THE GROWING GLOBAL THREAT OF CYBER CRIME: IMPLICATIONS FOR INTERNATIONAL RELATIONS

BY
FRANCISCA DUAH
(10200387)

THIS DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON, IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE MASTER OF ARTS DEGREE IN INTERNATIONAL AFFAIRS

LEGON
JULY 2013
DECLARATION

I hereby declare that this dissertation is the result of an original research conducted by me under the supervision of Professor A. Essuman-Johnson and that apart from other works, which are duly acknowledged, no part of it has been submitted anywhere else for any other purpose.

FRANCISCA DUAH
(STUDENT)

DATE

PROF. A. ESSUMAN-JOHNSON
(SUPERVISOR)

DATE
DEDICATION

This work is dedicated to my parents, Mr. and Mrs. Francis Duah; my uncle Mr. Duah Dankwah and his wife for their support and advice all these years; to my fiancé Joseph Ofori Appiah for his love and support and finally to my beloved brother Francis Boakye Duah, I say thanks for your prayers and assistance.
ACKNOWLEDGEMENTS

Thanks to the Almighty God for making all things possible and with whom this dissertation has seen the light of day. I am most grateful to Professor A. Essuman- Johnson for his patience, guidance and direction in supervising this work. I wish to also thank Mr Alex Amponsah and Mr. Eric Amartey for their support in diverse way. I further want to acknowledge the support of the Ministry of Foreign Affairs and Regional Integration for giving me this opportunity. I am grateful. To other friends - Sammy, Joshua, Clarebel and Grace, I say thanks for your encouragement when things were tough. Finally, I accept responsibility for the views expressed in this essay.
## LIST OF ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASEAN</td>
<td>Association of Southeast Asian Nations</td>
</tr>
<tr>
<td>C&amp;C</td>
<td>Command and Control</td>
</tr>
<tr>
<td>CD</td>
<td>Compact Disk</td>
</tr>
<tr>
<td>CEMAC</td>
<td>Economic and Monetary Community of Central Africa</td>
</tr>
<tr>
<td>CEOP</td>
<td>Communications Electronics Security Group</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CLPC</td>
<td>Cyberspace Law and Policy Centre</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>CSIS</td>
<td>Centre for Strategic and International Studies</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>EAC</td>
<td>East African Community</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECOWAS</td>
<td>Economic Community of West African States</td>
</tr>
<tr>
<td>ECT ACT</td>
<td>Electronic Communication and Transaction Act</td>
</tr>
<tr>
<td>EFCC</td>
<td>Economic and Financial Crimes Commission</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FRANCOPOL</td>
<td>France-Polish</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
</tbody>
</table>
GAF  Ghana Armed Forces
GDP  Gross Domestic Product
GNP  Gross National Product
IBM  International Business Machines
IC3  Internet Crime Complaint Centre
ICT  Information Communication Technology
INTERPOL  International Criminal Police Organization
IPV6  Internet Protocol Version 6
IRC  Internet Relay Chat
ISSER  Institute of Statistical, Social and Economic Research
ITU  International Telecommunication Union
KPMG  Klyneld Peat Marwick Goerdeler
LECIAD  Legon Centre for International Affairs and Diplomacy
NASA  National Aeronautics and Space Administration
NATO  North Atlantic Treaty Organization
NHTCU  National High Tech Crime Unit
OECD  Organization for Economic Cooperation and Development
SADC  Southern African Development Community
SCO  Shanghai Cooperation Organization
SOCA  Serious and Organized Crime Agency
UAE  United Arab Emirates
UK  United Kingdom
UNODC  United Nations Office on Drugs and Crime
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
<tr>
<td>US-CERT</td>
<td>United States Computer Emergency Team</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organization</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
<tr>
<td>WW1</td>
<td>Web War 1</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

DECLARATION ... ... ... ... ... ... ... ... ... ... i
DEDICATION ... ... ... ... ... ... ... ... ... ... ii
ACKNOWLEDGEMENTS ... ... ... ... ... ... ... ... ... ... iii
ACRONYMS AND ABBREVIATIONS ... ... ... ... ... ... ... ... iv
TABLE OF CONTENTS ... ... ... ... ... ... ... ... ... vii
ABSTRACT ... ... ... ... ... ... ... ... ... ... xi

## CHAPTER ONE: RESEARCH DESIGN

1.0 Background of the Study ... ... ... ... ... ... ... ... ... ... 1
1.1 Statement of the Research Problem ... ... ... ... ... ... ... ... ... ... 4
1.2 Objectives of the Research ... ... ... ... ... ... ... ... ... ... 6
1.3 Significance of the Study ... ... ... ... ... ... ... ... ... ... 6
1.4 Scope of the Study ... ... ... ... ... ... ... ... ... ... 6
1.5 Hypothesis ... ... ... ... ... ... ... ... ... ... 7
1.6 Conceptual Framework ... ... ... ... ... ... ... ... ... ... 7
1.7 Literature Review ... ... ... ... ... ... ... ... ... ... 8
1.8 Rationale of the Study ... ... ... ... ... ... ... ... ... ... 13
1.9 Research Methodology and Sources of Data ... ... ... ... ... ... ... ... ... ... 13
1.10 Arrangements of Chapters ... ... ... ... ... ... ... ... ... ... 13

Endnotes ... ... ... ... ... ... ... ... ... ... 14
## CHAPTER TWO: OVERVIEW OF CYBER CRIME

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Introduction</td>
<td>16</td>
</tr>
<tr>
<td>2.1</td>
<td>Origin of Cyber Crime</td>
<td>17</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Cybercrime before Internet</td>
<td>17</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Cybercrime after the Emergence of Internet</td>
<td>19</td>
</tr>
<tr>
<td>2.2</td>
<td>Definitions of Cyber Crime</td>
<td>21</td>
</tr>
<tr>
<td>2.3</td>
<td>Types of Cybercrimes</td>
<td>25</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Hacking</td>
<td>25</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Computer Virus</td>
<td>25</td>
</tr>
<tr>
<td>2.3.3</td>
<td>Malicious Software (Malware)</td>
<td>25</td>
</tr>
<tr>
<td>2.3.4</td>
<td>Botnets</td>
<td>27</td>
</tr>
<tr>
<td>2.3.5</td>
<td>Spam</td>
<td>29</td>
</tr>
<tr>
<td>2.3.6</td>
<td>Phishing</td>
<td>30</td>
</tr>
<tr>
<td>2.3.7</td>
<td>Scams</td>
<td>31</td>
</tr>
<tr>
<td>2.3.8</td>
<td>DNS Based Attacks</td>
<td>34</td>
</tr>
<tr>
<td>2.3.9</td>
<td>Spoofing</td>
<td>35</td>
</tr>
<tr>
<td>2.3.9.1</td>
<td>Cyber Terrorism</td>
<td>35</td>
</tr>
</tbody>
</table>

## Endnotes | Page |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>36</td>
</tr>
</tbody>
</table>

## CHAPTER THREE: IMPLICATIONS FOR INTERNATIONAL RELATIONS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Introduction</td>
<td>38</td>
</tr>
<tr>
<td>3.1</td>
<td>Internet and Cybercrime</td>
<td>38</td>
</tr>
<tr>
<td>3.2</td>
<td>Social Implications</td>
<td>39</td>
</tr>
</tbody>
</table>
3.3 Economic Implications ... ... ... ... ... ... ... 41
3.4 Implications on Market Value ... ... ... ... ... ... ... 45
3.5 National Security Implications ... ... ... ... ... ... ... 47
3.6 Challenges of the Law Enforcement Regulations and the Need for Collective Security in the World ... ... ... ... ... ... ... 51
3.7 Cybercrime in Africa ... ... ... ... ... ... ... 53
3.8 Current legislation and legislative efforts on Cyber Crime in Africa ... ... ... ... ... ... ... 53
  3.8.1 Nigeria ... ... ... ... ... ... ... 53
  3.8.2 South Africa ... ... ... ... ... ... ... 56
  3.8.3 Kenya ... ... ... ... ... ... ... 57
  3.8.4 Cameroon ... ... ... ... ... ... ... 59
3.9 Cybercrime Legislation and Cooperative Alliances in the United States, United Kingdom and Australia ... ... ... ... ... ... ... 59
  3.9.1 United States ... ... ... ... ... ... ... 59
  3.9.2 United Kingdom ... ... ... ... ... ... ... 61
  3.9.3 Australia ... ... ... ... ... ... ... 62
3.10 Legislations and Regulations on Cyber Crime: Case study of selected countries 64
3.11 Collective Security in the Fight Against Cyber Criminals ... ... ... ... ... 67
Endnotes ... ... ... ... ... ... ... ... ... ... ... ... ... 71

CHAPTER FOUR: SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

4.0 Introduction ... ... ... ... ... ... ... ... ... 74
4.1 Summary of Findings ... ... ... ... ... ... ... ... 74
4.2 Conclusions ... ... ... ... ... ... ... ... ... 77
<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3 Recommendations</td>
<td>77</td>
</tr>
<tr>
<td>Endnotes</td>
<td>81</td>
</tr>
<tr>
<td>Bibliography</td>
<td>82</td>
</tr>
</tbody>
</table>
ABSTRACT

The emergence of modern technology has brought about advancement in globalization. Computers and the internet have brought advancement with respect to the way people work, play and interact with each other. However, computers and the internet have presented new ways to engage traditional crimes such as theft, fraud and piracy in the 21\textsuperscript{st} century. These crimes due to the internet have become organized and sophisticated, leading to what is currently known as Cybercrime. The study therefore sought to analyze the implications of cybercrime, which has become an international problem. It further discussed on the weaknesses and challenges of existing laws and regulations. The qualitative method of analyzes was used in conducting the research work. The method focused on using secondary sources related to cybercrime and mainly sourced secondary materials such as existing books, articles and journal articles. The study found out that the implications of cybercrime have been witnessed in areas such as the economies of companies, governments, societal behaviour, the market value and the national security of nations. The study recommended that in order to prosecute cybercrime, a common framework must be created to punish criminals irrespective of where the crimes were committed. Even though most countries have enacted cybercrime laws, there is the need for a collective approach to fight the menace. The international community needs to revisit the issue of sovereignty since this has become a major standing block in the fight against cybercrime.
CHAPTER ONE

RESEARCH DESIGN

1.0 Background of the Study

The emergence of modern technology has brought about advancement in globalization. This has caused many countries to develop and expand their communication network which enables a faster and easier networking and information exchanges. In 2011 there were over 2 billion internet users and over 5 billion mobile phone connections worldwide and over “294 billion emails and 5 billion phone messages are exchanged every day.” Most of the world’s population now depend on constant access to the internet for survival. Due to the over dependence on digital networks by businesses, societies and governments, criminals on the other hand have also come to the realization of changing their ways of operations.

Crimes have become more organized and advanced with the help of technology, leading to what is now known as cybercrimes. According to Douglas W. Thomas and Brian D. Loader, “computer-mediated activities which are either illegal or considered illicit by certain parties and can be executed through global electronic networks.” Over the past few years, the global cybercrime background has changed immensely with criminals employing greater knowledge in cyber fraud, hacking, cyber terrorism, cyber pornography and money laundering which are destructive in all countries. During the past twenty years, smart computer users have fascinated the world and generated a strange feeling composed of admiration and fear by using their machines to commit crimes.
While the internet serves as a good cause for mankind in the form of faster and cheaper way of conducting global affairs, at the same time it frustrates such efforts. Crimes in cyber space bring together offenders, victims and targets situated in different countries and continents and so the offence goes beyond national territories and boundaries.\textsuperscript{6} The activity of cyber criminals have gone beyond minimal cyber hacking into activities which have not only crippled security systems of countries, but also the legislative and socio-economic wellbeing of states worldwide.

