

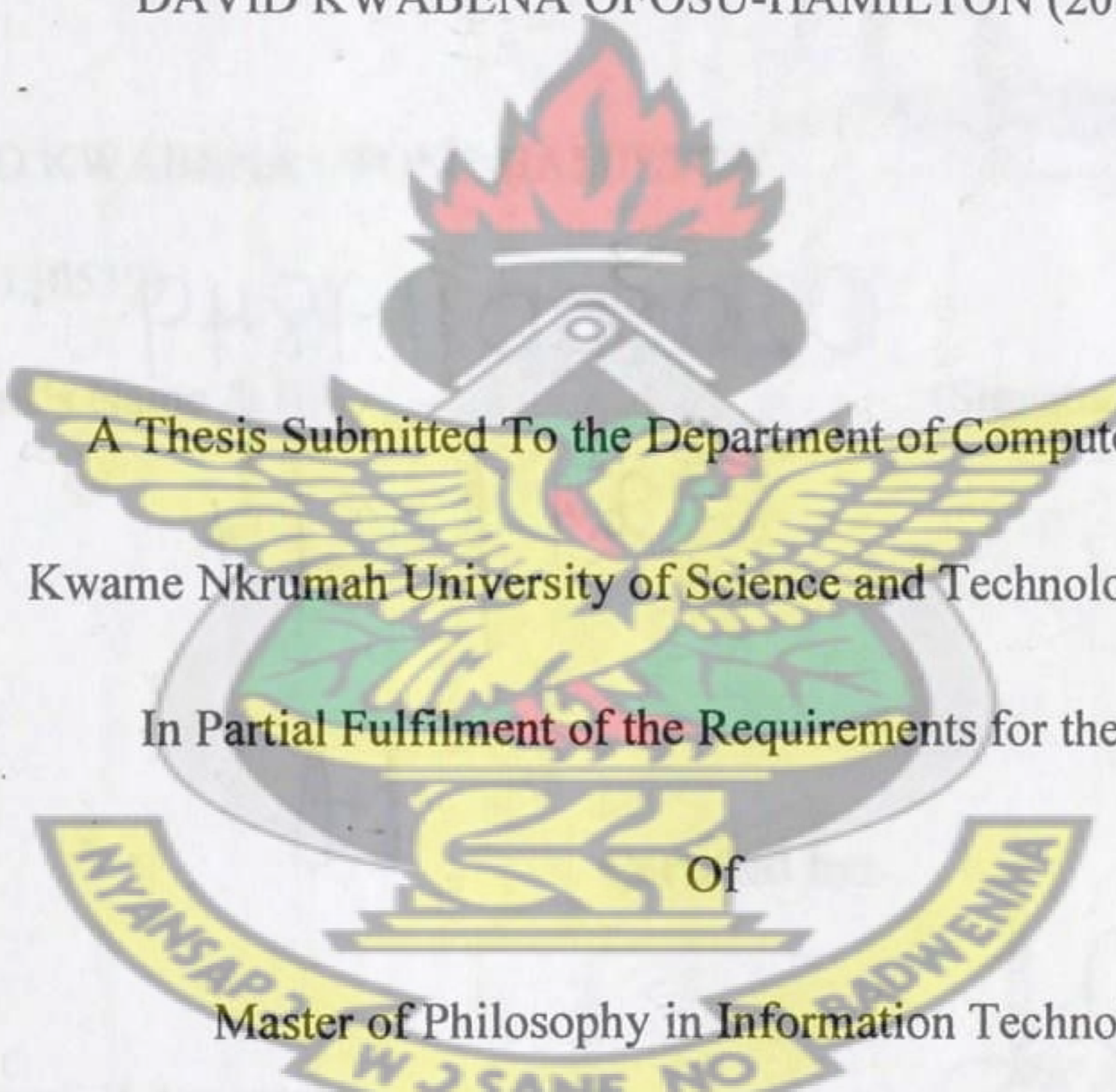
DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS) AS THREAT

VECTORS TO GHANA'S ECONOMIC INFRASTRUCTURE

(CASE OF GHANA'S EMERGING ECONOMY VIS-À-VIS NETWORK
INFRASTRUCTURE)

BY
KNUST

DAVID KWABENA OFOSU-HAMILTON (20130539)



A Thesis Submitted To the Department of Computer Science,
Kwame Nkrumah University of Science and Technology (KNUST)

In Partial Fulfilment of the Requirements for the Degree

Of

Master of Philosophy in Information Technology

COMPUTER SCIENCE DEPARTMENT

COLLEGE OF SCIENCE

February 2013

DECLARATION

I do hereby declare that this submission is my own work towards the MPhil (Information Technology) and that, to the best of my knowledge, it contains no material previously published by another person nor material which has been accepted for the award of any other degree of the University, except where due acknowledgement has been made in the text.

KNUST

DAVID KWABENA OFOSU-HAMILTON

(PG20130539)

(Student's Name & ID)

 16/5/13

(Signature)

(Date)



Certified by:

Mr. Dominic Asamoah

(Major Supervisor)

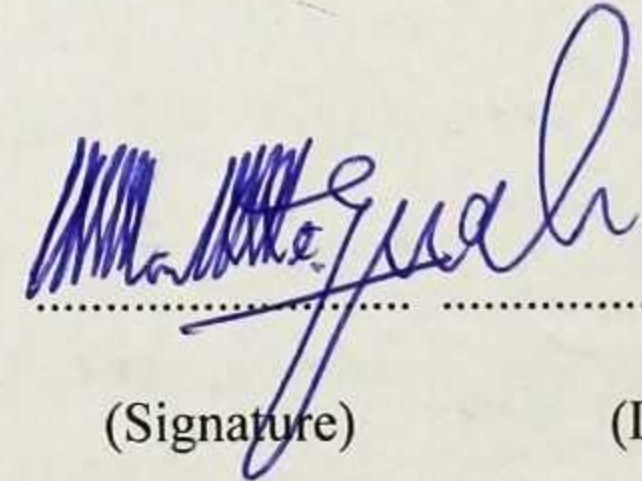
 22/02/13

(Signature)

(Date)

Dr. B. H Acquah

(Head of Department)

 26/5/13

(Signature)

(Date)

DEDICATION

This work is dedicated to my mother, Charity Ofosu, for all her struggle and toil in bringing me to this level.

I also dedicate it to my lovely Wife, Elsie Ofosu-Hamilton for the push to conclude this thesis despite the challenges and Mr Dominic Asamoah for the support, patience and encouragement in my eye opening academic pursuit in MPHIL.



ACKNOWLEDGEMENTS

My ultimate gratitude goes to the Almighty God for His mercies, kindness and love to me from the beginning to the completion of this work.

The journey one must make to earn an MPHIL can be very lonely and tormenting. I am fortunate to have had the support of many people from academia and industry along the way. I am sincerely indebted and thankful to all of them. This work could not have come together without their help.

I would like to express my sincere gratitude to all the people who made this proposal possible. First and foremost, I am indebted to my supervisor, Mr. D. Asamoah for his guidance and intuitive supervision, as well as patience during this period of study.

I wish to thank all my good friends, course mates and many Information Technology experts whose patience in answering my numerous questions have led to the completeness of this proposal.

Lastly, but certainly not the least, I would like to say a big “thank you” to my family for their continued support and encouragement throughout my sleepless nights of studies.

I also owe a debt of immense gratitude for the assistance offered me by Eddy of Vodafone Ghana, Samuel from the Tullow Ghana and to Mills of MTN Ghana.

Special thanks again goes to colleague students of the Department of Computer Science for their encouragement, I appreciate the advice of all.

ABSTRACT

With over 1 billion users today, the Internet and its accompanying infrastructure has changed the way traditional essential services such as banking, transportation, telephony, medicine, education and even defence are operated. It has also become a conduit for people, businesses and governments around the world to also regularly access useful information, perform tasks such as banking, information dissemination and shop at many different retailers across the globe.

Ghana has become highly dependent on the Internet now which is considered as the main infrastructure of the global information society. Therefore, the availability of the Internet is very critical for its socio-economic growth. However, the inherent vulnerabilities of the Internet architecture provide opportunities too for lot of attacks on its infrastructure and services.

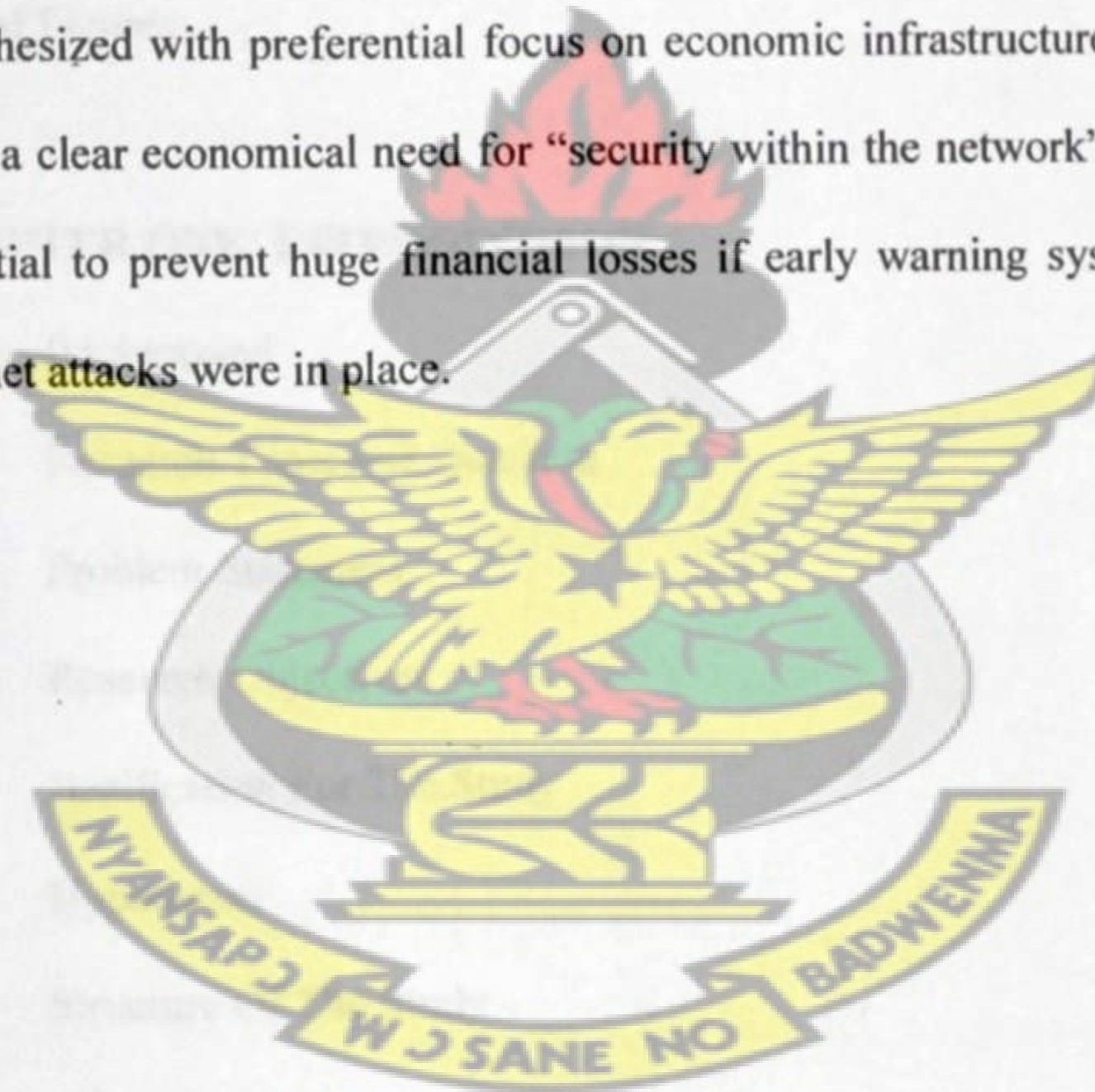
Distributed Denial-Of-Service (DDoS) attack is one such kind of attack, which poses an immense threat to the availability of the Internet by compromising the availability of networks and servers. DDoS attackers infiltrate large numbers of computers by exploiting software vulnerabilities, to set up DDoS attack networks. As specific countermeasures are developed, attackers enhance existing DDoS attack tools, developing new and derivative DDoS techniques and attack tools

It has been increasingly found to be affecting the normal functioning of e-commerce businesses and organizations causing billions of dollars of losses. The costs of DDoS attacks to critical infrastructure organizations and institutions can be significant and their impact can vary from minor inconvenience to the users of a web site or service, to serious financial losses to companies that rely on their on-line

availability to do business (Mirkovic, et al 2002; 2003) and culminating in huge financial loss to the Country.

