money service infrastructure					
Reduced staff					

10. What are the greatest barriers to adoption of Mobile money services in your dealership? Kindly tick all those that apply.

    i. Legal and regulatory gaps ( )
    ii. Data security and privacy ( )
    iii. Cyber extortionists ( )
    iv. Staff collusion with fraudsters (Insider breaches) ( )
    v. Sim swaps and Pin change (Account and Service hijacking) ( )
    vi. Virus attacks ( )
    vii. Vendor lock in ( )
    viii. Spams (Malicious code injections) ( )
    ix. Customer Awareness ( )
    x. Digital registration of customers ( )
    xi. Others, name them...

11. How much trust do you have in data security offered by Mobile money service provider to you as dealer? Tick one only.

    i. Very high ( )
    ii. High ( )
    iii. Moderate ( )
    iv. Low ( )
    v. No trust ( )

12. Have you ever incurred losses upon encountering problems with Mobile money service security?

Statement	**Yes**	**No**
Accidental leakage of Mobile money service number	**If yes, approximate** **KShs……….………..Year…………**	
Leakage of your own personal information	**If yes, approximate** **KShs………………...Year…………**	
Unauthorized access	**If yes, approximate**	

	KShs………………...Year…………	
Phishing	**If yes, approximate** **KShs………………...Year…………**	
Password sniffing	**If yes, approximate** **KShs………………...Year…………**	
Theft of data or information on Mobile money service	**If yes, approximate** **KShs………………...Year…………**	