The Chairperson of the National Crime Authority in Australia, Tom Sherman, stated that “criminals have begun to use technological advances to create new form of criminal activities many of which have taken an international dimension.”\textsuperscript{7} Cyber crime caught the attention of the forty-three member Council of Europe and its Observers such as the United States, Canada, Israel and Japan who drafted the first International Treaty regulating cybercrime. The treaty was voted on in June 22, 2001 and later approved and opened for signature in November 2001.\textsuperscript{8} This was necessitated after the following series of incidence occurred;

- March 2000 saw a joint operation by the Federal Bureau of Investigations (FBI) and the United Kingdom (UK) police, who arrested a computer hacker called “curador”. The hacker stole details of 26,000 credit cards from e-commerce websites worldwide. The man was identified as Raphael Gray, 18 years old. The cost of his activities was estimated at $3million (£1.8million).\textsuperscript{9}

- Another incident was in May 4, 2000, when a “worm” called the ‘Love Bug’ rapidly affected computers worldwide.\textsuperscript{10} The process was such that affected machines were used to email it, ‘worm’ to other users, corrupting files on computers as it went. Within hours, millions of computers were affected including that of the United Kingdom (UK) and United States of
America (USA) government agencies. The damage caused was alleged to have ranged from an estimated $7 million to $10 billion dollars. The prime suspect was Onel de Guzman, a 24 year old college dropout from the Philippines. The damage was alleged to have ranged from an estimated $7 million to $10 billion dollars. The prime suspect was Onel de Guzman, a 24 year old college dropout from the Philippines. In August 2000, all charges against de Guzman were dropped because the Philippines did not have laws that covered computer hacking under which he could have been convicted.

The Director of the Federal Bureau of Investigations (FBI) Robert Mueller in February 2003 at a USA senate meeting two years after the September 11 attacks is reported to have confirmed grounds made by cyber criminals. He is quoted as saying that “cyber terrorism is a growing threat to the US national security”. He stated that Al-Qaeda and other terrorist groups were increasingly becoming computer confident and would in future have greater chances to strike by targeting critical computer systems using electronic tools. In 2008 and 2011, hackers hacked into the systems of the Pentagon and made away with 24,000 files from the Defence Industry networks within a single invasion. This was confirmed by the Deputy Secretary of Defence, William Lynn.

A cyber attack on Estonia in 2007, blocked websites and paralyzed the country’s entire internet infrastructure. At the peak of the crisis, bank cards and mobile-phone networks were temporarily frozen. Cybercrimes have also become predominant on the African continent with countries like Nigeria, Cameroun and Ghana experiencing cybercrime activities. In Ghana, two middle aged Nigerians were on 11th November 2012, arrested for allegedly hacking into the mail server of the Ghana Armed Force (GAF) in an attempt to divert $13,978 belonging to the Ghanaian Peace keepers. Peter Gottschalk in his book titled “Policing Cybercrimes”, cited Nigeria as a
hub for financial crimes.\textsuperscript{19} He further stated that 122 countries at an INTERPOL meeting complained about Nigerian’s involvement in financial fraud popularly referred to as “Advanced Fee Fraud” (419) in their countries.\textsuperscript{20}

1.1 Statement of the Research Problem

Cyber crime like other forms of crime is multi-faceted and an ever changing problem. In the 21\textsuperscript{st} century, where there is advancement in technology, criminals are no more confined to their own countries but have crossed boundaries without fear. Offenders are not likely to be recognized physically by security authorities or even their victims because of the advancement in using the internet in communication. Criminals operate from country to country, taking advantage of the weaknesses of investigative tools of cybercrime in most countries. They hack the systems of businesses, individuals and governments making cybercrime transnational, which knows no boundaries.

Globalization, to a considerable degree, has created an interface that facilitates international trade, finance, political cooperation, security arrangements, among others. It is apparent that globalization has benign attributes, such as the proliferation of technology, merging of cultures, and the prevalence of international finance, among others. Consequently, it is tempting to presume that globalization has no dysfunction. However, in recent times, the globalization of insecurity points to a number of contending issues that the international community must grapple in the light of globalization. Of interest to this research, among others, is the prevalence of cyber crime, a product of globalization that has the potential to undermine the security profile of states and their relationship among each other.
For both developed and developing countries, the far-reaching implications of globalization have been witnessed in the area of security, where the widespread nature of cybercrime threatens to undermine the security profile of states and their interaction with each other. Cyber activities such as hacking, cyber pornography, fraud and many others have increased in sophistication due to advancement in technology. States are cautious when conducting businesses through the internet due to the infiltration of networks by cyber criminals. This research explores the various dimensions of cyber crime and the need of combating the menace in the wake of advancement in technology.

In this regard, the key research questions the study seeks to answer are:

- What policy measures have been adopted in the International system to address cyber security in the wake of globalization?
- What is the level of cooperation between states in the wider international community against the background that international cooperation is critical to ameliorating cyber crime?
- And what is the state of implementation of these policy measures if any?

1.2 Objectives of the Research

Considering the importance of the subject matter to the international community, this research seeks to do the following:

- Examine the policy measures available in curbing or stopping cyber crimes in the world in the wake of globalization.
- To know the level of cooperation between states in the fight against cyber crime.
• Assess how effectively the policy measures adopted are being implemented by States.
• To recommend appropriate responses if any to help curb or stop the cyber crime menace.

1.3 Significance of the Study

The study gives readers an understanding of what cybercrime is and how its emergence has the ability to disrupt security setups, economies, societies, market values of organizations and inter relations among states.

1.4 Scope of the Study

This study focuses primarily on the role and use of the internet in perpetrating crimes in the world and its implications for international relations. In addition countries such as Nigeria, South Africa, Kenya, Cameroon, United States of America, United Kingdom and Australia reported to have high cases of cybercrime would be discussed. Their legislative efforts in combating the menace would also be discussed.

1.5 Hypothesis

The emergence of technology has brought advancement in globalization and the overall drive towards development but a further increase in cybercrimes which threaten individual, national and global security.
1.6 Conceptual Framework

This study is situated within the concept of globalization, a concept that conceives the world as a whole niche which has many similarities and links that cut across political boundaries, national identities, and cultural differences. For the purpose of this study, Thomas Friedman’s definition of globalization is used. He defines the concept as “not a mere phenomenon, but an overarching international system shaping the domestic politics and foreign relations to virtually every country.”

Globalization has brought together various facets of issue areas, such as international trade, finance, telecommunication, religion, the merging of cultures, among others. In essence, globalization conveys the notion of a single community that is inextricably linked by a web of interactions. For instance, trade has accelerated, leading to the establishment of global institutions such as the World Trade Organization (WTO), to safeguard the overall interests of states in international trade. International finance is on the ascendancy, migration has accentuated as people move across borders in search of improved welfare. Health has assumed global dimensions, a fact evidenced by the rapid manner in which diseases move quickly across national borders.

Technology has made it possible to communicate thousands of miles apart as the world is said to be “at one’s fingertips”. Environmental issues have become global as corrosion in the environmental profile of one state, such as emission of greenhouse gases, has a snowballing effect on other states. Globalization analysts such as Joseph Stiglitz, James Mittelman, Thomas Friedman, Bhagwati Jagdish, among others, have explained the nuances of globalization, pointing both the positive dimensions and dysfunctions of globalization. There is a considerable
degree of consensus that globalization presents both opportunities and risks. Obviously, globalization is a formidable tool for socio-economic and political development of states.

Of concern to this research is that idea that globalization has the potential to trigger a universal pillage, a concept that denotes the exacerbation of insecurity in the light of globalization. At the heart of this research is the fact that globalization can also trigger insecurity globally. This is evidenced by the use of technology for criminal adventures, including defrauding, cyber terrorism, and computer hacking. It is in the light of the security implications of globalization that this research seeks to interrogate policy set up in response in the area of cyber crimes.

1.7 Literature Review

Authors of various books who write on cybercrime have alluded to the fact that there is an obvious link between the concept of globalization and cybercrime. Susan W. Brenner explains in her book, Cyber Crime; Criminal Threats from Cyberspace that crimes carried out by cyber criminals often reflect the emotions of persons in the society. She further mentions greed, obsession and the desire for revenge as reasons why many crimes are committed. She explains that the amazing fact about cybercrime is the realization that victims may be at a distance or a world away from each other.

A Twilight Zone episode aired in 1960 according to Brenner depicts how two aliens fiddled with the technology of residents of Maple Street resulting in humans turning against each other. She further argues that the only entities that could have implemented the said scenario in the Twilight Zone episode were utility companies. This perception currently does not hold as the present
human population uses cyber space in an essential and irreversible way. The most significant aspect of cyber space according to her is that, access to it erodes the monopolization of power by governments and corporations. The book recounts the first reports of computer related crimes in the 1960s when large mainframe systems were used without the internet. It states that computer crimes committed without the internet were not so much of an international problem but on a company-to-company basis committed by staff. The writer further talks of the emergence of computer expertise commonly known as hackers. They often make secured areas accessible to anyone with the requisite computer knowledge. The activities of hackers have been the backbone of all cyber attacks in recent times.

Yar Majid, in his work “Cybercrime and Society” views cybercrime as “not so much of a single, distinctive, kind of criminal activity; but more to a varied range of illegal and illicit activities that share in common the unique electronic environment (cyber space) in which they take place.” He argues that cybercrime is a phenomenon that affects a wide range of disciplines including criminology, sociology, law, socio-economy, cultural, media studies, science and technology business management and computing. Consequently, he states that different academic contributions tend to focus on some selected aspects of the cybercrime problem to the detriment or neglect of others. Yar talks about the effects of a non-consistent definition of cybercrime which to him affects law enforcement agencies and their ability to prosecute offenders. The author further in the book gives some reasons why cybercrime offences remain unreported. He states that in some cases victims consider the offence inadequately “serious” to warrant an arrest or they may feel that there is little likelihood of a satisfactory resolution. He classifies cyber crimes into two; the “computer-assisted” crimes which existed before the internet but takes on a
new life in cyber space such as fraud, pornography, money laundering, theft and sexual harassment. The “computer –focused” crimes on the other hand without the internet could not have worked. These crimes consist hacking, viral attacks and website defacement. It is evident that the writer agrees with the fact that laws on cybercrimes are either limited or nonexistent and therefore the arrest and conviction of offenders would prove difficult. However he fails to identify cooperation among law enforcement agencies.

According to George Curtis, cybercrime laws in recent times have experienced difficulty in keeping pace with advances in technology. He explains that this often affect any attempts to resolve issues relating to cybercrime. As a result, law enforcement agencies often attempt to solve issues relating to cybercrime by drawing some analogy to traditional crime. Curtis mentions that prior to 1984, crimes involving computers were prosecuted in federal courts under existing provision of the Federal Criminal Code dealing with other crimes, typically wired fraud. He further states that the first Federal Statute specifically addressing computer crime was the Counterfeit Access and Computer Fraud Act of 1984.

Peter Gottschalk, in his book “Policing Cybercrime” describes cybercrimes as a global issue affecting almost all countries. The author agrees with Adam Salifu that the internet is a “double-edge sword that provides many opportunities for individuals and organizations to develop and prosper, but at the same time opportunities to commit crime.” Gottschalk mentions Nigeria, as a hub for cybercrimes. He explains that Advanced Fee Fraud is the most perpetrated offence by Nigerians. He states that cybercrime is a de-territorialized phenomenon that has surfaced with globalization. In his book, he classifies computer crimes as financial crimes and gives examples
as fraud, theft, manipulation and corruption. He defines financial crimes as crimes against property, involving the unlawful possession of materials belonging to another and for one’s own selfish gains.³⁰

According to Gottschalk, cybercrime has gone beyond hacking into areas such as the development of fake websites which generates billions of dollars for offenders. The growth of these websites transcends countries and governments.³¹ In his view, most victims of these crimes are not to be blamed because development of fake websites are designed and made to appear as though they were original. This makes it difficult for users to identify it manually.³² He believes that people should be educated on what he terms as ‘fraud cues knowledge’ which he explains as the basic designed elements unique to all websites. To him the unavailability of such elements automatically disqualifies a particular website. He believes these could serve as indicators for victims.³³

1.8 Rationale of the Study

It is hoped that this research raises awareness about the various trends of cybercrimes and its alarming rate of increase. It further looks at the implications for international relations and seeks to provide valuable information for policymakers, civil society groups and the media on the need to regulate and implement extensive policies to help combat the menace through global cooperation.
1.9 Research Methodology and Sources of Data

The study uses mainly qualitative data analysis in conducting the research work. This method focuses on using secondary sources related to cybercrime. The study mainly sourced secondary materials such as existing books, articles and journal articles from the Balme library, ISSER library and the LEClAD library. Materials were also sourced from the internet.

1.10 Arrangements of Chapters

This study is divided into four chapters:

Chapter one of the studies constitutes the Research Design.

Chapter Two reviews the origin, history and types of cybercrime.

Chapter Three looks at the implications of Cybercrimes for international relations and further discusses the laws and strategies put in place by global security agencies and governments in curbing cybercrime activities.