This research paper presents an analytical view to determine the economic and indirect implications of DDoS attacks to Ghana's emerging Economy vis-à-vis network Infrastructure.

Furthermore, rationale of perpetrators' motives to instigate the attacks is hypothesized with preferential focus on economic infrastructure components and to show a clear economical need for "security within the network" and to illustrate the potential to prevent huge financial losses if early warning systems for large-scale Internet attacks were in place.



CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

2.1 Distributed Denial of Service

2.2 Network Security

2.3 Cloud Based Server

TABLE OF CONTENT

Declaration	ii
Dedication	iii
Acknowledgement	iv
Abstract	v
Table of Contents	viii
References	x
List of Tables	xi
List of Figures	xiii

CHAPTER ONE: INTRODUCTION

1..0	Background	1
1.1	Research Topic and Question	6
1.2	Problem Statement	7
1.3	Research Objectives	8
1.4	Justification For The Study	9
1.5	Hypotheses	10
1.6	Structure Of The Study	14

CHAPTER TWO: LITERATURE REVIEW

2.0	Introduction	15
2.1	Distributed DoS Attack	17
2.2	Network Security	19
2.3	Client Verses Server	20

2.4	OSI Reference Model	21
2.4.1	Typical Examples of OSI Attacks	23
2.5	Types of DDoS Attacks	25
2.5.1	Variants of An Attack	26
2.5.2	Attack Parameters	29
2.5.3	Example of DDoS Tools	31
2.6	Current DDoS Solutions And Reasons For Their Failure	33
2.6.1	Routers	33
2.6.2	Firewalls	34
2.6.3	Intrusion Detection System (IDS)	34
2.7	Motivations For DDoS	35
2.8	Financial Impacts Of DDoS	37
2.8.1	Financial Costs of DDoS	39
2.8.2	Intangible Consequences of DDoS	40
2.9	DDoS Threats to an Economy	41
2.9.1	Ghana's Emerging Economy	41
2.9.2	Telecos Contribution To Ghana's Economy vis-à-vis GDP	44
2.9.3	Ghana's E-Commerce Readiness	47
2.9.4	Trade Partners	49
2.9.5	Current Infrastructure	51
2.9.6	Targets by Industry	55
2.9.7	Cyber Crime and Combat Readiness	58
2.9.8	Estimating Losses Due To DDoS	61

CHAPTER THREE : METHODOLOGY

3.0	Research Phases	64
3.1	Calculating Financial Loss	67
3.1.1	Downtime Loss	69
3.1.2	Disaster Recovery Loss	70
3.1.3	Liability Cost	70
3.1.4	Customer Loss	71
3.2	The Questionnaire Format	72

CHAPTER FOUR: RESULTS AND DISCUSSION

4.0	Descriptive Results	74
4.1	Research Results	75
4.2	Estimating Financial Loss	84
4.3	Scenario	84
4.3.1	Downtime Loss	87
4.3.2	Disaster Recovery Loss	88
4.3.3	Liability Loss	90
4.3.4	Customer Loss	89
4.4	Final Analysis	92

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1	Summary	94
5.2	Conclusions	97
5.3	Recommendations and Suggestions for Future Research	98
5.4	Limitations of the Study	99

REFERENCES

100

APPENDICES

APPENDIX A : QUESTIONNAIRE

106

APPENDIX B : QUESTIONNAIRE DATA TABLE

108

KNUST



LIST OF TABLES

Table 1.0	Internet Users in Ghana (Source: www.gipcghana.com)	16
Table 1.1	Operators and Service Providers 2010	45
Table 3.0	Steps	66
Table 3.1	Motives	66
Table 3.2	Local Values	68
Table 3.3	Downtime Loss	69
Table 3.4	Disaster Recovery Loss	70
Table 3.5	Claim	71
Table 3.8	Customer Loss	72
Table 3.9	Questionnaire Table	73
Table 4.0	Are you aware of DDoS	75
Table 4.1	Have you ever experience any in your institution?	76
Table 4.2	What in your opinion is the largest Threat Vector perceived by your network today	77
Table 4.3	Which of the following attack vector was observed within the past 6months	78
Table 4.4	How do you Detect an attack?	80
Table 4.5	How do you mitigate an attack?	81
Table 4.6	What do you think would be the motives behind a DDoS attack if it is to happen to Ghana?	82
Table 4.7	Questionnaire Data Table	86
Table 4.7.1	Down Time Loss Data	87
Table 4.7.2	Disaster Recovery Loss Data	88

	Table 4.7.3	Liability Loss Data	89
	Table 4.7.4	Customer Loss Data	90
Table 4.8		Telco-M Estimated losses over a period of 48 hours	92
Table 4.9		Are you aware of any Cyber Crime Laws in Ghana?	93
	Table 4.9.1	Have your Institution ever taken any Culprit to a Law Court before?	93

KNUST



LIST OF FIGURES

Figure 1.0	Scheme of a DDoS attack	4
Figure 2.0	Critical Infrastructure	8
Figure 2.0	Distributed Denial of Service	18
Figure 2.1	What DDoS Looks Like To A User	21
Figure 2.2	OSI Reference Model	21
Figure 2.3	The standard TCP three-way handshake	24
Figure 2.4	Internet Bandwidth	27
Figure 2.5	Some Variants of the Basic Attack	28
Figure 2.6	Timeline For Evolution of DDoS Attacks	36
Figure 2.7	Financial Cost of DoS	38
Figure 2.8	Internet Development and Governance	52
Figure 2.9	Access To ICT	53
Figure 4.0	Awareness Of DDoS	75
Figure 4.1	DDoS Experience	76
Figure 4.2	Infrastructural Threat Vector	77
Figure 4.3	Attack Vectors	78
Figure 4.4	Attack Frequency	79
Figure 4.5	Attack Detection	80
Figure 4.6	Mitigation Techniques	81
Figure 4.7	Motives	83
Figure 4.8:	Total Economic Loss	91

CHAPTER ONE

INTRODUCTION

1.0 Background

Ghana's Information and Communication Technology Sector and its accompanying infrastructure has rapidly progressed over the last decade. As one of the first countries to introduce widespread liberalization in basic telecommunications services, in 1994, Ghana took an important step forward in embracing the potential of competitive markets to generate growth and innovation in the sector.

Ghana's ICT Industry comprises telecommunications operators, internet service providers, VSAT data operators, software manufacturers, ICT education providers, internet cafés, etc and generally, the Ministry of Communications and the National Communications Authority (NCA) oversee activities in the sector.

The infrastructural base of the sector includes licensed gateway operators, SAT-3 Access, Private Licensed VSAT Systems, Fixed Wired Line Networks, Wireless Mobile Operators, Public telephones systems, Tele Centres, Dedicated Transmission Networks, Public Distribution Networks (TV, DSL, etc.), Internet Service Providers, Internet Backbone Connectivity throughout the Country and Public Access Point and Broadcasting Systems.

As an initiative to support emerging technologies, the Ministry of Communications is also facilitating the establishment of Science and Technology Parks. Ghana remains a very safe and secure investment destination. It has established the necessary legal and regulatory framework which guarantees the safety of investments in the ICT industry.

Ghana has been recognized as an attractive destination for Business Processing Outsourcing (BPO) and was ranked the No. 1 destination in Sub-Saharan Africa (ahead of Senegal and South Africa) and No. 25 globally out of 50 countries by the A.T. Kearney Global Services Location Index (GSLI, 2011).

However, the phenomenal growth and success of the internet in Ghana and Africa as a whole has changed the way traditional essential services such as banking, transportation, marketing, education are operated.

Now they are being progressively replaced by cheaper and more efficient Internet, online and mobile based applications. Computer networks have therefore become the nerve systems of modern enterprise/businesses and the world is highly dependent on this critical internet infrastructure and highly considered as the main infrastructure of the global information society.

Therefore, the availability of the Internet or computer resource has become very critical for the socio-economic growth of every society. Conversely, with the number of nodes in the Internet's backbone networks going up exponentially the likelihood of surfacing of entities exhibiting seemingly hostile objectives has been increasing progressively.

The natural vulnerabilities of the Internet architecture has provided opportunities for a lot of attacks on its infrastructure and Services. A service is any aspect of a computer system's functioning that provides benefits to a user. Any intervention that reduces or eliminates the availability of that service is called a Denial of Service, often abbreviated DoS.

Denial of service (hereinafter DOS) attack is such a network-based incursion during which an agent intentionally saturates system resources by means of increased network traffic otherwise utilized to handle legitimate inquiries (Carl et al 2006).

The year 1998 brought the addition of three novel concepts to DoS attacks. The first is the idea of distributing the attack across several hosts. The second is the idea of coordinating the attack among many machines. The third is using the distribution system to thwart all attempts of discovering the origin of the attack.

A type of attack that is becoming more prevalent today is that known as a Distributed Denial of Service attack. Distributed Denial of Service (DDoS) attacks which takes advantage of the current situation and primarily aim at destabilizing or severely limiting usability of infrastructure to the end-users in part or whole.

These ideas constitute what is known as Distributed Denial of Service attack (DDoS). DDoS differs by using many hijacked systems in a hierarchical structure controlled by a single attacker (master) and represents coordinated effort aimed at destabilizing infrastructure elements (Garber 2000).

As DDoS is effectively a type of Denial of Service attack, throughout this research, references to DDoS include DoS. A scheme of an attack is as depicted in Figure 1. Distributed Denial of Service (DDoS) attacks have been increasingly found to be affecting the normal functioning of organizations causing billions of dollars of losses. For any organization, having a secure and available network is the primary aim to reach their business goal.



Figure 1.0: Scheme of a DDoS attack (Mirikovic et al 2004)

At present, reliability and availability of Internet services can be degraded

significantly within seconds. Such an attack can take many shapes, ranging from an

attack on the physical IT environment, to the overloading of network connection

capacity, or through exploiting application weaknesses. Flooding of critical

connections and vital services with attack traffic could result in total loss of Internet

connectivity.

Companies relying on the Internet for their daily business will inevitably

sustain substantial financial damage by such a large-scale attack that the situation can

easily pass as a threat vector to the National Economy. On one hand, direct damage

such as revenue loss during the attack and on the other hand indirect damage such as

customer loss due to degraded reputation will be suffered.

The costs of DoS attacks to critical infrastructure organisations and institutions

can be significant and their impact can vary from minor inconvenience to the users of

a web site or service, to serious financial losses to companies that rely on their on-

line availability to do business (Mirikovic, et al 2002; 2003) and culminating in huge

financial loss to the Country.

A respondent to the 2005 Australian Computer Crime and Security Survey reported a single-incident loss of \$8 million arising from a DoS attack which is a percentage of the country's GDP. For many critical infrastructure companies, a significant and prolonged period of system unavailability could result in losses in order of magnitude higher than this.

Internet-facing and other networked infrastructure components/institutions in Ghana are at risk of DDoS for two primary reasons:

1. As a developing country, resources such as bandwidth, processing power, and storage capacities are limited hence any DDoS attack will wreak havoc by targeting these resources in order to disrupt systems and networks.
2. Internet security is highly interdependent and the weakest link in the chain may be controlled by someone else thus taking away the ability to be self reliant.