Chapter four is a summary of the findings, conclusions and recommendations.
ENDNOTES

2ibid., p. 2.
3ibid., p. 2.
7ibid.
10ibid., p. 2.
11ibid., p. 3.
12ibid., p. 3.
13US Department of State, 2003 as cited by Yar Majid op.cit p.3.
14ibid., p. 3.
15ibid., p. 3.
16KPMG International Cooperative., p. 9.
20ibid., p. 14.
23ibid., p. 2.
24Yar Majid., p. 5.
25ibid., p. 5.
26ibid., p. 10.
29ibid., p. 14.
30ibid., p. 14.
31ibid., p. 17.
32ibid., p. 17.
33ibid., p. 17.
2.0 Introduction

This chapter reviews the origin, history and development of cybercrime. The history is divided into two parts comprising history of cybercrime before the advent of internet and after the advent of internet. It has been argued by many scholars that cybercrime took the shape of a more skilled and sophisticated crime after the emergence of internet technology in the 1990s. The other part of the chapter further discusses the different definitions of cybercrime by scholars which helps understand the phenomenon better. The concluding part of this chapter focuses on the types of cybercrime which are commonly committed in the world.

Since the advancement of technology and the emergence of the internet that brought about cybercrime, it has been referred to as crimes that happen specifically over networks. Cybercrime is the third top priority under the Federal Bureau of Investigations (FBI) in the United States of America. According to the FBI’s estimation, cybercrime in the USA cost industries about US$400 billion in 2004. At the international level, cybercrime is one of INTERPOL’S top five priorities. It is therefore of utmost importance to discuss how far the actions of cyber criminals have caused implications for international relations.

2.1 Origin of Cyber Crime

According to Professor Susan W. Brenner, in her book titled “Cybercrime: Criminal Threats from Cyber Space”, she divided the origin of cybercrime into two phases, firstly from the time of
mainframe computers to the 1990s when the internet and private computers were becoming more sophisticated and universal. The second phase according to the same book originates from 1990 to the present times. These two phases can further on be divided into two periods; prior to the emergence of the internet and the emergence of the internet.

2.1.1 Cybercrime before Internet

In the 1960s when computers were largely mainframe systems, the first imprint news of computer crimes were committed. Several companies in 1946 began working on a commercial mainframe and by 1951, the UNIVersal Automatic Computers (UNIVAC), created by a company of the same name was used by the Census Bureau.

The importance of the UNIVAC (UNIVersal Automatic Computers) was known when in 1951 CBS TV Network used a UNIVAC to forecast the results of the Presidential elections in the United States of America. This incidence also led to the popularization of the new technology. The world as at this period was introduced to a new type of computer which had a new set of multiprocessing and operational system. These were the mainframe computers which had no internet. In 1960, a typical IBM Mainframe cost several million dollars and also needed an entire room to house it. This type of computers required a special air conditioning system to ensure that its vacuum tubes would not overheat and fry the data in the computer.

Computer crimes in the 1960s and 1970s differed from the cybercrime we deal with today. There were no internet and mainframes were not networked to other computers. It must be emphasized that at this period, only a selected group of researchers were allowed to use a
mainframe. According to Brenner W. Susan, to access a mainframe, a researcher had to give the
data to a key punch operator who used a machine to punch holes in “manila cards”.\(^\text{11}\) The holes
code the researcher’s data into a form the machine can read. The cards are then given to another
operator who feeds it into a machine that transmits the information to the mainframe. At some
point, the researcher would receive a printout showing the machine’s analysis of his data.
Mainframes were expensive and not easy to be used due to the processes one had to go through.
Only a few people could utilize it. Due to the fact that mainframes were not networked with
other computers, only a few people were in the position to commit computer crimes.\(^\text{12}\) Those
who had the opportunity to commit crimes were employees who had access to mainframes. The
most common type of computer crimes in this era was financial crimes, whereby an employee
uses his access to a mainframe computer to improve his life.

An example of such an incident was committed in the mid-1960s, by Val Smith (an alias), an
accountant who used UNIVAC to automate billing processes to dummy companies he had set
up to provide imaginary services to his employer. He is reported to have made $250,000 a year.\(^\text{13}\)
In California, a teller used his access to a bank’s computer to steal more than $100,000 from his
employers.\(^\text{14}\) The crimes committed before the emergence of the internet had one thing in
common. The victims were a company, an institution or a government agency who could afford
to buy the mainframe computers.\(^\text{15}\) However one must know that these crimes were generally
incapable of inflicting “harm” on an individual. In the 1970s, the use of computer systems and
computer data increased further.\(^\text{16}\) At the end of the decade, an estimated number of 100,000
mainframe computers were operating in the United States.\(^\text{17}\)
2.1.2 Cybercrime after the Emergence of Internet

The Internet’s rapid growth has far outpaced methods of regulatory control, and this has led to the emergence of new criminal opportunities and presented important challenges for policing across all corners of the globe.\(^\text{18}\) In the 1980s, personal computers became popular with an increasing interest in the development of software by the youth at the time and also researchers. This period also saw the emergence of the first forms of software piracy and crimes related to copyright.\(^\text{19}\) The 1990’s saw an era whereby the internet growth was tremendously fast due to globalization. This was the time when personal computers and internet were becoming sophisticated and criminals emerged to take advantage of the opportunities and vulnerability both offered.\(^\text{20}\) The emergence of networking during this time enabled offenders to enter a computer system without being present at the crime scene. The period came with an opportunity which allowed culprits to spread malicious and computer viruses.\(^\text{21}\)

The 1990s saw the introduction of the graphical interface (“www”) followed by a rapid growth in the number of internet users which led to new challenges. With the help of the internet in the 1990s, local crimes such as theft, fraud, money laundering and others committed in the 1960s and 1970s became rated as transnational crimes because they defiled boundaries of countries. Further, information legally made available in one country was made available globally—even in countries where the publication of such information was criminalized.\(^\text{22}\) In December 1995 there was an estimated 16 million people who could use the internet worldwide. The figure rose to over 580 million by May 2002 which was almost 10 percent of the world’s total population.\(^\text{23}\)
The 21st century came with its highly advanced methods of committing crimes such as “phishing” and botnet attacks. The spread of internet-related crimes was more frequent in areas like the USA, Canada, Europe, Australia and Japan. The internet crimes that emerged during this period were known as hacking and not cybercrime as now called. Hackers interfered with the systems they invaded and has been established as one of the crimes that come within the domain of cybercrimes.

The most notorious hacker of the 1990s was Kevin Mitnick. He grew up in Southern California and was a phone phreak. In 1988, he hacked a computer at the NASA Jet Propulsion Laboratory and the same year FBI agents arrested him for hacking the Digital Equipment Corporation and stealing prototype operating system software valued at $1 million. The company alleged that it spent $4 million tracking Mitnick’s invasion into their system. Other hackers such as Edwin Pena and Robert Moore in 2006 were arrested by the FBI for hacking into phone services to resell for profit. They were further accused of hacking the networks of 15 communications providers and hundreds of businesses. Today’s crimes cause humiliations to individuals, institutions and governments in general because of the dependency on electronic devices. Currently people handle their businesses in their homes just with a click of a button. The over dependency on the internet has led criminals to re-strategise their ways of operations.

2.2 **Definitions of Cyber Crime**

The term cyber is derived from the word cybernetic, taken from the Greek word “kybernetes”. The term was invented in 1948 by a United States Mathematician Norbert Wiener, the originator of cybernetics who defined it as “a formalization of the ideas of feedback, with many
implications for engineering, systems control, computer science, biology, philosophy and the organization of society” 30 Wiener saw cybernetics as a research tactic which was to help bring all disciplines together in researching.

The United States Department of Justice in an attempt to define cybercrime summaries the definition in a three-stage classification:

- Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and Dos attack.
- In an existing offence where the computer is a tool used to commit the crime. For instance child pornography, stalking, criminal copyright, violations and fraud.
- Crimes in which the use of the computer is an incidental aspect of the execution of the crime but may help generate evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between an offender and a victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more of a repository for evidence. 31

Cybercrime is defined as crimes committed through illegal use of computer systems. The United Nations Congress on the Prevention of Crime and Treatment of Offenders, at its tenth workshop devoted to the issues of crimes related to computer networks, defined cybercrime in two subcategories: Cybercrime in a narrow sense and cybercrime in a broader sense.

- Cybercrime in a narrow sense is related to any illegal behaviour operated by using the electronic medium which targets the safety of computer systems and the data processed by them.
In a broader sense, it is also defined as any illegal behaviour committed using a computer system or networks. It includes crimes like illegal possession and distributing of information using a computer system or networks. In his view, every crime committed on a computer connected to the internet is always a cybercrime.

Another definition is by Pavan Duggal, a cyber law expert who states that, “any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime.” In his view, every crime committed on a computer connected to the internet is always a cybercrime.

Douglas Thomas and Loader Brian describes cybercrimes as “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.” They further explain that, the global connectivity of the internet makes it much easier for criminals to act beyond national boundaries to conduct their illegal affairs. In the same way, the United States Department of Justice (DOJ) defines computer crimes as “any infringement of criminal law that involves knowledge of computer technology for their perpetuation, investigation or prosecution.” The Department further expands the definition of cybercrime to include, any activity that uses a computer for the storage of evidence. With this definition the DOJ sees cybercrimes as crimes that are committed with the sole intention of using the computer system for an unlawful operation. Another view of what is cybercrime is more easily expressed by David Wall who categories cybercrimes into four established legal grouping:

a) Cyber-trespass which implies the crossing of boundaries to possess people’s property and further causing harm. He gives examples of such activities as hacking and the spreading of defacement viruses.
b) Also deception in cyber space and thefts or stealing of either money or property using credit cards or piracy is considered as cybercrime.

c) Cyber pornography is also another illegal breach of the law. It defiles the morality and decency in the society.

d) Cyber-violence and the causing of psychological harm to a person is a cyber offence. Wall further explains that rousing up physical harm against others, thereby violating laws relating to the protection of the person is a cybercrime. The practicing of hate speeches and stalking on the internet is also prohibited.

This definition confirms the views of scholars that cybercrime does not take into account the boundary limitations of a country.\(^{36}\)

The Council of Europe’s Convention on Cybercrime’s definition of cybercrime has also come to be of legal standing. The Convention which was established in 2001 is aimed at protecting society against cybercrime by adopting appropriate legislations and fostering international co-operations.

The Convention defines cybercrime in four main categories according to its nature.

a) Offences against the privacy, integrity and availability of computer data and systems. This is mentioned in Article 2 to 6 of the Convention;

b) Computer-related offences which include computer related forgery and fraud. Articles 7 and 8;

c) Content-related offences; this contains certain provisions for offences related to child pornography. Article 9 is important to it;
d) Offences related to the infringement of copyrights and related rights, this explained in Article 10 of the Convention.\textsuperscript{37}

\section*{2.3 Types of Cybercrimes}

According to scholars these are the most committed cybercrimes in the world:

\subsection*{2.3.5 Hacking}

Hacking has been a very frequent form of cybercrime in recent times. It can be referred to as the testing and exploring of computer systems, highly skilled computer programming or the practice of accessing and changing other people’s computer. It is often intended to disrupt the normal behaviour of network connections and connected systems. Hacking may be carried out with honest aims or with criminal intent.\textsuperscript{38}

\subsection*{2.3.6 Computer Virus}

A computer virus is a computer program that connects to an application program or other system software which subsequently activates, causing severe damages to computer systems or files.\textsuperscript{39}

\subsection*{2.3.7 Malicious Software (Malware)}

Malware (for “malicious software”) is a general term for software designed to damage or subverts a computer or information system.\textsuperscript{40} Some malicious software includes viruses, worms, Trojan horses, backdoors, spyware, and programming that gather details about a computer user without permission.\textsuperscript{41}

**Brief explanations to these Malicious Software**

- Spyware- Spyware is any technology that helps in getting information about a person or an organization without them knowing. It can also be programmed into someone's computer to assist in obtaining secret information about the owner of the computer. The information obtained is sometimes passed on to advertisers or other interested parties.
Spyware can get in a laptop as a software virus or as the result of installing a new program.

- **Virus** - A virus is a program or programming code that continuously repeats itself when copied or initiating its copying to another program, computer boot sector or document. Viruses can be spread as attachments to an e-mail note or in a downloaded file and are most often present on diskettes or compact disks (CD).

- **Worm** - Worms are self-replicating viruses that do not change files but duplicates it. Worms are commonly noticed only when their uncontrolled replication guzzles system resources, slowing or halting other tasks.

- **Logic bomb** - A logic bomb is a programming code which is mostly inserted either secretly or deliberately. It is designed to execute its functions under circumstances such as the drop of a certain amount of time or the failure of a program user to react to a program command. It can also be referred to as a delayed-action computer virus or Trojan horse. When a logic bomb gets to its peak of destruction it displays or prints out false messages, delete or corrupt data and can have other undesirable effects.

- **Trojan (Trojan horse)** - A Trojan horse is a program where malicious or harmful codes are contained inside. This is seen as harmless programming or data which can be controlled. Trojan horses can ruin certain areas on a hard disk and may be generally redistributed as part of a computer virus.\(^{42}\)
2.3.4 Botnets

A botnet is a gathering of internet-connected programs that correspond with other similar programs in order to perform tasks. This can be normal as keeping control of an Internet Relay Chat (IRC) which is a procedure for live interactive internet text messaging (chat). It can be used to send spam email or take part in a distributed denial of Service attack (DDos). Computers can be co-opted into a botnet when they execute malicious software. These enable a cyber criminal to remotely control an infected computer over a network. Such an affected computer is often called a “robot” or “bot” computer. When several computers are affected with a backdoor ;( a
category of malware) and become a bot, they can be simultaneously controlled from a single remote ‘command and control’ (C&C) mechanism. These remotely controlled networks of bot computers are known as “botnets”.

**FIGURE 2** The biggest botnets for 2009

<table>
<thead>
<tr>
<th>botnet</th>
<th>estimated botnet size</th>
<th>Country of Infection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rustock</td>
<td>540k to 810k</td>
<td>Brazil (21%), USA (9%), Poland (7%)</td>
</tr>
<tr>
<td>Cutwail</td>
<td>100k to 1600k</td>
<td>Vietnam (17%), RepKorea (12%), Brazil (10%)</td>
</tr>
<tr>
<td>Bagle</td>
<td>520k to 780k</td>
<td>Brazil (12%), Spain (9%), USA (9%)</td>
</tr>
<tr>
<td>Bobax</td>
<td>100k to 160k</td>
<td>Spain (12%), Italy (7%), India (7%)</td>
</tr>
<tr>
<td>Grum</td>
<td>580k to 860k</td>
<td>Vietnam (18%), Russia (17%), Ukraine (8%)</td>
</tr>
<tr>
<td>Maazben</td>
<td>240k to 360k</td>
<td>Romania (17%), Brazil (11%), Saudi Arabia (7%)</td>
</tr>
<tr>
<td>Festi</td>
<td>140k to 220k</td>
<td>Vietnam (31%), India (11%), China (5%)</td>
</tr>
<tr>
<td>Mega-D</td>
<td>50k to 70k</td>
<td>Vietnam (14%), Brazil (11%), India (6%)</td>
</tr>
<tr>
<td>Xarvester</td>
<td>20k to 36k</td>
<td>Brazil (15%), Poland (11%), USA (10%)</td>
</tr>
<tr>
<td>Gheg</td>
<td>50k to 70k</td>
<td>Brazil (15%), Poland (8%), Vietnam (8%)</td>
</tr>
<tr>
<td>Unclassified Botnets</td>
<td>120k to 160k</td>
<td></td>
</tr>
<tr>
<td>Other, smaller botnets</td>
<td>130k to 190k</td>
<td></td>
</tr>
</tbody>
</table>


According to the Cyberspace Law and Policy Centre (CLPC), from the University of New South Wales, botnets are considered to be one of the biggest enablers of cybercrime. The Law further states that almost every major online crime being committed in the world can be traced to botnets.47
FIGURE 3: Initiation, growth and function of a botnet

Source: OECD Committee for Information, Computer and Communications Policy, Malicious Software (Malware): A Security Threat to the Internet Economy, OECD, June 2008 p.23

2.3.5 Spam

A spam is the electronic equivalent of a “useless mail” which is unwanted and usually sent in bulk to thousands or even millions of people as messages at a time. Spam impedes the flow of legitimate internet messaging around the world. A spam is executed by the computerized
harvesting of email accounts and by spyware. Some spam advertises unwanted products which are often harmless.\(^4\)

2.3.10 Phishing

Phishing is the making of an effort to acquire information such as usernames, passwords, and credit card details through illegal means masquerading as a trustworthy entity in an electronic communication.\(^5\) The Australian Institute of Criminology in its High Tech Crime Brief, Canberra, 2006 provided an example of a Phishing website which shows how a website has been forged. The Figure 4 shows the top section of a web page which appears to be from the legitimate “Bank of the West” website.

![Figure 4: Example of phishing.](image)

Source: Australian Institute of Criminology, Exhibit No.5, and p.8 as quoted in in Hackers, Frausters and Botnets: Tackling the Problem of Cybercrime report by the Parliament of Australia in 2010.

However, in Figure 5 shown below it would be proven how, upon a closer view of the web address in the top bar of the browser, it can be seen that the ‘W’ in the “Bank of the West” has been replaced with two ‘V’ to give the appearance of a W.
2.3.11 Scams

Online scams have become another profitable activity for cyber criminals. Some of the scams are romance scams, Advanced Fee Scams, fake lottery and ticketing or online shopping scams.\(^{50}\)

The Federal Trade Commission\(^{(FTC)}\)\(^{51}\) have listed some commonly used scams being used by scammers. The Commission is however of the view that these listed scams are merely “recycled scams” that were being used before the emergence of emails and which have now become the predominantly used approaches by scammers. The List includes;\(^{52}\)

- Bogus business opportunities
- Chain letters
- Health and diet scams
- 419 Advanced Fee Fraud and;
- “Free” goods scam

The following sections describe some common fraud schemes initiated through email:
Bogus Business Opportunities

The work of these scammers is to promise their victims of an opportunity beyond their wildest dreams which is expected to make them a great deal of money within the shortest time. It is the responsibility of these scammers to entice their victims with headline emails such as “Be your own boss”, “Make $100 a day”, “Work only 8 hours a week” and “Work from home.” These emails can further have subjects lines that look like the following;

- Get Rich Quick
- Use the Internet to make money
- Make your Computer Work for you very efficiently!
- Succeed by Using the Internet.

These scammers mostly provide their victims with addresses or websites from which one can for a fee acquire an “information kit” or a form to fill.

Health and Diet Scam

This type of scammers play on the emotions of their victims who feel insecure either about their figure or health status. Such victims are persons who find it difficult to discuss their problems with doctors, families and also find it financially difficult to afford drugs. The scammers offer them solutions which seem to be easily accessible and cheaper.

The emails have subject titles that read like the following:

- DECERASE YOUR WEIGHT FAST,
- Feel Healthy and younger
- Enhance your Sexual Performance Drastically
- Fight Cancer at the lowest cost
While these drugs have testimonies online by supposed users, they are in most cases fake.

**419 Advanced Fee Fraud**

The term ‘419’ is taken from the section of the Nigerian Penal code that addresses fraud.

These type of scam have been associated with Nigerian citizens across the world. 419 scams are identifiable by their subject lines like URGENT REPLY NEEDED and Re: Pleased to meet you!

A ‘419’ Advance Fee Fraud comes in the form of an email that looks like this

Date: Wednesday, August 24, 2008 5:55 PM -0700 From: "Mr. Henry BasseyUdoma" <henrybassey_udoma@example.com.ar> To: mrtarget@example.com Subject: From: Henry (Regarding Dr. H. Paul Jacobi)

From: Henry (Regarding Dr. H. Paul Jacobi)

Hello, I am sending you this private email to make a passionate appeal to you for assistance. Kindly accept my apology for contacting you this way and forgive me if this is not acceptable to you. My name is Henry Bassey Udoma; I am an auditor at one of the Nigerian Banks. On Tuesday, 19 January, 2006, one Dr. H. Paul Jacobi a foreigner, made a numbered time (Fixed) Deposit, valued at £10,550,000.00 (Ten Million, Five Hundred and Fifty Thousand Pounds) for twelve calendar months in my Bank Branch.

Upon Maturity, we sent a routine notification to his forwarding address but got no reply. After a month, we sent a reminder and finally we discovered from his company that Dr. Paul A. Jacobi was aboard the Egypt Air Flight 990, which crashed into the Atlantic Ocean on October 31, 2006. After further investigation, it was discovered that he died without making a WILL and all attempts to trace his next of kin proved abortive…

With this the scammers try to get the victim to sympathize with them, and then slowly convince the victim of the legitimacy of their deals with usually forged documents to back their claims.

After the necessary verifications, the perpetuators further request that the victims make advance money to pay bogus fees or bribes to get the transactions through.

**2.3.12 DNS Based Attacks**

The Domain Name System (DNS) decodes web and e-mail addresses into arithmetical strings, serving as a kind of telephone directory for the internet. Every internet request has to go through
a DNS Server and DNS is one of the foundations of the internet. Thus, the DNS enable users have easy access to computers that host web pages without the need for complicated codes. Cyber criminals subvert the DNS in a number of ways, such as ‘domain hijacking’ where a cyber criminal takes control of a domain name by stealing the identity of a domain name owner. The hacker then uses this domain name to host a malicious website. DNS hijacking needs the serves of a Trojan that changes the settings on a user’s computer to access the DNS server instead of legitimate ISP server, thus enabling users to be diverted to false websites.\textsuperscript{54}

**Figure 6 shows how DNS works:**

*Source: www.bustathief.com accessed on 10\textsuperscript{th} June 2013*
2.3.13 Spoofing

The word “spoof” means to hoax, trick, or deceive. In the IT world, spoofing refers to tricking or deceiving computer systems or computer users. This is typically done by hiding one’s identity or faking the identity of another user on the internet.\textsuperscript{55}

2.3.13.1 Cyber Terrorism

According to Dorothy Denning, a security expert, cyber terrorism is “politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage.”\textsuperscript{56}
ENDNOTES


3 Brenner S. W., Cybercrime: Criminal Threats from Cyber Space (Santa Barbara, California: Greenwood Publishing group 2010), p. 46.

4 ibid p. 46.

5 ibid p. 46.


7 ibid.


9 ibid p. 19.

10 Brenner Susan W., p. 10.

11 A manila card is a type of paper from a semi-bleached wood fibre which has better printing qualities. It originates from the Philippines and can be referred to as ‘vanilla paper’ and given to children to draw their art.

12 ibid., p. 11.

13 ibid., p.10.

14 ibid., p. 12.

15 ibid., p.12.


20 Brenner Susan W., p. 23.

21 Malicious software is a general term for software designed to damage or subverts computer or information systems. A computer virus is a computer program that connects to the application or other system software which subsequently activates, causing severe damages to a computer system or a file.


24 The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to “phish” for passwords and financial data from sea of Internet users.

25 Botnets is a short term for a group of compromised computers running software that are under external control.


27 Mitnick Kevin’s, history is taken from these sources, cyber punks, Hafner Katie and Markoff John and Cyber crime, Brenner, Susan W. as quoted by Khadam, Nadia’s; Insight to Cybercrime p. 65.


30 ibid.


32 The UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April, 2000. P. 5

33 http://www.rediff.com/netguide/index.html


37 Council of Europe Convention on Cybercrime, (Budapest, 23.XI.2001).


40 Urbas G. and Choo K.R, op. cit.

41 www.starstandard.org/guidelines/DIG2012v1/ch11s03.html accessed on 10th June 2013.

42 ibid.


44 ibid.


46 ibid.

47 Cyberspace Law and Policy Centre(CLPC), submission 62, p.3 from http://www.cyberlawcentre.org/index.html.


50 AIC, Submission 41, p.4; Mr. Scott Gregson, Australian Competition and Consumer Commission (ACCC), Transcript of Evidence, 18 November 2009,p.1: ACCC,Exhibit 16, p.10.


53 www1.villanova.edu/villanova/publicsafety/crime/recognizing_and_avoiding_email_s.html.


CHAPTER THREE

IMPLICATIONS FOR INTERNATIONAL RELATIONS

3.0 Introduction

This chapter tests the hypothesis which shows how the emergence of globalization has brought advancement in technology but a further increase in sophisticated cybercrimes which threatens individual, national and global security and the overall drive towards international development. In sum the chapter looks at the social, economic, market value and national security implications of these cybercrimes. The work also looks at the challenges or weaknesses faced by security agencies and governments in enforcing laws and regulations which makes them powerless in arresting the situation. The chapter further discusses the need for a collective approach in dealing with the cybercrime menace.