Over the years, the Information Technology industry has seen a huge boost but however has also seen many DDoS attacks, including some that took down the services of well-known, major global enterprises. Despite the efforts of the security community, DDoS continues to wreak havoc on the Internet and accessible networks.

1.1 Research Topic and Question

Research is a methodical procedure of gathering and examining data to increase or add knowledge of the subject area under study (Matos 2012).

The title of this thesis is “*Distributed Denial-Of-Service (DDoS) Attacks as Threat Vectors to Ghana’s Economic Infrastructure (Case Of Ghana’s Emerging Economy Vis-À-Vis Network Infrastructure)*”.

Ever since the inception and introduction of the internet into the country in the early 1990s, Ghana’s economy now utilizes much of the internet or network environment and infrastructure to transact business. With the construction of the E-governance network infrastructure across the country and the cost involved, there may be something to protect against illegal access to prevent huge financial losses to the state. The information technology industry now contributes a significant proportion to the country’s annual GDP. Many financial institutions for instance, are networked and span across the whole country and can be physically identified. This means that, a potential attacker can target such institutions for possible vulnerabilities, and hereby launch offensive attack. Accurate data is not available in Ghana about whether attacks are actually on-going, have gone on, or have been used against any Ghanaian institution or organization and has incurred some amount of losses.

This research will raise efforts to analyze the scanty data and review motives that might drive cyber criminals to launch DDoS attacks in or against Ghana, and whether such motives can be prevalent in Ghanaian socio-economic environment.

Therefore, the question this research seeks to answer is; *whether a DDoS attack in Ghana is really a threat vector, how much of economic damage can it cause to the economy and the motives behind it?*

1.2 Problem Statement

The Internet has become part of Ghana's critical infrastructure. Critical services like banking, bill payment, tax payment, booking travel reservations, and shopping etc. now require secure and reliable communications. These secure system's communications habitually use the Internet and its security flaws expose these services to abuse.

A secure system should be able to correctly respond to attacks. To be secure, a system must provide availability, data integrity, confidentiality, nonrepudiation, access control and authentication [W. Stallings, 1995].

Without Availability, Confidentiality and Integrity are "Not Available". Weakness in any of these areas can be exploited to undermine system integrity by a DDoS. When these three major principles (Confidentiality, integrity and Availability) of information are ensured, the requirements of secure information are satisfied. Keeping information private and secure is confidentiality; information remaining unchanged is integrity and making information and services ready for use when needed is availability. These C-I-A triad should be addressed (Kim and Solomon, 2012) to prevent DDoS from penetrating.

These attacks on the whole can cost the target a great deal of time and money but however a DDoS attack does not usually result in the theft of information.

Ghana's information and communication technology infrastructure has developed progressively since the economic adjustment programme. These vital infrastructure consists of the physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the Nation.

In this perspective, the following industries as depicted in Figure 2.0 are considered to be critical with utilities and telecommunications providing the underpinning support services.

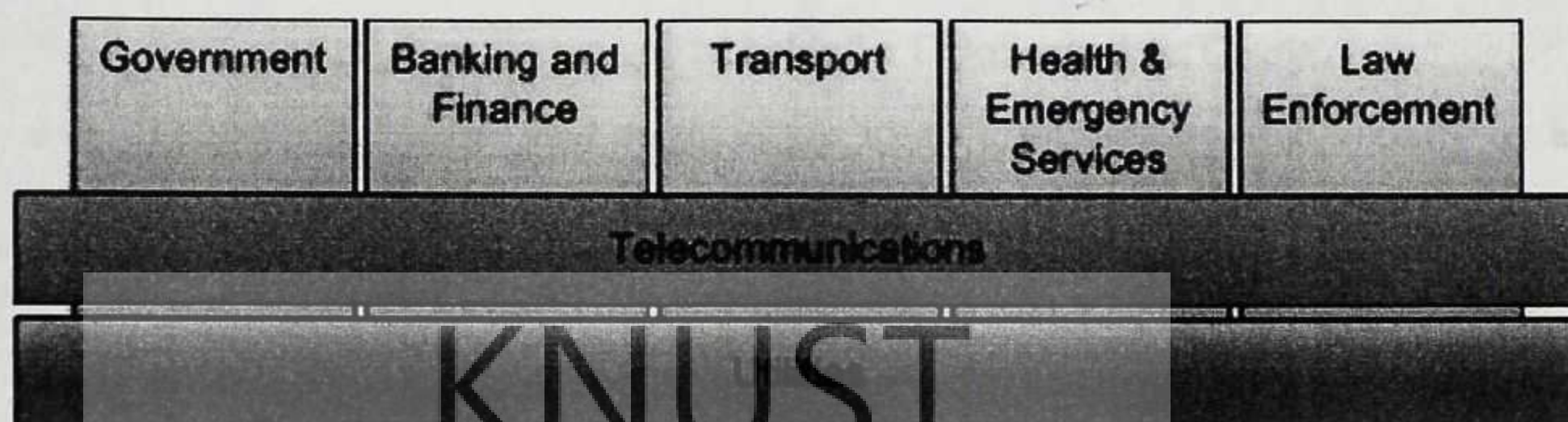


Figure 2.0 : Critical Infrastructure

DDoS attacks are not only directed to the internet environment but also to any (or all) IP networks. The target may be a branch of networked bank, or Municipal District Assembly on E-government network, or even ISP who offers e-commerce services to many subscribers. Distributed denial of service attack on a small IT infrastructure-based country such as Ghana, will register an enormous economic damage across the economic landscape of the nation.

1.3 Research Objectives

Ghana may not have seen much of cyber-attacks as in other developed countries where internet is a basic platform for meeting customers, trade and conducting transactions but the menace of sakawa gives a prelude to worry.

This research is aimed at studying various threats and vulnerabilities associated with DDoS attacks on network infrastructure and analyzing the magnitude of economic damage it can cause to the Nation. In the study too, many other means will be sought to recommend, prevent or counter measure by which the economic damage may be prevented.

The Objectives of this study are therefore to;

- Technically probe and analyze whether DDoS attacks are actually on-going, have gone on, and or ever happened against any Ghanaian institution or organization.
- Study the motives that might be behind a DDoS attack in Ghana.
- Estimate the losses that might occur to an institution and the country as a whole as a result of an attack.

KNUST

1.4 Justification For The Study

DDoS attack aims to intentionally deprive legitimate users of a resource (or service) provided by a system, typically by overloading that system with a flood of data packets from multiple sources. These attacks have emerged as a prevalent way to compromise the availability of networks/servers/infrastructures, which imposed financial losses to businesses and a country as a whole.

VeriSign's iDefense predicts that the number of financially motivated cyber criminals will grow. A DoS attack that seemed a negligible risk could easily turn into a massive financial loss problem that may quickly become too difficult to handle, perhaps driving into "National Economy State-Of-Emergency".

Organizations today are linking their systems across enterprise-wide networks and virtual private networks (VPNs), as well as increasing their exposure to customers, competitors, browsers and hackers on the Internet (John Vacca, 2006). Thus, in Ghana online businesses and indeed, economic venture or government information network with a Web presence need to be aware of the growing threat from these kinds of attacks. An effective DDoS mitigation system can safeguard business operations against DDoS-related outages.

This research study provides the premises for evaluating DDoS as a threat vector in Ghana's economy, with extended scope of reviewing the motives behind such attacks and the development of a concept to counteract DDoS as well as ensure the availability of a network/connectivity in order to contribute a good percentage to the country's GDP.

The main research goal will be to show a clear economical need for "security within the network" and to illustrate the potential to prevent huge financial losses if early warning systems for large-scale Internet attacks were in place.

The research will also tackle core problems by contributing an Economic Damage Model for DDoS attacks which will be the first comprehensive model to estimate the financial damage caused by DDoS attacks suffered by Internet-dependent organisations and the Nation. With this model, we would be able to estimate an instance of the whole of Ghana being affected by a massive DDoS attack lasting for week.

Although there is very little public information concerning DDoS attacks in Ghana, analyzing the few available and reliable sources helps to gain a better understanding of the current motives and methods of DDoS attackers

1.5 Hypotheses

This research also seeks to answer the question of who commits attacks and why through the means of the DDoS attack, which is currently perhaps the most harmful of cyber-attacks worldwide.

Most attacks are of a “hacktivist” nature (D. E. Denning 1999). Hacktivists as the name suggests are hacking activists who use the tools of the Internet to gain attention to their cause. Common hacktivist tactics include web defacement and email bombs, and sometimes using DDoS (Nagpal 2002) such as web sit-ins of the Zapatista movement and WTO trade talks as well as DDoS attacks related to the bombings in Kosovo (Nagpal 2002).

It is quite understandable why someone with a goal might seek to use these tools as a form of protest. In live protests some participants often become rowdy and in much the same sense some members of a group with an online petition and movement might become aggressive on the Internet.

Another motive for cyber-attack seems to be criminal. The possibility was discussed regarding the Estonian attacks and it is very popular in general. Syndicates like the Russian Business Network have been cited as sources of attack before and it is not surprising that this will continue (Shachtman, 2009).

As early as year 2000, officials were concerned about the use of the Internet for the purposes of extortion and the possibility of this threat continues to exist today (Freeh 2000, Wilson 2008). The botnets controlled by crime syndicates such as the Zhelatin gang's Storm botnet are strong enough to keep a site down for many days.

The threat of cyber-extortion is enormous as the use of cyber-attacks to enforce requests may cause a site to go down indefinitely. Syndicates use the strength of their botnets to extort money from gambling websites (Haug 2007). Such sites rely on the strength and trust of their customer base to continue business, which requires them to maintain continuous operation.

Mirkovic and Reiher discuss this possible loss of trust as a reason for the lack of reporting concerning attacks, as companies fear the end result (Mirkovic and Reiher 2004).

The possible economic loss from an online-attack can be sometimes immeasurable as the five most costly viruses of all time summed up to \$102 billion in losses (Borglund, 2009).

While the economic motive for a-attack might also be common, most attacks of an economic motive would most likely be in conjunction with an attack that had a political or criminal motive, the true motive being to see the victim suffer financially or to enhance the attacker financially. Economic motive does not seem to truly be that much of a threat singularly.

Mobile phone usage in another perspective has become an increasingly critical service, so smart phones open up new possibilities for DDoS attacks with potentially serious impacts on the economy because of the rippling effect of any DDoS attack.

Based on this literature I was able to form two hypotheses regarding DDoS attack if it is to happen in Ghana's case. The first is that if there is a DDoS attack, then it will be politically motivated and hacktivist in nature. Such groups have used the Internet more popularly and are also known to have launched attacks.

While economic and criminal attacks in Ghana like the sakawa menace are sometimes better reported it is political attacks that seem to have the largest following and I hoped to test that notion with this research.

My own hopes for the research and the literature strongly supported the formulation of this hypothesis. A scholar points out “while many computer networks remain very vulnerable to attack, many critical infrastructures are equally vulnerable” (Lewis, 2002).

The online populace in Ghana now relies on a number of websites and or internet based services and should those services be interrupted it could result in the loss of large amounts of revenue for a company and the clientele. At the same time because these people rely on these services they must have a great deal of trust to be handing out their private information.

An attack of a certain magnitude may result in a loss of trust in the system that would lead to negative long-term effects for not only the Internet economy but also the economy as a whole (Karatzogianni 2002).

It's fair to say that there is a little discussion of the threat of online attack and information warfare in the literature but at the same time, just because the threat isn't large now in Ghana does not mean it cannot be in the future.

A report on online security prepared for President Obama notes that “foreign entities have been able to penetrate poorly protected computers and collected immense quantities of information” and that “exploiting vulnerabilities in cyber infrastructure will be part of any future conflict” (Lewis 2008).

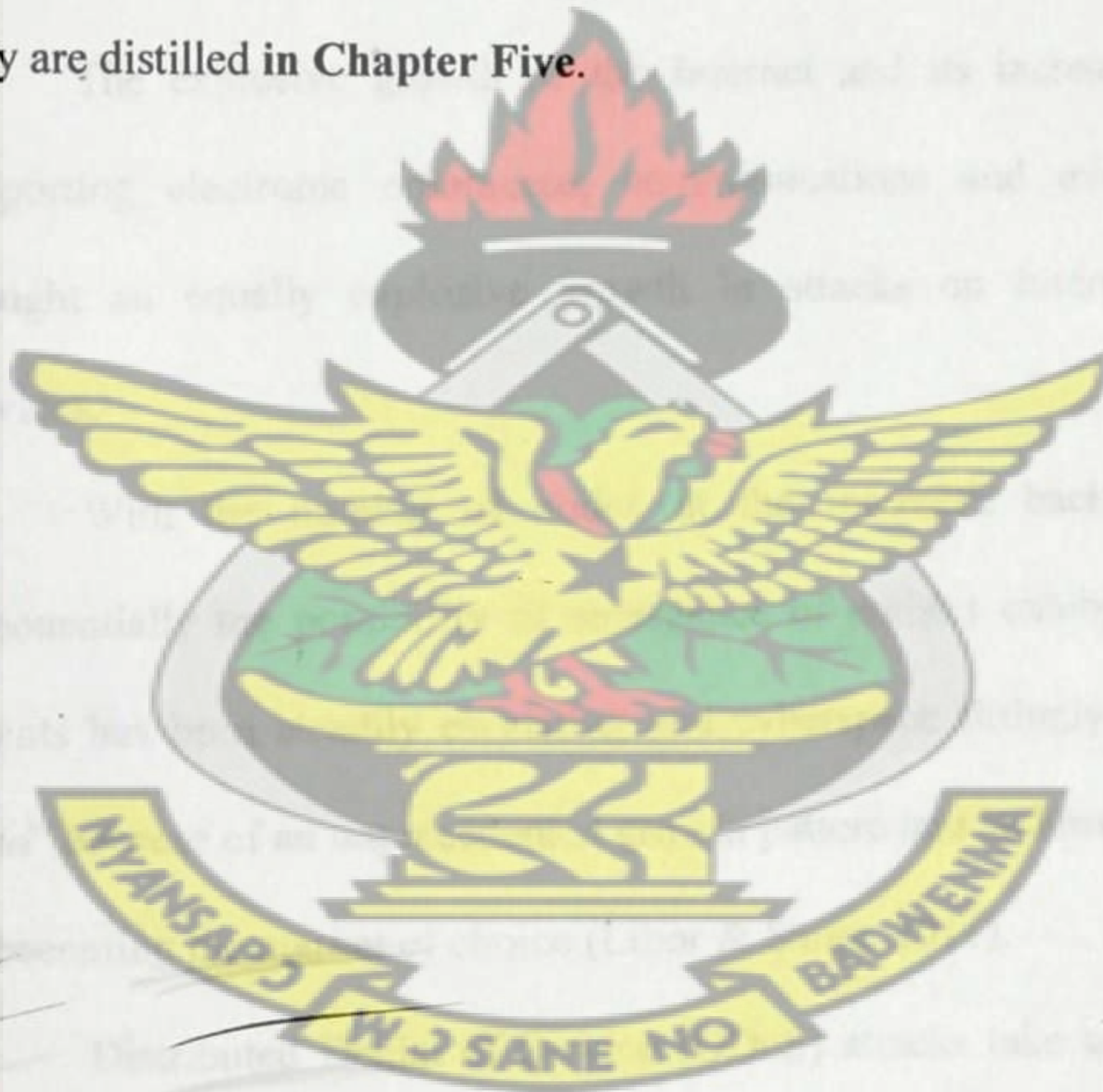
Distributed denial-of-service (DDOS) attacks therefore stands out as a rampant way to compromise the availability of networks and servers, which imposed financial losses for e-commerce businesses and even the normal brick and mortar companies.

1.6 Structure Of The Study

The study is organised into five chapters: **Chapter One** provides the introduction, problem statement, objectives and justification of the study.

Chapter Two gives an overview of literature relevant to the study. **Chapter Three** outlines the methodology employed to achieve the objectives of the study.

In **Chapter Four**, the empirical results are provided and conclusions from the study are distilled in **Chapter Five**.



CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

As the use of computers and networks has expanded in Ghana, researchers and practitioners have shown increasing interest in the role of network security in protecting the confidentiality, integrity, and availability of information and its impact on organizations.

The explosive growth of the Internet and its increasingly critical role in supporting electronic commerce, communications and even transportation has brought an equally explosive growth in attacks on Internet infrastructure and services.

With the number of nodes in the Internet's backbone networks rising exponentially the possibility of emergence of entities exhibiting outwardly hostile intents has been steadily escalating and cyberspace fittingly termed "*the no man's land*" because of an unprecedented growth pattern and lacklustre control mechanisms is becoming the market of choice (Libor & Sarga, 2011).

Distributed Denial of Service (DDoS) attacks take advantage of the current situation and primarily aim at destabilizing or severely limiting usability of infrastructure to the end-users in part or whole. It does this by overwhelmingly flooding a victim's network or system with packets generated from many different sources, with the intent of preventing legitimate use of services. Typically, DDoS attacks are directed at one or more targets, such as end-users, web servers, entire networks or parts of networks, or networking infrastructure components.

DDoS attacks pose a severe threat to the nation's ability to conduct business and provide vital government services to its citizens.

Today, with the advancement of information and communication technologies, our societies are evolving into global information societies and this ever-present computing environment has made cyber-attacks much more sophisticated and threatening than ever before [APEC. 2005].

In addition, with the spread of e-commerce, e-government and e-learning, most traditional economic and social activities have become dependent on the online environment. Over the last decade, internet usage has greatly increased mobile cellular market, the internet market in Ghana presents an important potential for growth and development. As a critical source of information, the internet is viewed as a significant development enabler. In 2000, Ghana had an estimated number of 30000 internet users. This has increased over the years reaching 609800 in 2006. By June 2009, Ghana had nearly eight times as many internet users as it did in 2000 with the number of 997000 internet users as seen in the table below.

Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Total (000s)	30.0	40.0	170.0	250.0	368.0	401.3	609.8	880.5	997.1	1297.0
Per(100) Inhabitants	0.15	0.20	0.83	1.19	1.72	1.83	2.72	3.85	4.27	5.44

Table 1.0 Internet Users in Ghana (Source: www.gipcghana.com)

In 2000, there were Distributed Denial of Service (DDoS) attacks against sites like Amazon, Yahoo and eBay. These DDoS attacks were made possible by botnets (*networks of PCs compromised by malware and under the control of an attacker*). One analyst assessed the damage of these attacks at \$1.2 billion.

About \$1 billion of that amount was the result of a negative impact on stock prices; about \$100 million was lost revenue from sales and advertising, and about \$100 to \$200 million were put into security upgrades (Niccolai 2000).

However, the victims saw it rather differently. Yahoo, for example, argued that it did not suffer major losses and that the losses in advertising could in part be recovered by replacing their own ads with those of paid clients (Denning 2000).

Misuse of the online environment through spam, identity theft, fake websites and other means threaten to undermine the potential economic and social benefits of the online environment by eroding the trust and confidence in the safety and security of the online environment. These developments have made a safe and reliable online environment an important factor for competitiveness.

2.1 DDoS Attack

A Distributed DoS attack is a type of DoS attack, which employs multiple disparate attacking entities to execute an attack; however, it is common for the distributed entities to be effectively be under the control of a single primary attacker.

Rather than attacking a target directly, perhaps a single high-speed connection, the attacker will instruct a number of previously compromised computers (which individually may only possess slow to moderate connections), to attack the target. The combined power of many scarcely resourced attacking entities creates a significant resource.

A DDoS attack will typically proceed as follows (TISN, 2006):

1. An attacker will compromise many hundreds or even thousands of machines via automated means, such as a worm, or by manually breaking into each system over a period of time. The compromised machines are known as 'zombies' (Handlers).
2. Malicious software called a 'bot' (short for robot) will be installed on each compromised machine to allow future remote control of the machines. These are collectively known as Agents or 'botnet' (short for robot network).
3. Once an attacker has control over a sufficiently sized botnet, they will instruct all the zombies to attack the target simultaneously.
4. Due to the vast bandwidth resources available to the botnet, the target system or underlying network will collapse under the sheer volume of connections as shown in the Figure 2.0 below.

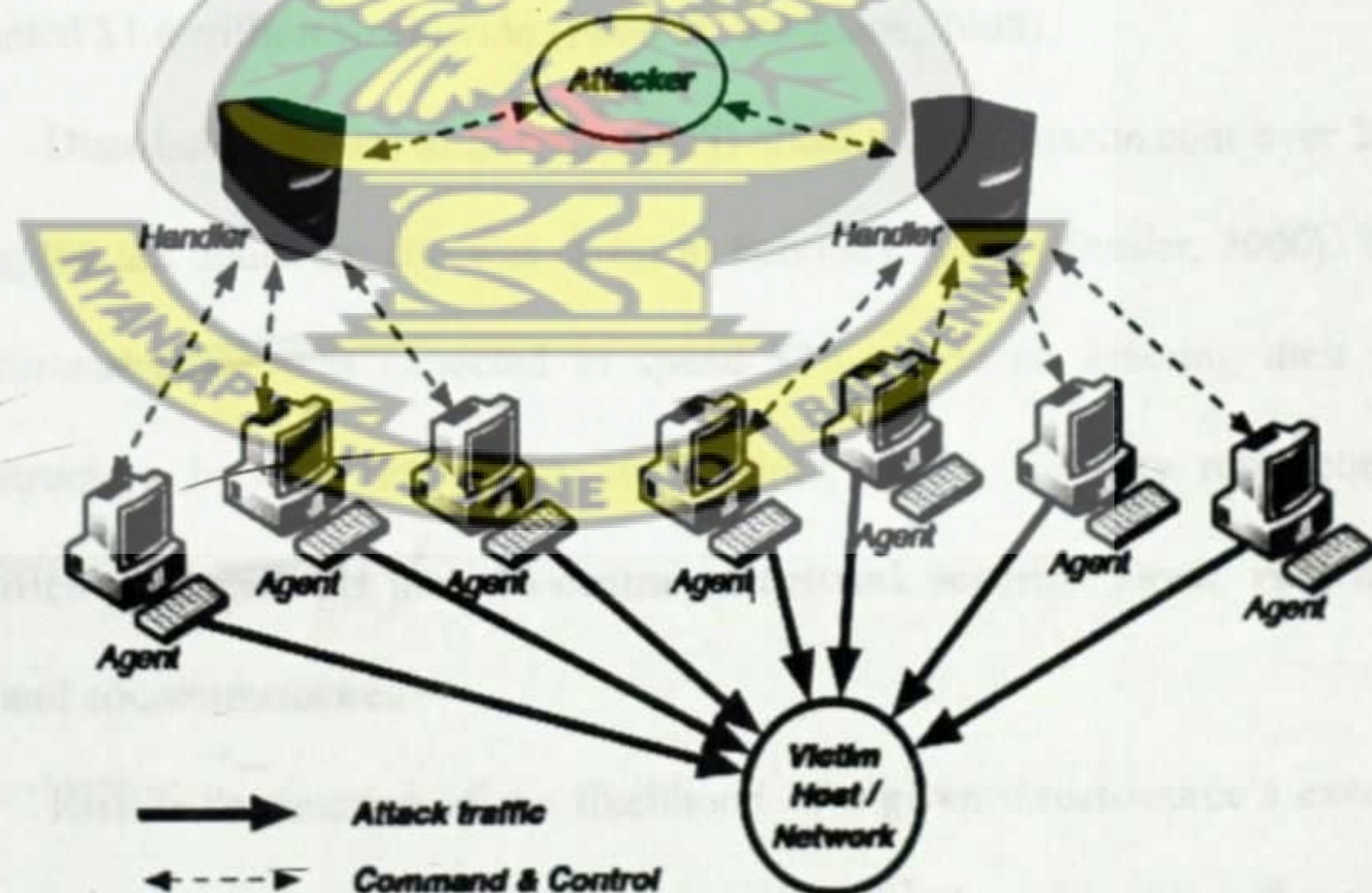


Figure 2.0: Distributed Denial of Service (source : Scarfone et al. 2008)

2.2 Network Security

The identification of Information and Communication Technology (ICT) as an essential tool for sustainable development and economic growth has proved to be worth every investment in Ghana and Africa as a whole. As a result of this, Internet usage in Ghana has grown rapidly resulting in the explosion of Internet Service Providers (ISPs) and Internet access points. However, network security has not been well catered for.