3.1 Internet and Cybercrime

The development of advanced computer crime in the 21st century is due to the use of the internet. The term internet can be defined as the gathering of millions of computers that provide a network of electronic connections between the computers.\(^1\) In 2011, at least 2.3 billion people, equivalent to more than one third of the world’s total population had access to the internet.\(^2\) The United Nations Office on Drugs and Crime (UNODC) report of 2013 stated that as at 2011, 62 per cent of all internet users were in developing countries. It further reported that some 45 per cent of the world’s internet users were below the age of 25 years.\(^3\) These statistics show the dependence of society on the internet. However the emergence of the internet has brought up a new twist known as the cybercrime. The weightiness of the emergence of cybercrime was more evident when the
Love Bug virus of 2000, damaged millions of Windows personal computers and was estimated to have cost computers worldwide $3 billion and $15 billion.\textsuperscript{4}

Organized crime groups are using the internet for major fraud and theft activities. There are trends indicating organized crime involvement in white collar crimes. As criminals move away from traditional methods of criminal activities, internet-based crime is becoming more prevalent. Internet-based fraud has earned criminals millions per year leading to loss of investors making it a productive area for such crimes. Cybercrime like other crimes has its different effects on the respective society and the world at large. By the observation of cybercrime and its phenomenon it is revealed that like other crimes it has affected negatively on the social, economies, market value and the national security setup of governments of states in the world. This chapter therefore seeks to outline the implication of cybercrime on International Relations.

### 3.2 Social Implications

As today’s consumer has become increasingly dependent on computers, networks and the information these are used to store and preserve, the risk of being subjected to cybercrime is high. Cybercrime has social implications on developed and developing countries. Despite the fact that cybercrime affects developed countries, it has a more rippling effect on developing and under developed countries that turn to have a high financial cost in handling cases with respect to investigations and prosecuting of fraudsters. These developing countries most often have to budget for the fighting of cybercrimes and ignore other important social projects for the advantage of the society. Nations and individuals put up with two main disadvantages of cybercrimes: one being target of cybercrime and secondly the allocation of national funds for its
prevention, ignoring any other national problem or program that might be of great importance to them.

One other social impact is described by Elgie McFayden Jr. in his paper “Implications of White collar crime”, that in some part of the world the youth perceive white collar crimes as a way of getting quick wealth for themselves and their families. During this period, they fail to recognize the implications of these acts. The emergence of online social networks, including Twitter and Face book, has also provided a ready supply of millions of prospective scam or fraud victims.

According to reports sponsored by the Better Business Bureau Online, over 80 per cent online shoppers cited security as a primary worry when conducting business over the internet. About 75 per cent of online shoppers stop an online transaction when asked for their credit card details. The view that the internet is an avenue for widespread credit card fraud and security hazards is growing. This has been a problem for e-commerce. Consumer perception can be just as powerful or damaging. Hence users concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of insecurity seriously hinders potential business.

### 3.3 Economic Implications

Information and Communication Technology (ICT) plays an important role in the economic aspects of every company and state. The advancement in ICTs helps improve a person’s access to information and provides a faster, cheaper and a more reliable means of communication. It has
further contributed to the improvement of products in terms of their design, reproduction and also their distribution process. The internet has helped economies of states to move to the international scene with their domestic products by helping to advertise their products.

Unfortunately, the internet is a double edge sword which has introduced cybercrimes that negatively affects the economy of a country. It affects the Gross Domestic Product (GDP), the Gross National Product (GNP), income levels, inflation levels and the economic structure of an economy. The financial costs to economies from cyber attacks consist of the loss of intellectual property, financial fraud, low productivity and damage to reputation of a business. The loss of revenue and low productivity, make up a large proportion of the reported cost of cyber attacks and viruses. Other businesses also face damages from financial fraud and theft of intellectual property over the internet. As the economy increases its reliance on the internet, it is exposed to all threats posed by cyber criminals. In modern times, stocks and bank transactions are performed by the use of the internet. Currently purchases of goods have moved from shops to the use of credit card. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy of the state.

According to a 2011 Norton report on cybercrime, over 74 million people in the United States were victims of cybercrime in 2010. The report further stated that these criminal acts resulted in $32 billion in direct financial losses. The subsequent 2012 Norton report on cybercrime also stated that the global price tag of consumer cybercrime has risen to US$110 billion annually. With the interdependence of the world’s economic system, the disruption in one region or country of the world will have ripple effects in other regions. Hence any disruption of these
Markets such as that in the United States could send shock waves to the other markets globally.\textsuperscript{10} The world through the attacks from worms, viruses, botnets and others has productivity at risk. Machines of factories could perform more leisurely; servers might be difficult to get to, networks might be blocked and so on.\textsuperscript{11} Such instances of attacks affect the productivity of the user, the organization, and the economy of a state. In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. This can also result in the loss of a considerable portion of e-commerce revenue generation among states.

\textbf{Table 3.1}

\begin{center}
\textbf{Global Statistics on Incidence of Cybercrime}
\end{center}

\begin{tabular}{|l|p{15cm}|}
\hline
\textbf{Hacking} & In 2008, Verizon Communication Inc. observed the compromise of over 180 million business records due to hacking. \\
\hline
\textbf{Malware} & Symantec Corporation, American global computer security software corporations detected a total of approximately 2.6 million different malware programs 60 per cent of which were detected in 2008. \\
\hline
\textbf{Malware Infection via legitimate sites web} & A 2007 study of 4.5 million web pages by Google found that one out of every ten websites contained malware. \\
\hline
\textbf{Botnets} & - McAfee estimates that nearly 40 million computers were recruited to botnets in the first three quarters of 2009.  \\
& - The internet society of Australia submitted that estimates of the number of bot computers range from five percent of all computers connected to the internet. (over 250 million) \\
\hline
\textbf{DDoS attacks} & Telstra Corporation Limited in Australia submitted that the size of the largest DDoS attacks increased a hundred folds between 2001 and 2007, from 0.4 gigabits per second to 40 gigabits per second. \\
\hline
\end{tabular}
Cybercrime industry

Verizon reports that 91 per cent of the data breaches it observed in 2008 were linked to organized criminal networks.

Phishing and Spam

- In the year 2008, Symantec noticed a 349.6 billion spam messages across the internet.
- Symantec claims that in 2008 approximately 90 per cent of spam was sent via botnets.
- The Anti-Phishing Working Group, an international consortium of organizations against phishing identified over 210 thousand unique phishing websites in the first half of 2009.


The financial losses caused by cybercrimes are overwhelming. Figure 3.1 illustrates the yearly dollar loss due to the activities of cyber attacks since 2001 to 2009. Between 2008 and 2009, financial losses caused by cybercrime doubled. In 2009 alone 560 USDs was lost through cybercrime activities. This figure as at then summed up the GDP of the three poorest countries in the world.
**Figure 3.1: Yearly Dollar Losses**

*Source: The 2009 Internet Crime Report by the Internet Crime Complaint Centre (IC3); a multi-agency task force for cybercrime cases.*

**Figure 3.2** further gives the recent trends that were reported to the FBI scams, on-delivery of goods or services and advanced fee fraud toppled the list.

![Bar chart showing yearly dollar losses](chart.png)

*Figure 3.2 was sourced from the 2009 Internet Crime Report by the Internet Crime Complaint Centre (IC3); a multi-agency task force for cybercrime cases.*
3.4 Implications on Market Value

The economic impact of security violation is of great importance to companies trying to decide where to establish their information security budget. The worry by these companies further has to do with how to engage insurance companies that provide cyber-risk policies.\textsuperscript{12} The issue of company information security heightened when a ruling in favour of Ingram Micro Company Inc. stated that “physical damage is not restricted to physical destruction or harm of a computer circuitry but includes loss of use and functionality.”\textsuperscript{13} This new and evolving perception of damage becomes even more important as many companies rely on information systems in general and the internet in particular to conduct their business. This pattern may force many insurance companies to have no choice than to pay compensation to businesses for damage due to hacker attacks and other security breaches.

As the definitions and description of security violation change, companies frequently re-examine their information security environment for threats.\textsuperscript{14} Recently, some insurance companies have created actuarial tables that they believe provide ways to determine losses from computer interruptions and hacker attacks that have an effect on companies and businesses. However, these estimates are questionable mostly due to the lack of historical data that are mostly unavailable due to the perceptions of society.\textsuperscript{15} Many believe that the rates for such plans are mostly set by guesswork. Industry experts cite the need for improved return on security investment studies that could be used by insurance companies to create “hacking insurance, with flexible rates based on the level of security employed in the organization and by the organization to justify investments in security prevention strategies.”\textsuperscript{16}
The size of a company plays an important role in the cost to be incurred when a comprehensive assessment of the required information security is done. Information security risk assessment provides a means for identifying threats to security and evaluating their severity. In information security, risk assessment addresses the questions of what is the impact of an information security breach and how much will it cost the organization. However, assessing the financial loss from a potential information security breach is a difficult step in the risk assessment process for the following reasons:

- Many organizations are hesitant to work out their financial losses due to security breaches.
- Lack of historical data due to unreported cases because companies are cautious to disclose cyber attacks on their information systems due to management mortification, fear of future attacks and fear of negative publicity from society. Companies are also wary of competitors utilizing these cyber attacks to gain competitive advantage.
- Furthermore, human beings by nature react negatively to the news that a company may have security breach in their system. Research suggests that public news of a cyber attack that is generally seen as bad for business will cause a drop in a company’s stock price.

3.5 National Security Implications

Cyber attacks, security of networks and the lack of safety for information create complex problems that reach into new areas for national security. Cybercrime poses a great threat to the national security of all countries. These cyber space crimes results in the loss of billions of dollars by companies and government institutions. Every day, almost 150,000 viruses and other malicious codes circulate through cyberspace, affecting 148,000 computers in cooperate and
government offices. In the USA, spanning for a year in 2009, the amount of information lost to cybercrime nearly doubled from US$ 265 million in 2008 to US$ 560 million according to a report by the Internet Crime Complaint Centre (IC3), which is supported by the US Federal Bureau of Investigation (FBI).

This study looks at one set of issues related to cyber terrorism and cyber attacks on critical infrastructure and institutions in a country and their implications for national security. According to the United States of America (U.S.A) Federal Bureau of Investigation, cyber terrorism is “any premeditated, politically stimulated attack against information, computer systems, computer programs and data which result in violence against non-combatant targets by sub-national groups or secret agents.” Cyber terrorism can further be explained as the use of computer network tools to shut down essential national structures such as energy, transportation and government businesses.

Unlike virus or computer attacks that result in denial of service, a cyber terrorist attack can be destructive, disruptive or exploitative. According to the U.S Commission of Critical Infrastructure Protection, probable cyber-terrorist targets include the banking industry, military installation, power plants, air traffic control centres and water system.

Cyber terrorism exits when “unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective or to cause grave harm or severe economic damage.”
The basis of cyber terrorism is that as nations and significant infrastructure become more reliant on computer networks for their operation, new weaknesses are created. A hostile nation or group could exploit these weaknesses that emerge in the systems to penetrate a poorly secured computer network and disrupt or even shut down critical functions. For the past few years some major potential cyber terrorist attacks have been noticed and it has already rung the alarm. From these incidents the world has come to the realization that terrorism has gone through a different era with advancement in technology and a new phase of modern terrorism. In March 2011, United States (US) officials announced that they were investigating plans by members of the hacking group ‘Anonymous’ to hack into the Marine Corps base in Quantico, Virginia. The group is a major protestor of the US government’s conduct against whistleblower Wiki Leaks. The reason the group gave for allegedly targeting the base was that one of the alleged informants to Wiki Leaks was imprisoned there.

Another report that shocked the world was on December 2009, when BBC reported that a US Drone had been hacked by Iraqi insurgents; the reported which read: “Iraq insurgents 'hack into video feeds from US drones”, further explained stating that:

Insurgents in Iraq have hacked into live video feeds from unmanned American drone aircraft, US media reports say. A senior Pentagon official is quoted by the Wall Street Journal as saying that although militants were able to view the video, there was no evidence that they were able to jam electronic signals from the aircraft or take control of them. The unnamed official said the US Defence Department had addressed the issue by working to encrypt all video feeds provided by drones in Iraq, Afghanistan and Pakistan.