Stallings (2007) defined network security as “the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks” (Stallings, 2007). The strategic impact of network security is vast; a survey conducted by PricewaterhouseCoopers (PwC, 2008) of 4900 IT professionals across 30 countries found that poor network security resulted in a loss of 39,363 human years of productivity in 2008; costing an estimated \$1.6 trillion worldwide (Final IT Solutions, 2008).

Distributed Denial of Service (DoS) attacks cost Amazon.com over \$600,000 during the ten hours the site was down in February, 2000 (Kessler, 2000). The U.S. government alone was expected to spend \$30 billion on securing their network infrastructure between 2008 and 2015 (Gold, 2008). Security researchers have identified four concepts that are central to network security: threat, vulnerabilities, risk, and countermeasures.

Risk is “a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization” (Stoneburner et al, 2002). Put simply, a threat is any action that can cause damage or allow unauthorized access. Vulnerability is a known bug or opening that can be used to cause damage or gain unauthorized access.

A risk is the potential for someone to exploit that vulnerability. Counter measures are designed to minimize risk by securing vulnerabilities and reducing the overall threat to the systems and data connections. DDoS attacks against the server side of the connection are by far the most common because, in general, the attacker intends to affect all users (clients) of a resource rather than a particular subset. Furthermore, it is usually difficult to identify the users of a system and directly target them.

KNUST

2.3 Client Verses Server

Accessing a networked service or functionality at a high level involves two parties. The first, loosely termed the *server*, provides the service to the accessing party, loosely termed the *client*. Although other networking paradigms such as peer-to-peer do exist, any communication still occurs between two high-level parties, each of which is a potential target for attack.

The prevention or delay of authorised access to a system resource can therefore be achieved in one of two ways:

1. By impeding the ability of the server to provide the service; or
2. By impeding the client's ability to access the service.

DoS attacks against the server side of the connection are by far the most common because, in general, the attacker intends to affect all users (clients) of a resource rather than a particular subset. Furthermore, it is usually difficult to identify the users of a system and directly target them. A typical example of what an end-user might experience as a result of DDoS attack is as shown in Figure 2.1.

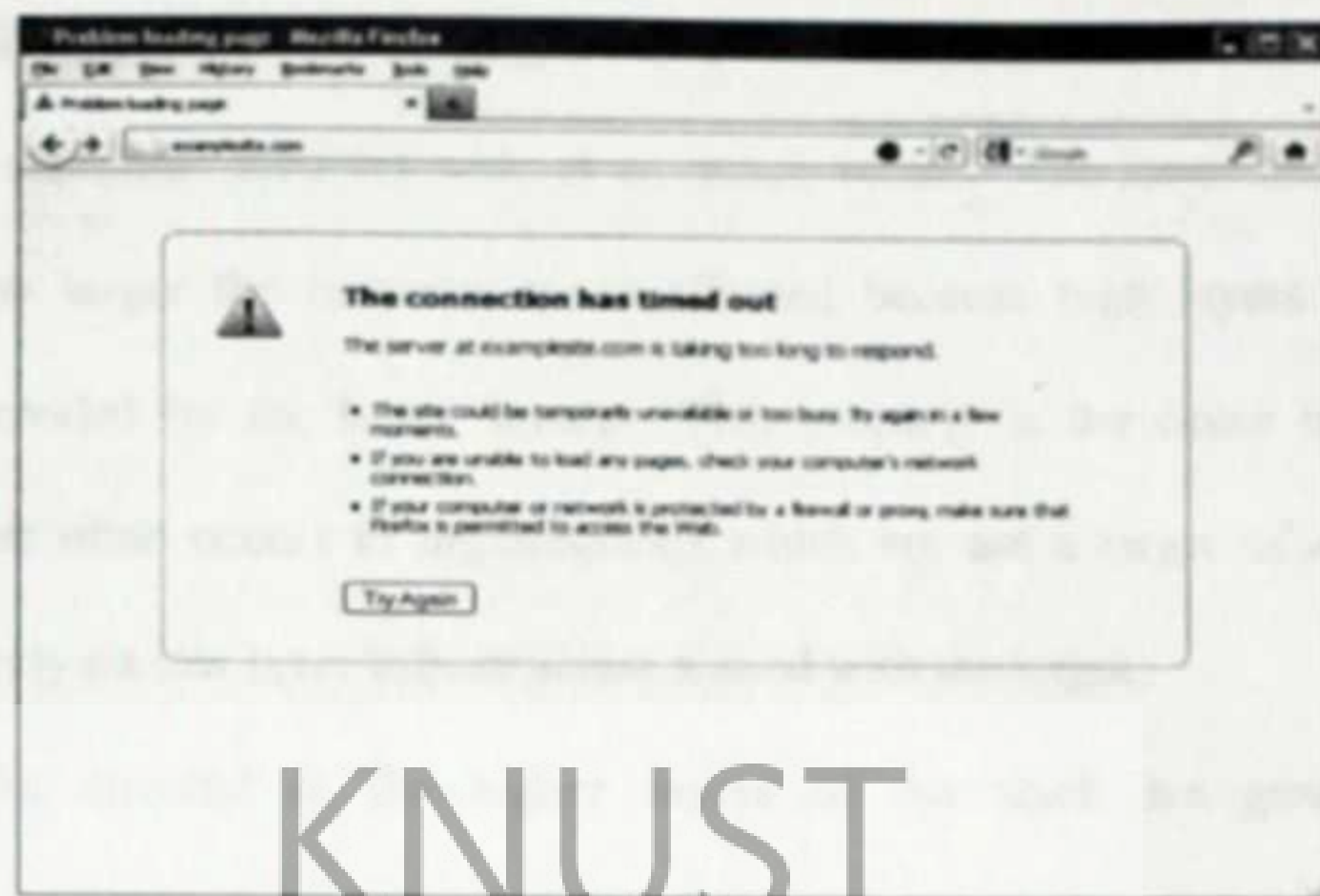


Figure 2.1 What DDoS Looks Like To A User (source: jumbojoke.com/images/fast.jpg)

2.4 OSI Reference Model

The ISO Open Systems Interconnection Reference Model (ISO, 2000) divides communications into seven layers as shown in Figure 8: OSI Reference Model, below. Each layer is dedicated to performing a specific function on the data being communicated. The application layer is where the meaningful business logic occurs while the actual data transfer occurs at the physical layer, with intermediate layers translating between data types and facilitating meaningful exchange.

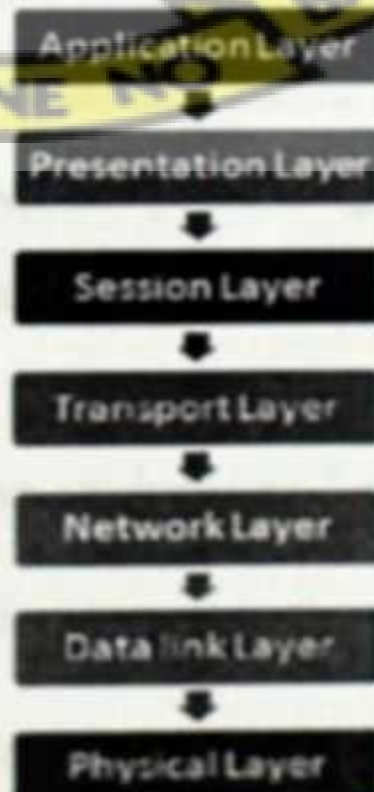


Figure 2.2: OSI Reference Model (source : net.tutscity.com)

It is therefore possible to target any of these layers in a DoS attack because there is no electronic medium without an attack vector. The lower the layer being attacked, the larger the resource space affected because high layers rely on the services provided by the lower layers. This property is the cause of 'collateral damage' that often occurs to organisations which are not a target of a given DoS attack, but rely on low layer infrastructure shared with the target.

Attacks directed at the higher layers of the stack are generally more sophisticated and tend to be harder to detect and prevent. Examples of attacks on each layer include:

- Application—corrupting the application database so that no processing of data is possible (Waldegger, 2006).
- Presentation—injecting formatting tokens so that information presented is no longer understandable.
- Session—submitting a logout message using a session identifier that is bound to another user.
- Transport—using a 'SYN flood' to cause the server to allocate vast amounts of resources for connections that will never be completed.
- Network—using a 'Teardrop' attack which involves sending highly fragmented IP packets to a target, requiring significant resources to reassemble.
- Data Link—using an 'ARP spoofing' attack to pose as a gateway by supplying a spoofed address, and subsequently refusing to deliver messages.
- Physical—Unplugging of the network cable connected to a server.

In addition to the above layers, an underlying 'environment' layer is necessary to describe threats posed to physical facilities hosting systems and networks.

An example threat at this layer is the use of a fire alarm to prevent IT administrators from accessing equipment for a short period.

2.4.1 Typical Examples of OSI Attacks

Application Layer 7 attacks (HTTP/1.1 GET): An Application layer DDoS attack can be carried out on a network by an attacker sending large amounts of legitimate requests to an application. For example, an HTTP flood attack can make hundreds of thousands of page requests to a webserver which can exhaust all of the server's processing capability.

With an HTTP flood attack, an attacker sends a SYN packet, and the target system responds with a SYN ACK. The attacker will complete the three way handshake with an ACK packet and then issues an HTTP GET request for a common page on the target system. This process amplified on a network can cause a very high computational load on the target system and may result in degradation of the network to a complete loss of availability of the application being requested by users.

One of the best examples of an HTTP flood attack was the MyDoom worm, which targeted many thousands of sites. In the case of MyDoom, 64 requests were sent every second from every infected system. With thousands of infected systems, the attack can prove to be over whelming.

Transport Layer 4 attacks (SYN) : A Transport layer DDoS attack can be carried out on a network and involves sending many connection requests to a target host. This attack is targeted against the operating system of the victim. It is very effective and extremely difficult to trace back to the attacker because of IP spoofing techniques used. An example transport layer attack is the TCP SYN flood. The SYN flood attack exploits a vulnerability of the TCP/IP protocol and is one of the most powerful and commonly seen attacks in the Internet (Moore, 2001).

When a normal TCP connection starts, the client sends a SYN packet from a specific port to a server where the port is in a listening state. The server will then send back a SYN ACK. The server will wait for an ACK acknowledge of the SYN ACK before the connection can be established. This is known as the TCP three-way handshake.

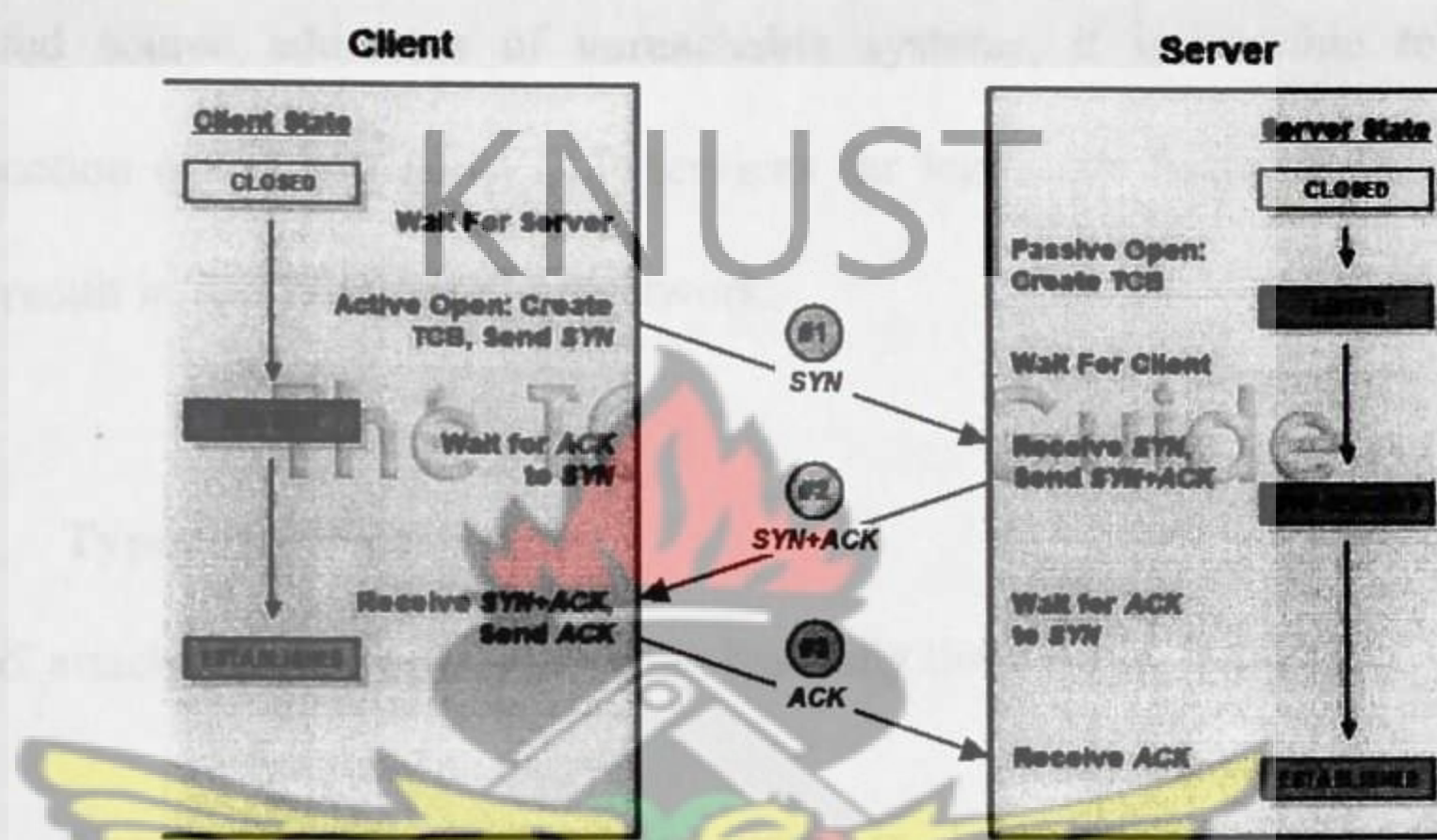


Figure 2.3: The standard TCP three-way handshake

(source: www.tcpipguide.com/free/diagrams/tcpopen3way.png)

However, the problem with the TCP three-way handshake process is that systems allocate resources to connections that have not been fully established - these are also known as **Half-Open Connections**. Too many of these potential connection requests can exhaust all resources allocated to setting up a connection.

When the SYN flood attack starts, attackers will send large amounts of SYN packets to the target system. These SYN packets can be from spoofed source addresses of unreachable systems. If the attacker is spoofing source addresses from systems that are unreachable, the target system will attempt to complete the session by sending back SYN ACK packets which will never be acknowledged or reset (ACK or RST packets).

The target system is now committed to setting up a connection, and this attempted connection will only be removed from the queue after the connection establishment timer expires. The three-way handshake is therefore never completed and the system under attack will not be able to clear the queue before receiving new SYN requests. If the attacker generates SYN packets at a very rapid rate from spoofed source addresses of unreachable systems, it is possible to fill up the connection queue and deny TCP services for legitimate users on the network and may result in degradation of the network.

2.5 Types of DDoS Attacks

DDoS attacks can disrupt networks in basically three ways, through:

Targeted Attacks usually work in layers 4-7 of the Open System Interconnection (OSI) model and take advantage of known vulnerabilities in specific applications, such as a programming flaw in a system, service, or protocol. The main objective of a targeted attack is to emulate the real world operation of a given resource, overrunning it with traffic. An example of such an attack is the *HTTP GET*. An attacker uses a zombie network to create numerous HTTP/1.0 or 1.1 compliant GET requests to consume all network and server resources available on the victim network.

Consumption Attacks (also known as flooding attacks) typically employ botnets to direct large amounts of traffic at a system or network in an attempt to consume all available network resources and shut down a system. Such attacks can cripple not only corporate networks but entire backbones.

An example is the *SYN Flooding Attack*- In SYN Flooding, an attacker initiates a TCP connection with the victim machine, sending only the SYN, which is the first part of the three-way TCP handshake. The victim machine returns the SYN-ACK, waits for the ACK packet to return and reserves one of the limited number of data structures required to complete the connection. Legitimate connections are denied while the victim machine waits to complete the bogus connection.

Exploitative Attacks are a type of consumptive attack that targets bugs in operating systems and works with other consumption attacks to cause network congestion. The most sophisticated attacks today encompass elements from all three types of attacks. An example is a *Tear Drop* where in some TCP/IP implementations, large packets of data are split into smaller segments, each of which is identified to the next by an offset marker; the receiving system later uses the offset marker to help reassemble the packets.

In a teardrop attack also, the attacker enters a confusing offset value in the second or subsequent fragments, which can crash the recipient's system. Attackers will go after all visible resources, attacking DNS servers as well as the full path of the network to find the weakest route until all network resources are consumed.

2.5.1 Variants of An Attack

Direct Attack is a situation where attackers rapidly send SYN segments without spoofed IP source addresses. This method of attack is very easy to perform because it does not involve directly injecting or spoofing packets below the user level of the attacker's operating system by simply using for example many TCP connect() calls. To be effective, however, attackers must prevent their operating system from

responding to the SYN-ACKs in any way, because any ACKs, RSTs, or Internet Control Message Protocol (ICMP) messages will allow the listener to move the TCB out of SYN-RECEIVED.

This scenario can be accomplished through firewall rules that either filter outgoing packets to the listener (allowing only SYNs out), or filter incoming packets so that any SYN-ACKs are discarded before reaching the local TCP processing code.

When detected, this type of attack is very easy to defend against, because a simple firewall rule to block packets with the attacker's source IP address is all that is needed. This defense behavior can be automated, and such functions are available in off-the-shelf reactive firewalls. In the past, comparatively simple, single-source DoS attacks were successful in bringing down Web servers; however, these types of DoS attacks rarely occur anymore. There are many reasons for this trend. Currently, Web servers are very powerful machines with large amounts of disk storage and processing capacity. Moreover, the bandwidth employed by modern-day Web servers is large compared to that of the past. Thus, it has become increasingly difficult for a single attacking computer to bring down a well-provisioned Web server; hence, the need for multiple sources.

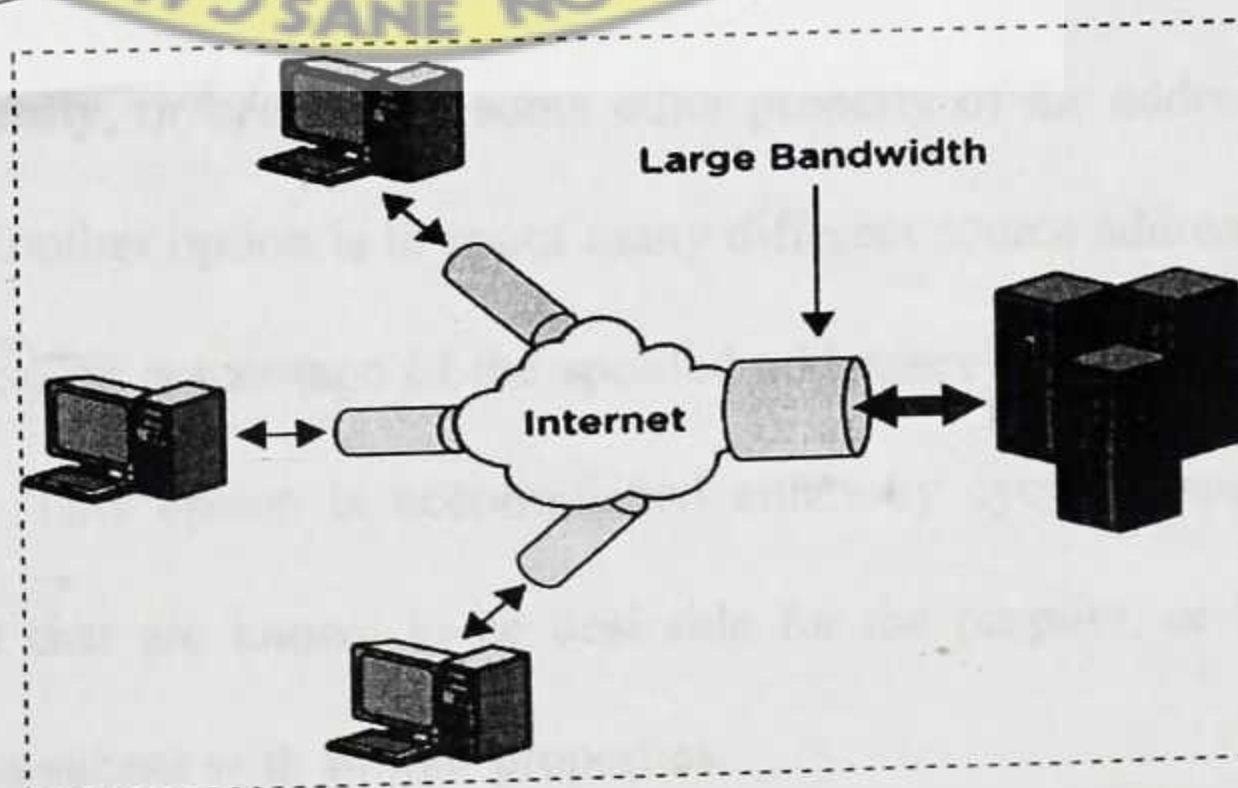


Figure 2.4 Internet Bandwidth

Spoofing-Based Attacks are another form of SYN flooding attacks that uses IP address spoofing, which might be considered more complex than the method used in a direct attack, in that instead of merely manipulating local firewall rules, the attacker also needs to be able to form and inject raw IP packets with valid IP and TCP headers.