The unmanned aerial vehicle (UVA) drones used by the United States Air Force is slightly controlled by trained pilots who are mostly a distance away from the UVA. The purpose of the drone is that, it is used for surveillance and monitoring. These drones have stashed in them two missiles which can be fired by using the same communication channel. In a similar incident
reported by the Centre for Strategic and International Studies (CSIS) in a report titled “Transnational Threats update,”

CSIS wrote:

The Pentagon has been forced to acknowledge a major security breach after the Wall Street Journal reported that militants battling U.S. forces in Iraq and Afghanistan have been intercepting videos transmitted between American drone and U.S. ground forces in the two theatres. Although the exact details have yet to emerge; defence officials told the Journal that captured Iraqis had been found to have “days and days and hours and hours of (footage)” from U.S. aircraft on their laptops.28

The Pentagon was forced to render inoperative up to 1,500 computers, as hackers further breached an email system at the office of the Secretary of Defence. Another attack on the US occurred in 2008 when the US military’s classified computer network was hacked by an unidentified intelligence agency which infected their system with a malicious code through a flash drive. Pentagon in its efforts to save the situation again disallowed the use of USB drives as at November 2008.29 In 2006, the networks of the US State Department were hacked by some unidentified persons who downloaded classified data. The Centre for Strategic and International Studies (CSIS) regarded this incident as a serious threat to the national security. According to CSIS,

If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards and spend the night carting off file cabinets it would be an act of war, but when it happens in cyberspace we barely notice.30

Canada has also been a victim of cyber attacks which targeted important infrastructure and government institutions. In January 2011, hackers infected computers in two Canadian government departments leaving many officials with no internet for almost two months. This attack crippled the government machinery causing confusion for more than two months.31 Another cyber terrorist attack was against Estonia and Georgia. The attack against these two countries was enormous. In April 27, 2007 Estonia became the target of Dos attack
that came to be known as the “Web War 1” (or WW1). This affected the country’s media houses, parliament, ministries and banking sectors bringing Estonia to a standstill.\textsuperscript{32} From 2008 to 2009, a connected cyber terrorism attack took place in Georgia during its war with Russia.\textsuperscript{33} In his effort to calm situations in Georgia, President Mikheil Saakashvili shifted the country’s website to the Tulip system, which is a US–based server, believed to be capable of fighting off cyber attacks.\textsuperscript{34}

Global summits have also become prime targets for cyber terrorism. Hackers in some occasions tampered with systems prior to summits. One of such attacks happened on March 2011 when the computer network at the European Union (EU) headquarters was attacked by hackers prior to an EU leader’s summit on Economic Reforms and Current Affairs, disrupting the organization of the event.\textsuperscript{35} This trend continued with an attack on the French Finance Sector in December 2010, where hackers broke into computer systems and stole sensitive information related to the G20 Summit which was held in France on February 2011.\textsuperscript{36} The criminals took control of nearly 150 computers at the French Finance Ministry and accessed many documents that had sensitive information on the G20 summit.\textsuperscript{37} It is evident that terrorists have employed the services of highly skilled hackers whose services tend to be cheaper, faster and untraceable when executing attacks using the internet.

### 3.6 Challenges of the Law Enforcement Regulations and the Need for Collective Security in the World

Many governments in the world are making strenuous efforts to enact policies and make necessary investments to fight cybercrimes. These policies are done to assure their citizenry of the state’s ability to protect their private lives in cyber space. The ability to enact laws and implement them is an effective way to fight against cybercrime and a necessary requirement to
support the persistent process of preventing the menace. Without creating the legal structure that enables law enforcement agencies to identify cyber criminals and prosecute them, it is almost impossible to stop cybercrime attacks. Legal frameworks and their implementation need to go hand in hand with technical approaches or protective measures in the prevention of cybercrime. Legal frameworks become important in areas where technology is not available, failed or avoided and bringing the need for laws to maintain cyber security.

Cyber threats have in recent time damaged national interests and caused the slow development in government institutions and individuals. It has gained a position as an important element of national security. To this effect law enforcers in countries are constantly making efforts to prevent and control cybercrimes. Beginning in the 1990s, many police departments had begun developing cybercrime units in an effort to combat internet crimes. There are also several statutes worldwide forbidding a wide range of online activities. In 2010, different laws were focusing on almost every known type of internet crime including hacking, password cracking, viruses, cyber fraud, cyber stalking, cyber bullying, cyber terrorism, theft of identity and online child pornography in the United States of America (USA) which has the highest rate of cybercrime in the world.

This section of the study addresses the challenges that are emerging in the world which seems generally ill equipped to address the issues of cybercrime. Despite the high rate of cybercrime in the United States and United Kingdom, they have been able to balance this out through implementing regulatory and technologically advanced measures to curb cybercrime. This study further mention the various laws put in place by some developed countries like the United States,
United Kingdom and Australia to curb cybercrime activities. Also, the section discusses the various anti-cybercrime legislation set up by some African countries that have been identified as having the highest rate of cybercrime. It looks at the current legislative efforts in the continent and a selective case study of key countries in Africa. Cameroon, Nigeria, Kenya and South Africa would be discussed.

3.7 Cybercrime in Africa

Africa as a continent has become a fertile ground for cyber criminals who ply their trade for reasons ranging from underdeveloped technology, high crime rate and archaic legislation. All the commonly done cybercrime activities in the other parts of the world mentioned in chapter two of this study are found on the African continent. Cybercrime, according to researchers is growing at a faster rate in Africa. Cyber security experts estimate that 80 per cent of PCs on the African continent are already infected with viruses and other malicious software.\(^{43}\) The introduction of broadband internet to Africa has also the likelihood to spell doom for the continent and has a high impact on the world. With this growth the internet world has become a small global village leading to easy penetration by cyber criminals from within Africa into any part of the world.\(^{44}\) Africa has become a hub to cyber criminals due to the lack of protection for user activities over the internet and what happens in cyber space in Africa should not only concern Africa but the entire “global village.”

3.8 Current legislation and legislative efforts on Cyber Crime in Africa

In this section, the focus is placed on specific countries representing the Africa continent which are recognized globally as being a hub for cyber criminals.
3.8.1 Nigeria

There is presently little law that is specific to cybercrime in Nigeria. This does not mean that Nigeria has abandoned the global quest in fighting cybercrime. Nigeria, ready to fight the menace has in placed other general laws related to cybercrime prosecution. Some of these laws are; the Nigerian Criminal Code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act, 2004 and the Advance Fee Fraud and other related Offences Act, 2006.  


The Criminal Code Act of 1990 criminalizes any type of stealing of funds in no matter the form the incident occurs. This is an offence punishable under the Act. Although cybercrime is not mentioned in the Act, it is recognized as a type of stealing done in cyber space punishable under the Chapter 38 of the Criminal Code Act, concerned with crimes committed when a person “obtains the property of another by false pretences or by fraud.” The exact provisions relating to cybercrime is in section 419 which states that “any person who by any false pretence and with intent to defraud, obtains from any other person to deliver to any person anything capable of being stolen, is guilty of an offence and is accountable to imprisonment for three years”.

- The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act, 2004, provides the legal framework for the establishment of the commission. Some of the major responsibilities of the Commission according to the part 2 of the Act include:

1. The investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfer, future market fraud, fraudulent
encashment of open to discussion instruments, computer credit card fraud and agreement scam.\textsuperscript{48}

2. The Commission is further responsible for the management and enforcement of all laws against economic and financial crimes and the enforcement functions presented on any other person or authority in the performance of their actions.\textsuperscript{49}

- **Advance Fee Fraud and Related Offences Act, 2006**

According to Part IV, section 20 of the Advance Fee Fraud Act, 2006, “false pretence means a representation, whether conscious or reckless, made by word, in writing or by conduct of a matter of fact or law either past or present, which representation is false in fact or law and which the person making it knows to be false or does not believe to be true.”\textsuperscript{50} Also a definition from Chapter 34, Section 383(1) of the Criminal Code of Nigeria states that stealing is when “an individual fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to have stolen that thing.”\textsuperscript{51} These two, false pretence and stealing are constantly in the domain of cybercrime activities.

There are several related bills before the Nigerian legislature and the National Assembly, none of which have been passed into law.\textsuperscript{52} Some of these bills are; the Cyber Security and Critical Infrastructure bill, the Privacy bill, the Electronic Commerce bill, Computer Security Protection bill, and the Evidence Act Amendment bill among others.\textsuperscript{53} These bills being related to cyber security are yet to be passed into law. Nigeria as a country can find itself in a disadvantaged position especially with recent expansion in its broadband networks with the introduction of two
submarine cables of Main One and Glo1 in 2010. The country’s inability to pass bills into law is likely to cement its status as the third country with the highest rate of cybercrime in the world after the US and the UK.\textsuperscript{54}

3.8.2 South Africa

South Africa is one of the advanced countries on the continent. Its advancement is spread across to all aspects of their development especially technological advancement. This has seen South Africa having to deal with a fast increase in cybercrime. It passed the Electronic Communication and Transactions Act (ECT), No. 25 of 2002 referred to as the ECT Act and which was assented to on 31 July 2002.\textsuperscript{55} The main objective of the legislation is to “provide for the facilitation and regulation of electronic communications and transactions. It further seeks to ensure the universal assessment to electronic communication and transaction.”\textsuperscript{56}

The Act seeks to criminalize actions related to the illegal access and unauthorized modification of information as well as the possession and distribution of hardware devices and software programs that facilitate an offender’s action of cybercrime. The ECT Act sufficiently deals with “jurisdiction, the acceptability of data messages, the admissibility of electronic signatures, as well as the regulation of cryptography.”\textsuperscript{57} The South African law enforcers in fighting cybercrime have come up with cyber inspectors who are tasked to monitor internet activities and further ensure that the provisions of the ECT Act are complied with.\textsuperscript{58} Cybercrimes prohibited under the ECT Act is stated under chapter XII (13) of the Act. These activities are grouped into four categories: those involving unlawful access to data, interception and interference with data and computer related extortion, deception and forgery.\textsuperscript{59}
The ECT Act which is the main law in South Africa in fighting against cybercrime has some specific provision that specifically speaks to the issues of cyber activities prevalent in the world today. Section 86(1) of the ECT criminalizes all forms of hacking, with section 88(1) of the Act also criminalizing any attempt by criminals to gain unauthorized access. The country in its attempt to fight cybercrime on the global scale has formed an alliance with the European Cybercrime Treaty, which outlaws cybercrime and encourages treaty member states to make laws criminalizing cybercrime. Other laws such as the Electronic Communications Security Act (Act 68 of 2002) and the State Information Technology Agency Act (Act 88 of 1998) are used South Africa to curb to global cyber menace.

3.8.3 Kenya

Kenya enacted the Kenya Communications Amendment Act, 2009, which recognizes cybercrime and sets out legal protection for government and businesses. The Act defines “cybercrime as offences against the information technology infrastructure, from unauthorized access to and interpretation of computer services, modification of computer material, data and unauthorized change of mobile telephone equipment”. The Act further gives the communications commission of Kenya the power to protect the right to privacy of all persons. It is worthy to note that section 83U of the legislation of the Act prohibits unlawful access to computer system. The Act, among other things also set out to; make regulatory, advisory and dispute resolution bodies to support the implementation of the national ICT policies and provide for the licensing of country code top-level domain administrator and provides for electronic transactions-related offences, including cybercrime and reprogramming mobile phones. This law governs and
regulates the telecommunications sector in the country. The Minister of Information in Kenya stating the views of the government stated that “as the reliance on ICT increases, recognizing and monitoring of risks involved in their use has become an important but challenging task.”

As a technical strategy to fight cybercrime, Kenya has developed a national Computer Emergency Response Team (CERT) and is part of the International Telecommunication Union (ITU) Global Resource Centre (GRC). The objective of the country is to support ITU member states in fighting against with cybercrime through the establishment of national CERTs. The Communications Commission of Kenya has developed a framework that facilitates the set up of Certification Authorities for the issuance of digital certificate to protect online transactions in the country and help encourage e-commerce. Other technical strategies by the Kenyan authorities in dealing with the cybercrime menace include, the Domain Name System (DNSSEC) and the Internet Protocol version 6 (IPV6), which authorities believe could provide end-to-end internet protocol security. At the East Africa level, Kenya chairs the cyber security Taskforce whose main objective is to facilitate the development of national CERTs in the East African region.

### 3.8.4 Cameroon

Despite the fast growing nature of cybercrime activities in Cameroon, not much legislation has been put in place to combat cybercrime. Cameroon comes in second after Nigeria as the country with the most rampant cybercrime activities. A report by the McAfee cyber security firm states Cameroon “as the world’s riskiest destination for internet surfers with more than third of websites hosted in Cameroon being suspicious.” The country in wanting to limit the situation has in response to these reports, through its Ministry of Post and Telecommunications and the
National Agency for Information and Communication Technologies advanced a bill to parliament that allows them to set up a cyber police force. The bill is also expected to help law enforcement agencies with the tussle of defining major crimes and determining legal practices to help fight cybercrime.