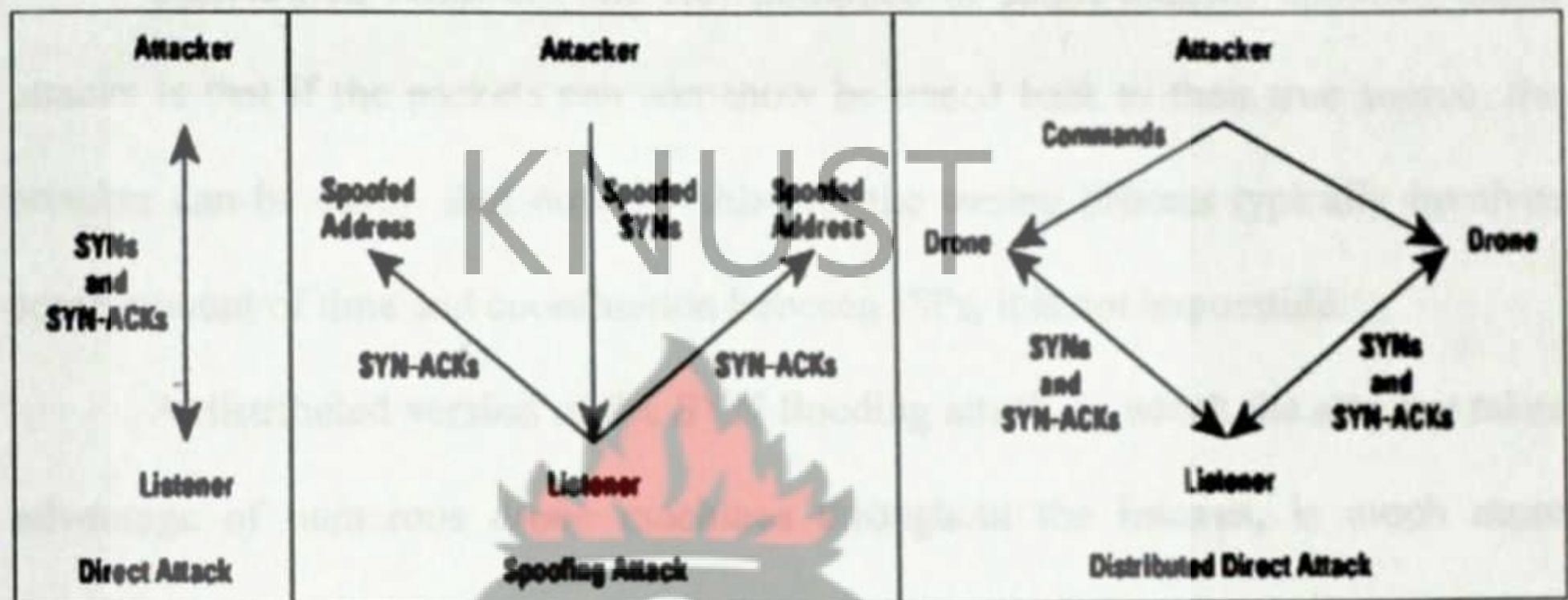


Figure 2.5: Some Variants of the Basic Attack (Source: Cisco.com - Defenses Against TCP SYN Flooding Attacks)

For spoofing attacks, a primary consideration is address selection. If the attack is to succeed, the machines at the spoofed source addresses must not respond to the SYN-ACKs that are sent to them in any way.

A very simple attacker might spoof only a single source address that it knows will not respond to the SYN-ACKs, either because no machine physically exists at the address presently, or because of some other property of the address or network configuration. Another option is to spoof many different source addresses, under the assumption that some percentage of the spoofed addresses will be un-respondent to the SYN-ACKs. This option is accomplished either by cycling through a list of source addresses that are known to be desirable for the purpose, or by generating addresses inside a subnet with similar properties.

If only a single source address is repetitively spoofed, this address is easy for the listener to detect and filter. In most cases a larger list of source addresses is used to make defense more difficult. In this case, the best defense is to block the spoofed packets as close to their source as possible.

Distributed Attacks -The real limitation of single-attacker spoofing-based attacks is that if the packets can somehow be traced back to their true source, the attacker can be easily shut down. Although the tracing process typically involves some amount of time and coordination between ISPs, it is not impossible.

A distributed version of the SYN flooding attack, in which the attacker takes advantage of numerous drone machines throughout the Internet, is much more difficult to stop. In the case shown in Figure 2.5 above, the drones use direct attacks, but to increase the effectiveness even further, each drone could use a spoofing attack and multiple spoofed addresses.

Currently, distributed attacks are feasible because there are several "botnets" or "drone armies" of thousands of compromised machines that are used by criminals for DoS attacks. Because drone machines are constantly added or removed from the armies and can change their IP addresses or connectivity, it is quite challenging to block these attacks.

2.5.2 Attack Parameters

Regardless of the method of attack, SYN flooding can be tuned to use fewer packets than a brute-force DoS attack that simply clogs the target network by sending a high volume of packets. This tuning is accomplished with some knowledge of the

listener's operating system, such as the size of the backlog that is used, and how long it keeps TCBs in SYN-RECEIVED before timing out and reaping them. For instance, the attacker can minimally send a quick flight of some number of SYNs exactly equal to the backlog, and repeat this process periodically as TCBs are reclaimed in order to keep a listener unavailable perpetually.

Default backlogs of 1024 are configured on some recent operating systems, but many machines on the Internet are configured with backlogs of 128 or fewer. A common threshold for re-transmission of the SYN-ACK is 5, with the timeout between successive attempts doubled, and an initial timeout of 3 seconds, yielding 189 seconds between the time when the first SYN-ACK is sent and the time when the TCB can be reclaimed.

With a backlog of 128 and an attacker generates 40-byte SYN segments (with a 20-byte TCP header plus a 20-byte IP header), the attacker has to send only 5.12 kilobytes (at the IP layer) in order to fill the backlog. Repeated every 189 seconds, this process gives an average data rate of only 27 bytes per second (easily achievable even over dialup links). This data rate is in stark contrast to DoS attacks that rely on sending many megabits per second of attack traffic.

Even if a backlog of 2048 is used, the required data rate is only 433 bytes per second, so it is clear that the ease of attack scales along with increases to the backlog—and more sophisticated defenses are needed.

2.5.3 Example of DDoS Tools

It has become easy to implement DDoS attack as lots of automated tools are now available. To scan and propagate among vulnerable hosts, DDoS attackers install attack tools on the compromised hosts and use them as the attacking machines. Some of the most common tools are:

- **Stacheldraht** is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.
- **Trinoo** (Mirkovic & Reiher, 2004; Dittrich, 1999) can be used to launch a coordinated UDP flooding attack against target system. Trinoo deploys master/slave architecture in which a source attacker controls a number of Trinoo master machines. The machines can't be taken over by any other machine as both master and slave are password protected. Wintrinoo is a Windows version of trinoo that was first reported to CERT on Feb 16, 2000.
- **TFN** (Dittrich, 1999) can implement Smurf (Huegen, 2000; Azrina & Othman, n.d.), SYN Flood (Schuba et al., 1997; Farrow, n.d.; CERT Advisory, 1996), UDP Flood (Azrina & Othman, n.d.), and ICMP Flood (Azrina & Othman, n.d.; Papadopoulos et al., 2003) attacks. It uses a command line interface via ICMP echo reply packets to communicate between the attack source and the control master program.

- **TFN2K** (Douligeris & Mitrokotsa, 2004; Barlow & Thrower, 2000; CERT Coordination Centre, 1999) a more advanced version of TFN network which uses key-based CAST-256 algorithm for en-cryption between master and slave communication. It uses TCP, UDP, ICMP, or all three for communication. TFN2K can implement Smurf, SYN, UDP, and ICMP Flood attacks.
- **Shaft** (Dietrich, Long, & Dittrich, 2000) It works like Trinoo but the communication is done through ports. Thus, it has ability to switch control master servers and ports in real time. Communication is achieved using UDP packets. Shaft can implement UDP, ICMP, and TCP flooding attack.
- **Mstream** (Dittrich et al., 2000) It attacks target machine with a TCP ACK flood by using TCP and UDP packet communication. Communication is not encrypted and the master connects via telnet to zombie. Masters can be controlled remotely by one or more attackers using a password protected interactive login.
- **Trinity** (Hancock, 2000; Marchesseau, 2000) is an IRC based DDoS attack tool. It can implement UDP, IP fragment, TCP SYN, TCP RST, TCP ACK, and other flooding attacks. Each trinity compromised machine joins a specified IRC channel and waits for commands. It uses IRC service for communication between attacker and agents.

2.6 Current DDoS Solutions And Reasons For Their Failure

Currently, online organizations installed devices such as routers, firewalls and Intrusion Detection Systems (IDS) to secure their websites. Yet, while these solutions protect enterprises from many forms of attacks, none was designed to defend against DDoS attacks and therefore, they exhibit serious limitations when faced with a state-of-the-art DDoS attack.

2.6.1 Routers

Modern networks require many types of routers, including Layer 3 & 7 routers that service specific internet connections and Layer 4 switches that serve the outer edge of the network. All of these routers analyze incoming and outgoing traffic and route it to its intended destination. In the process, routers provide filtering that protects against simple attacks, such as ping attacks.

However, routers are not effective at mitigating most DDoS attacks especially unable to process the millions of packets-per-second that characterize a standard DDoS attack. When attacked, the line cards in a vulnerable router can fail and take the entire router offline. Most routers must be manually configured to stop even simple attacks - something usually performed only after an attack has taken down a site.

Furthermore, most DDoS attacks today use valid protocols and spoof valid IP address spaces that are essential for internet operations, rendering protocol and IP address filtering useless. However, the enormous packet flows seen in DDoS attacks can overload a router's CPU and cause it to fail. Even if the router remains operational, legitimate traffic will be limited as well.

2.6.2 Firewalls

The next line of defence - Firewall, basically reside in Layer 5. A firewall separates a trusted environment, such as a corporate intranet, from an untrusted environment, such as the Internet, and regulates traffic to limit access to the trusted environment to users with proper authorization.

Firewalls however mitigate many types of attacks, including certain known worms, malicious URLs, and man-in-the-middle attacks but are not really designed to protect services that are available to the public over the internet and are thus unable to guard against DDoS attacks.

2.6.3 Intrusion Detection System (IDS)

Intrusion detection systems (IDS) are solutions designed specifically to analyze traffic, detect and identify attacks. While such information helps companies respond more quickly to an attack, these solutions are unable to mitigate attacks. Further, because IDS examines nearly every packet, the sheer volume of DDoS attacks can cause IDS systems to fail.

Unfortunately, all the above solutions suffer from performance limitations. After hardware devices reach their limits, they allow “attack leakage” back onto the system, hurting the network. Modifying these solutions to add capacity is a slow process that can take days to years - far slower than the rate at which attack sizes are increasing. Networks themselves can also be a bottleneck. Should a high packet per second DDoS attack cause a network or upstream router to fail, the network can crash before the mitigation hardware has a chance to do its job.

2.7 Motivations For DDoS

It is normally difficult to understand the motivation or goals behind specific DDoS attacks or why they occur. Because the machines or computers performing the attack are being controlled by some hidden external source, it is difficult to pinpoint the origin of the attack. When it is already hard to find out *who* are conducting the attacks, it is even harder to understand *why*. Therefore, many explanations of why DDoS occurs are theories based on speculation or small amounts of evidence.

Government websites are a common target for DDoS. Naturally, one can assume that there are some people, organizations or even other governments that do not support this government, and utilize DDoS as a form of cyber warfare to attack this government. Examples include the DDoS attacks against government websites owned by Russia, Georgia, United States, and South Korea.