3.9 Cybercrime legislation and cooperative alliances in the United States, United Kingdom and Australia

Having examined the anti cybercrime legislative framework in Africa, I now look at the position in countries with advanced technology such as the United States, the United Kingdom Australia and China facing cyber attacks.

3.9.1 United States

The United States of America (USA) Defence Secretary Robert Gates has stated that in his view after wars have been fought on lands, the 21st century should expect to fight current wars in the air and space cyberspace.68 The USA government has focused its interest on protecting its digital infrastructure; pronouncing it a “strategic national assets”.69 The US a highly developed technologically state, has one of the most reputable legislative and cooperative frameworks on cybercrime. These include:

- A federal criminal code related to computer invasion that include a number of federal criminal statutes relating to computer invasion.70
- Sentencing guiding principles relating to computer intrusions.71
- The USA further ratified the Cybercrime Convention in August 2006 and entered it into force on 1 January, 2007.
In the USA there are more than 40 federal statutes that govern the prosecution of computer-related crimes, as well as various state statutes. There are also several key players in the field helping in the fight against cybercrime. These include:

- The Department of Justice
- The FBI
- The Computer Emergency Response Team (CERT)
- Computer Crime Research Centre
- Centre for Democracy and Technology
- The United States Secret Service
- The US Cyber Command

The USA has entered into alliances with several governments and organizations through the efforts of the US-CERT. The mission of the US-CERT is to improve the nation’s cyber security stance, coordinate cyber information sharing and positively manage cyber risks collaborations with other national CERTs.

### 3.9.2 United Kingdom

The legislative responses to cybercrime in the United Kingdom include:

- The Computer Misuse Act of 1990, which was the first piece of UK legislation designed to specifically address computer abuse. The Act came into force as a major answer to already existing worries of the lack of effect cybercrime legislation. The Computer Misuse Act, 1990 is also an Act that makes provisions for securing computer materials from the activities of hackers. For connection purposes the Act has set out three computer
misuse offences; namely “unauthorized access to computer materials, unauthorized access with intent to commit or facilitate the commission of further offences and the unauthorized modification of computer materials.”

The maximum prison sentences stated by the Act for each offence were six months, five years and five years respectively.

- The UK also introduced the Privacy and Electronic Regulations (EC Directive) 2003, Act which tries to address the problem of spam activities. According to the Act, Regulations 22(1) admonishes all companies seek for the permission of clients or an individual’s before sending emails or SMS messages to them. On the subject of emails, the law states that “a person shall neither transmit, nor prompt the transmission of, unwanted communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of the sender”.

- Another cybercrime law adopted by the UK government is the European Convention on Cybercrime, designed to provide a common international framework for dealing with cybercrime, which was introduced by the European Union Committee of Ministers of the Council of Europe in November, 2001.

The treaty is wide-ranged and covers all aspects of cybercrime, including illicit access, unlawful interception of data, data intrusion, system interference, abuse of devices, computer-related sham, computer related fraud, crimes related to child pornography and offences related to violation of copyright and related rights. This treaty is also designed to provide a common law
enforcement framework for dealing with cyber criminals and to foster the sharing of information among all signatories. 75

The UK government in its efforts to enforce these laws have in place some key players such as the Serious and Organized Crime Agency (SOCA) set up a non-governmental public body of the UK government which fights crimes. Its major task is to prevent major organized crimes including cybercrime done through the internet. Also in place are the Child Exploitation and Online Protection Centre (CEOP) 76 and the Communications Electronics Security Group (CESG). 77 These two agencies are responsible for securing the communications and information systems of the United Kingdom. It has liaised with law enforcement agencies in Australia, Canada, The United States of America and INTERPOL.

3.9.3 Australia

Australia is one of the front runners in the fight against cybercrime with a record of success. Apart from its cybercrime legislation, it is consistently involved in forming alliances with other countries to improve the efficiency in combating cybercrime on a global scale. Australia has been a participant in a number of Organizations for Economic Cooperation and Development (OECD) and International fora dealing with e-commerce issues. For example, Australia has been an active participant in the World Intellectual Property Organization’s (WIPO) programme on electronic commerce and domain names, including implementation of standards consistent with WIPO copyright Treaty, WIPO Performance and Phonograms Treaty and WIPO programme on Database Treaty. 78 Australia’s new cybercrime law which came into being on 1 March 2013 establishes the legislative framework for Australia’s accession to the Council of Europe’s
Convention on cybercrime. The essence of the new cybercrime law is to empower Australia’s law enforcement and intelligence agencies to compel carriers to preserve the communication records of persons suspected to cyber-based crimes. The new law also expands the common wealth cybercrime offences and facilitates international cooperation between state parties to the convention through the cross-border sharing of communication records. Other related cybercrime legislations were the Electronics Transactions Act of 1998, the Spam Act of 2003 and the Australian CERT.

3.9.4 China

Although China has been regarded as the largest source of targeted hacking attacks, the country is also at the receiving end of attacks. In 2009, nearly 200 Chinese government websites were attacked on a daily basis. This encouraged the country to incorporated computer crimes into its criminal law legislation. The Criminal Law of the People’s Republic of China makes mention of articles 285 and 286 which states hacking as a crime which violates the laws of China. China further on 28, December, 2000 adopted the “Decision of the Standing Committee of the National People’s Congress on the preserving computer network security” which sought to ensure “operational security of computer networks.”

The country has collaborated with the United Nations, the Association of Southeast Asian Nations (ASEAN) and other international communities and governments in efforts to fight cybercrime. In 2009, China signed the ASEAN-China Coordination Framework for Network and Information Security Emergency Responses. In a further effort to protect confidential information, China in May, 2010 tightened its Guarding Status Secrets Law by holding internet
and mobile phone operators responsible for customers who try to leak confidential information.\textsuperscript{84}

The Chinese public security organ also participated in the Interpol Asia-South Pacific Working Party on IT crime, the China-US joint liaison group and other forms of International cooperation and has conducted bilateral and multilateral meetings successfully with countries such as the US, UK, Germany, Italy and the Hong Kong.\textsuperscript{85}

\section*{3.10 Challenges Faced by Countries in Legislation and Regulating on Cybercrime}

One of the main challenges faced by nations in legislating on cybercrime is the lack of uniformity and consistency in the laws in this field. This is also marred by a slow law making process and the levels of ratification of parliaments in nations after the signing of treaties have been done. While there is active focus by governments in fighting and preventing cyber criminals from damaging the social, economies, market value and security of societies, the very nature of cyber space poses a number of challenges to the implementation of cyber regulations in any country. The need for uniformity is important to foster more effective cooperative alliances within the world.

Within cyber space it is often difficult to determine political borders and culprits since most cyber offenders can be described as “faceless”. Cyber criminal communities and their techniques are continuously evolving, making it more challenging for governments and companies to keep up with their ever-changing tactics. Rob Wainwright, Director of EUROPOL, states that criminal investigations of cybercrimes are difficult by nature because the criminal activity itself is borderless by nature. He added that tracing cyber criminals poses a challenge.\textsuperscript{86}
A major threat that could affect the fight against cybercrime is the growth of secretive economies, which many cyber criminals see as a lucrative venture. The desire to make huge amounts of money attracts computer experts in many countries. In the cyber world, the hackers and organized crime groups operate by selling classified stolen intelligence. According to the KPMG report in 2011 on cybercrime, research shows that criminals are selling bank account information for US $10-125, credit card data for up to US $30 per card and email account data for up to US $12. Often, the acquired data is used in dishonest online purchases and in exchange for other fiscal transactions. The intractability of the origin of these transactions poses a major challenge to government agencies in their efforts to fight crimes of this nature.

New and advanced technologies are being developed by culprits to aid them in the perpetration of cybercrime. For example, there are obfuscation programs available to help cyber criminals hide their identities making it difficult to trace the source of these attacks. This challenge is further worsened by the lack of the necessary funding needed to equip law enforcement or relevant agencies in detecting quickly the origin of cyber attacks. Adequate funding coupled with the right training is a likely formula for success and a step in the right direction.

According to Ronald Kenneth Noble, Secretary General of INTERPOL, for a cyber attack to be described as efficient it does not necessary require a militia but rather it takes just one individual. However, he complained about the severe shortage of skills and expertise to fight this type of crime not only at Interpol, but also in law enforcement agencies in every country. It is unfortunate also to realize that in most countries, most trained or skilled people in technologies are recruited by the private sectors, as it offers higher remunerations compared to government
institutions. In Australia for instance, majority of the cybercrime incidents, particularly trivial incidents remain unsolved or are not looked into due to the lack of Forensic skills and expertise.\(^9\)

Another major challenge that hinders the fight against cybercrime and the enforcement of laws is related to the level of interaction of different organizations and institutions at both the national level and international co-operation on the global level. The successful investigation of cybercrime on a national level can in general only be carried out if the victims or the organizations involved in the fight against cybercrime and other corporate bodies work together more closely. Most victims at the national level do not report cyber attack cases because they believe it is an undue disadvantage on its consumer trust of its services.

Cybercrime is truly an international phenomenon. Due to the structure of the network, an offender can act from any place in the world and attack victims worldwide. The inability of national law enforcement agencies to investigate these crimes that have an international dimension is limited due to the principle of national sovereignty which restricts the authority to carry out investigation in foreign territories.

### 3.11 Collective Security in the Fight against Cyber Criminals

Global cooperation efforts in the world in ensuring peace and security will yield substantial results in a stable and secure environment. It is for this reason that cybercrime, a threat to global security and stability should be addressed. The fight against organized cyber attacks requires nations of the world and their respective law enforcement agencies to work much more closely
together, both bilaterally and multilaterally. Cybercrime is an international phenomenon and so needs a transnational solution.

International organizations such as European Police office (Europol), the North Atlantic Treaty Organization (NATO) and the International Telecommunication Union (ITU) have made significant efforts to zero in on cyber security. For instance, in June 2010, EUROPOL created the “European Union Cybercrime Taskforce”. The taskforce includes expert groups of representatives from Europol, Eurojust; the European Union (EU) judicial cooperation body and the European Commission. EUROPOL has in many ways provided the European Union (EU) members with investigative and analytical support on cybercrime and facilitates cross-border cooperation and information switch over. At the North Atlantic Treaty Organization (NATO) summit in November 2010, the EU, NATO and the United States approved plans for a coordinated approach to tackle cybercrime in member states. It was decided at the summit that by 2013, an EU cybercrime centre, currently in place will be established to coordinate cooperation between member states. The European Commission (EC) created a network of Computer Emergency Response Teams (CERTs) in most of its member states. This is to help the EC respond or react in case of any computer-related emergencies such as cyber attacks.

The African continent also realizing the need for cooperation efforts in ensuring peace and stability in cyber space have made coordinated efforts within the continent to form cross border alliances in the fight against cybercrime. Examples of these involve efforts by regional bodies such as the Economic Community of West African states (ECOWAS), East African Community (EAC), Southern African Development Community (SADC) and the Economic and Monetary
Community of Central Africa (CEMAC) to harmonize laws, organize law enforcement officers and form partnerships with international organizations. There are some mutual assistance and multi-stakeholder approach involving the government, manufacturing sectors and civil society organizations by some East African countries in their efforts to combat cybercrime. A cyber security management task force chaired by Kenya has been coordinating activities aimed at rooting out cybercrime in the five East African countries. This taskforce is responsible for ensuring cyber security at legal, policy and regulatory levels. Countries from the East African region namely, Uganda, Kenya, Tanzania, Rwanda and Burundi to set up computer Emergency Response Teams (CERTs) just like that of the EU member countries to fight cybercrime is under way as countries concerned seek to involve the International Telecommunications Union (ITU) help.

Due to the collective collaborative efforts by these countries that are at different stages of developing their internet laws, the laws will be uniform across board with just few in-country peculiarities sticking out. The first West African cybercrime summit was convened on 30th November, 2011 to 2nd December, 2011 in the Nigerian capital, Abuja. The summit, organized by the Economic and Financial Crime Commission (EFCC), the ECOWAS and Microsoft focused on the theme “The Fight Against Cybercrime: Towards Innovative and Sustainable Economic Development”. Members from different continents around the world considered local and international cybercrime strategies and policies with a view to strengthen international cooperation and developing a regional road map that tackles cybercrime and foster economic growth.
Over 450 people were in attendance from across the world with Togo, Guinea, Guinea Bissau, Gambia, Ghana, Senegal, and Ivory Coast, Niger, Austria, United Arab Emirates (UAE), Tunisia and Nigeria. Various international and regional organizations such as the UNODC, Council of Europe (CoE), Interpol, US Federal Bureau of Investigation (FBI), the US Federal Trade Commission, US Department of Homeland Security, ECOWAS, EU and Franco-Polish (Francopol) were all present at the summit. The summit among other issues discussed ways on how best to strengthen trust by developing partnerships among various stakeholders at the national and international levels. These collective efforts have been made internationally to help in the fight against cybercrime. However, the cyber problem does not seem to arouse a sense of urgency in the African continent as it does in the developed countries.

Although cybercrime activities on the African continent may seem insignificant, in global terms it threatens the world’s development efforts. These collective efforts of managing cybercrime should further be directed also to the development of more collective law enforcement agencies such as INTERPOL. Here countries would have to have a fine balance between national interest and global interest in handling cybercrime cases. Member States need to further learn to give up their sovereignty due to the transmittable nature of cybercrime in the world. A threat to the survival of one State becomes a threat to all in the global world when it comes to cyber activities. Anything short of these will not address the increasing trends in cybercrime activities and the individual, national and global security of the world could be at risk.
ENDNOTES

3. Ibid., p. 1.
8. Ibid.
9. Ibid.
11. Ibid.
25. Ibid., p. 8.
29. Ibid.
32. KPMG International Cooperative., p. 9.
33. Ibid., p. 9.
34. Ibid., p. 9.
35. Ibid., p. 9.
36. Ibid., p. 9.
37 ibid p., 9.
39 ibid p., 140.
40 Ibid.
42 Ibid., p. 160.
45 Ewelukwa, N., This Day Newspaper, Nigeria, March 31, 2011.
47 Ibid.
48 The Economic and Financial Crime Commission Act, 2004, Part II section 7(2)
49 ibid.
50 Advanced Fee Fraud and Related Offences Act, 2006, Part IV, Section (20).
53 Ibid.
54 Ibid.
55 The Electronic Communications and Transactions Act (ECT), Act No. 25, 2002.
56 Ibid
57 The Electronic Communications and Transaction Acts, Part 1, 2 and Chapters V and XIV of the Act respectively.
58 Ibid, (Interpretation, Object and Application) Chapter 1(d).
59 Ibid, Chapter XII.
60 Ibid Section 86(1) and 88(1) respectively.
61 Wada F & Odulaja G.O Vol. 4.No. 3.
62 Ibid.
63 Kenya ICT Action Network, Women and cybercrime in Kenya: The dark side of ICTs, Working document V1
64 Kenya Communications Amendment Act, 2009.
72 United Kingdom Computer Misuse Act, 1990, Chapter 18 (1).
74 Ibid.
75 Ibid.
76 http://www.ceop.police.uk.
80 Ibid.


85 The internet in China, Xinhuanet, op.cit.


87 Cybercrime as a business, The digital underground economy, EUROPOL, January 6, 2011.

88 ibid.

89 Is the hiding of intended meaning in communication, making communication confusing, willfully ambiguous or harder to interpret. It has appeared in print at least as early as 1959 when it was used as a section heading in a NASA document.


92 KPMG International report., p. 12.

93 ibid., p. 12.

94 KPMG International Cooperatives op.cit.

95 Oluwabukola A., ‘Catching up with the rest of the world, the legal framework of cybercrime in Africa’, p.13.

96 ibid., p. 13.


98 ibid. P. 100.

99 ibid. P. 100.
CHAPTER FOUR

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

4.0. Summary of Findings

The study focused on how cybercrime threatens global security and hamper international relations. It was guided by the hypothesis that the emergence of globalization has brought advancement in technology but a further increase in sophisticated cybercrimes which threaten individual, national, global security and the overall drive towards development. The study establishes that, cybercrime with the help of technology and the internet assumed complex and sophisticated trends. Cybercrime has evolved before and after the emergence of the internet. The first stage before the internet was when mainframe computers were used to execute crimes in the 1960s which was referred to as computer crimes. However the name cybercrime came into being when the internet emerged. The networking of computers helped criminals to operate without being at the crime scene. This period witnessed the spread of software and malicious computer viruses. This period also saw an increase in internet users and an urgent desire by the youth to acquire money through internet scams and fraud.

In meeting the objectives of the study, I examined the international implications of cybercrime, one of the major threats of security. The national security of a country is threatened by cybercrime activities. According to the KPMG report on cybercrime, everyday just about 150,000 viruses and other malicious codes circulate through cyberspace, affecting 148,000 computers in cooperate and government offices. These malicious viruses mostly caused damage
to critical infrastructure and institutions in a country and caused national security implications. This many scholars referred to us cyber-terrorism.

Cybercrime is a crime that goes beyond boundaries and possesses the ability to have huge economic impact on victims. The financial costs to economies from cyber-attacks are enormous. In the United States alone over 74 million people were victims of cyber-attacks in 2010. These attacks further caused a loss of $32 billion in direct financial losses. With the interdependence of the world economic system, the crumpling of a market such as that of the US could affect other markets globally.

The study further established some form of cooperation among countries since cybercrimes committed in one country often involves several nationalities and the impact is felt in the whole world. This situation makes it important for cybercrime activities in the world to be tackled collectively for the benefit of all. However, collective security among nations to a large extent borders on the principle of sovereignty. It requires nations to submit to the larger goal of global security setting aside its own national security. A state in dealing with cybercrime attacks will for instance have to take a decision on how much of its national budget should be allocated to national security and what portion will go to cater for global security. As established by this study, where cybercrime is concerned there is no borders. Criminals of cyber attacks do not consider borders; they see it as non-existent. It is important to also note that in dealing with cybercrime, sovereignty and the national interest should not be a standing block. Furthermore, due to the technological advancement and the emergence of the internet in the era of globalization, it will be difficult for one country to fight cybercrime within its borders. It is for
this reason that it needs the collaboration of other nations. A global cooperation effort in tackling cybercrime is of great importance to ensure peace and security. Cybercrime is an international phenomenon which needs a transnational solution.

The fight against organized cyber attacks requires nations of the world and their respective law enforcement agencies to work much more closely. However it is evident that law enforcement agencies are faced with several weaknesses and challenges. With countries having differences in legal systems, definition of cybercrime and the state-to-state perception of cybercrime, it makes cooperation not too smooth. The cybercrime situation if not dealt with systematically will worsen the already existing economic social, market value and national security problem as a result of cyber attacks. It will further wear down any progress that has been made in the world and hinder what is yet to be achieved. No country acting alone will succeed in countering the threat posed by cybercrime. All countries will have to put their resources together and come up with practical means of achieving this goal for the generations to come. The study by the end of the chapter three, affirms the hypothesis of how the emergence globalization has brought advancement in technology but a further increase in sophisticated cybercrimes which threatens individual, national and global security and the overall drive towards international development.

4.1 Conclusion

Cybercrime transcends beyond borders and possesses the ability to cause negative implications for the world without any caution. It is the fastest growing crime in the world due to the fact that it is global in nature. This phenomenon therefore calls for a collective approach by all to eradicate. It further calls for urgent education of the masses, starting from teenagers, the business
community, government officials, enforcement officers and many others on the implications of cybercrime and how to prevent and prosecute criminals. On the part of the governments, there is the need for constant investments in technology and innovation in the fight against cybercrime.

4.2 Recommendations

From the above discussion, the following recommendations are therefore made here for considerations:

- Despite the fact that there is no unique established definition for what cybercrime entails, cybercrime activities cannot be avoided by the international community. There is the need for the creation of a common platform to address the issue of cyber security. This is needed since the cybercrime phenomena have come to stay. The menace cannot be fought by an individual country. There must therefore be cooperative efforts to deal with cyber threats both at the national and also the global level. There must be the existence of bilateral and multilateral mechanisms to assist law enforcement agencies with the requisite advantages to prosecute and overcome all jurisdictional boundaries that may come up in the fight against cyber criminal activities. With the necessary cooperation, nations can be assured of the maximum assistance in the conduct of international investigations to bring accused persons to trial. Swift extradition processes of culprits should be encouraged with the participation of international organizations such as INTERPOL.

- INTERPOL as an internationally recognized crime fighting body needs to enhance its knowledge in computerization and also endeavour to follow the modern trend in
telecommunication. This effort by the organization is sure to help individuals; governments and other private cooperatives interact with each other more rapidly and on a secured system. INTERPOL should maintain an intelligence database, which can be accessed by other law enforcement agencies anywhere in the world. The organization must also be ready to assist both developed and developing countries with the necessary fighting tools against cyber criminals.

• The international community may have to revisit the issue of sovereignty since this has become a major standing block in the fight against cybercrime. There is the need for a global convention on the gathering of evidence in criminal cases. States must be prepared to extradite or prosecute persons who commit cybercrimes. It is important for all states to make readily available all form of evidence for the prosecution of offenders in the courts of other states without having to pass through the unnecessary red tape. Law enforcement agents in all countries should be able to interact with each other effectively.

• Before cybercrime can be effectively addressed globally, there is the need for consorted efforts on the part of the private, public and legal entities to better understand the global implications of their actions. There should be an institution or entity responsible for the detection, prevention and prosecution of cyber criminals in each region of the world. Cyber criminals have become sophisticated, technologically advanced, well-trained and organized. They have most importantly cost governments and private organizations hundreds of billions with their activities. Their actions if left unattended to could have adverse financial impact worldwide.
• The United Nations as an international organization that seeks to promote international security and socio-economic growth must be willing to support the actions of governments willing to detect, deter and prosecute offenders.

• Governments around the world in trying to fight against cybercrime should make the necessary efforts at synchronizing their legal systems to help overcome some legal hurdles, while regulating effectively their criminal justice systems. As such governments should examine and strengthen their law enforcement capabilities to deal with cybercrime. Training and refresher courses in technological studies for law enforcement officials should feature prominently in the drive towards effective law enforcement in the world. Individual nations should increase their political and financial commitments to combat crime. With these financial adjustments, law enforcement agents can be motivated with the necessary logistics and materials for their work. The cost of managing the effects of cyber attacks is huge and requires more of a prevention attitude by all countries.

• An internationally acclaimed facility where victims can report cases of cyber-attacks should be established. The global public should be educated on what computer crimes are and how best they can prevent or minimize the challenges. The police in individual countries needs to further build the maximum trust and confidence in their population by using the media and vice versa so that more incidents of cyber attacks can be reported without fear. Informant, sources and agents should be infiltrated in every facet of public
life. The people must be rewarded in order to maintain their loyalty and confidence in law enforcement agencies. Civil society groups should be encouraged to assist governments in sensitizing the public on the effects of cybercrime. Religious groups, professional bodies and non-governmental organizations should all take up the fight against cybercrime.

- Although a number of countries have enacted cyber laws, most of them are out moulded. These countries should have their legislations amended to keep up with the emerging cyberspace risk, as criminals are coming up with new technological avenues to evade the law and process of prosecution.
ENDNOTE

2 KPMG International Cooperative., p.6.
3 Ibid p. 6.
Bibliography

A. Books

Brenner W. Susan, Cybercrime: Criminal Threats from Cyber Space. (Santa Barbara, California: Greenwood Publishing Group 2010).


B. Journal Articles


C. Reports/Documents/Papers

Advance Fee Fraud and other related offences Act, 2006 (1). Laws of the Federation of Nigeria.


The Electronic Communication and Transaction Act (ECT), No. 25, 2002.


Advanced Fee Fraud and Related Offences Act, 2006.


Dorothy Denning ‘Activism, Hackism, and Cyber terrorism: The Internet as a tool for Influencing Foreign Policy’ in John Aquilla and David Ronfeldt, (eds.), Networks and Net wars, (Rand Corporation, 2001).


Tushabe F. and Baryamureeba V. ‘Implications of cybercrime on Socio-Economic Development’, Department of Computer Science, Makerere University, 2010.


Hacquebord F.and C Lu, Rogue Domain Name System Servers, Trend Labs Malware.

University of Science and Technology, Department of Computer and Information Science, 2010.


Mitnick Kevin’s, history is taken from these sources, cyber punks, Hafner Katie and Markoff John and Cyber crime, Brenner, Susan W. as quoted by Khadam, Nadia’s; Insight to Cybercrime.


**D. Internet Sources**


Cyberspace Law and Policy Centre(CLPC), submission 62,p.3 from [http://www.cyberlawcentre.org/index.html](http://www.cyberlawcentre.org/index.html).


www.starstandard.org/guidelines/DIG2012v1/ch11s03.html accessed on 10th June 2013.

www1.villanova.edu/villanova/publicsafety/crime/recognizing_and_avoiding_email_s.html

E. Newspaper

Ewelukwa, N., This Day Newspaper, Nigeria, March 31, 2011.