For sure, politics is involved in these DDoS attacks and is what motivates them, but it is unclear who is performing the attacks. Regular Internet users may attempt to attack a large company's website simply because they can. Being able to take down a large company or organization's website can be enticing to the average, insignificant computer user. With the amount of information and resources available on the Internet, it may even be possible for a user with little technical knowledge to download and run a simple script that performs a DDoS attack. It is now even easier to perform an attack using DDoS as can be seen in Figure 2.6

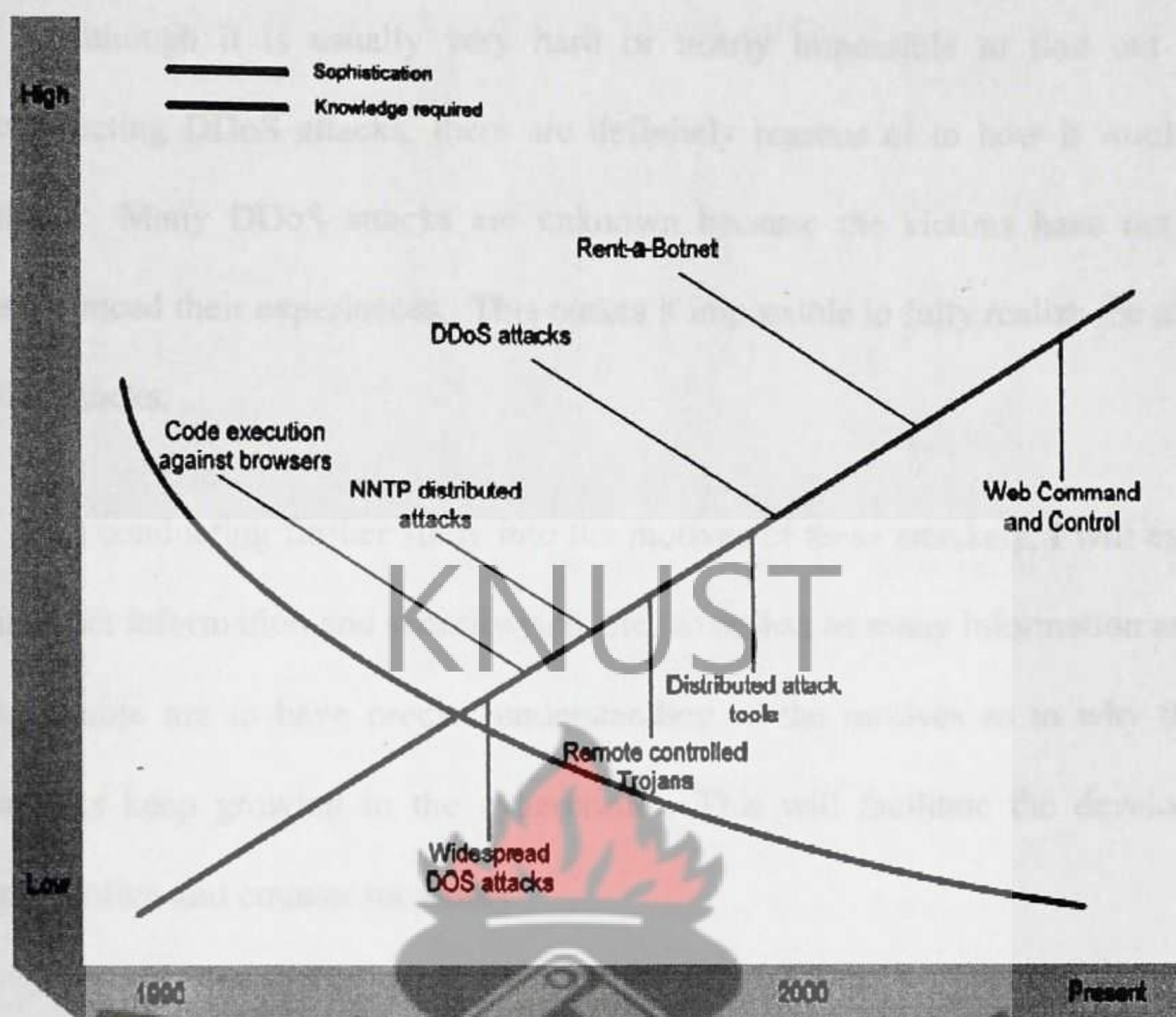


Figure. 2.6: Timeline For Evolution of DDoS Attacks (Source: iDefence)

Some theories state that company websites under attack are being attacked by competing companies. This can disrupt or damage the target company's services, which may very well boost the sales or amount of website views for the competing company.

Small disruptions or downtime can translate to thousands of dollars lost for companies that conduct most of their business online, so there are definitely huge gains for a competing company performing DDoS attacks (or losses, in the case of the site being attacked). Apparently, DDoS attacks are very common in online gambling websites, where supposedly competing websites constantly DDoS each other.

Although it is usually very hard or nearly impossible to find out who are conducting DDoS attacks, there are definitely reasons as to how it would benefit them. Many DDoS attacks are unknown because the victims have not publicly announced their experiences. This makes it impossible to fully realize the motives of the attacks.

In conducting further study into the motives of these attackers, I will explore the internet information and security web sites to collect as many information as possible to enable me to have precise understanding of the motives as to why the DDoS attacks keep growing in the cybercrimes. This will facilitate the development of preventive and counter measures.

2.8 Financial Impacts Of DDoS

The impacts of DDoS attacks can be many and varied and can have immense direct financial consequences but typically the intangible ramifications outweigh the monetary. This might be typical of a small and emerging economy like Ghana's.

In 2005 an Australian Computer Crime and Security Survey found that Only 14 per cent [of respondent companies] reported experiencing Denial of Service (DoS) attacks which resulted in financial losses which accounted for about 53 per cent of total losses reported by survey respondents (nearly \$9 million).

Even though, during the survey period one institution reported losses due DDoS attack of \$8 million, if this figure is excluded, more typical average losses hovers around \$70,000 (ausCERT, 2005) as can be seen in Figure 2.7 below.

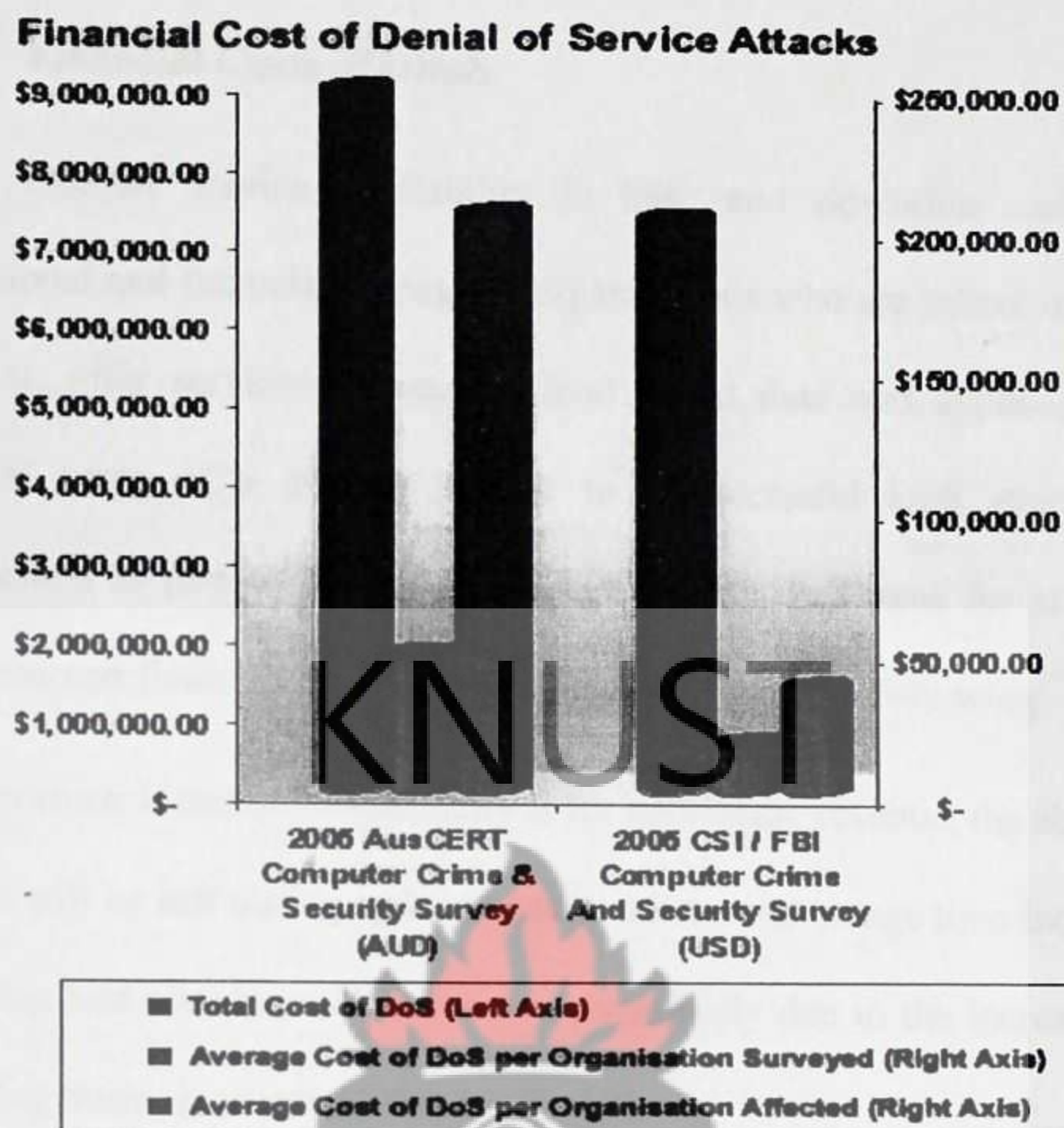


Figure 2.7: Financial Cost of DoS (Source: ausCERT, 2005)

This illustrates that despite the limited likelihood of DDoS, a single occurrence may have catastrophic consequences. Furthermore, many DDoS incidents are never reported nor their impact qualified as direct financial loss.

Unfortunately, data on DDoS attacks which indirectly impact organisations relying on shared infrastructure is unavailable. For example, many organisations suffer the consequences of spam emails which cause immense volumes of DNS traffic, impacting DNS servers which are used by many customers of ISPs.

2.8.1 Financial Costs of DDoS

Internet service availability is key, and downtime can cause significant reputational and financial damage to organisations who are reliant on the Internet to sell products, offer services or access cloud based data and applications. The potential financial costs of a disaster similar to a successful DoS attack may already be documented as part of a business impact analysis in Ghana for any company but the most common financial costs of DDoS would include the following:

Lost revenue: If online functionality is for generating revenue, the ability to generate that revenue will be lost during system unavailability. As outage time increases linearly, it is likely that lost revenue will increase exponentially due to the increasing customer base (including business partners) that is affected.

Contractual violations: Disruptions in service often hamper the ability of organisations to meet Service Level Agreements (SLAs) which often carry monetary penalties especially B2Bs.

Litigation costs: There are various situations under which the target of an attack may face litigation, including failing to provide a service or causing damage to a third party.

Service provider expenses: Telcos are likely to be engaged in detection, reaction, and analysis of DoS attacks and may charge the client organisation for these additional services. Excess bandwidth usage is the responsibility of the subscriber.

Incident handling and recovery costs: As the target organisation recovers from an incident, human resources must be employed to analyse the attack and restore services. Costs are incurred in the redirection of these resources from their normal tasks.

Stock price fluctuations: In the event business critical services are interrupted for substantial periods of time, the business impact may produce investor uncertainty.

2.8.2 Intangible Consequences of DDoS

Intangible costs of DDoS often do not receive as much attention when conducting risk analysis. However, the below list demonstrates such costs are an integral part of the full impacts of such an attack especially in comparison to the GDP of a Country like Ghana.

Third-party damage: As discussed above, if an attack is targeted at one organisation it may impact others through shared infrastructure. Insecure machines in an organisation's network also may be used to attack other organisations.

Morale: Employees are motivated when they are able to work efficiently and without interruption. Continual outages may become a burden to those who feel they are unable to complete assigned tasks.

Lost productivity: If critical systems are inaccessible, valuable time may be lost in completing work-related assignments.

Brand damage: Today's information economy relies on the ability to access resources on demand. Downtime can therefore have long-term impacts, particularly on those organisations which provide public services, gain competitive advantage through reliability, or where customer loyalty is easily swayed.

Human costs: Included among critical infrastructure organisations are law enforcement, health, utility and emergency services. Any disruption to these services may also result in injury or loss of life.

E-commerce credibility: Prolonged and sustained attacks against critical infrastructure entities and organisations with a high-visibility presence on the Internet may degrade consumer confidence in e-commerce. Damage to the credibility of these systems may have an economy-wide impact.

2.9 DDoS Threats to an Economy

The true danger of cyber-attack is that, as technology advances and critical infrastructure becomes more dependent on computer networking for its operations, these systems become more vulnerable to threats of operational failures. These threats can present costly downtime for these industries and negatively impact the economy.

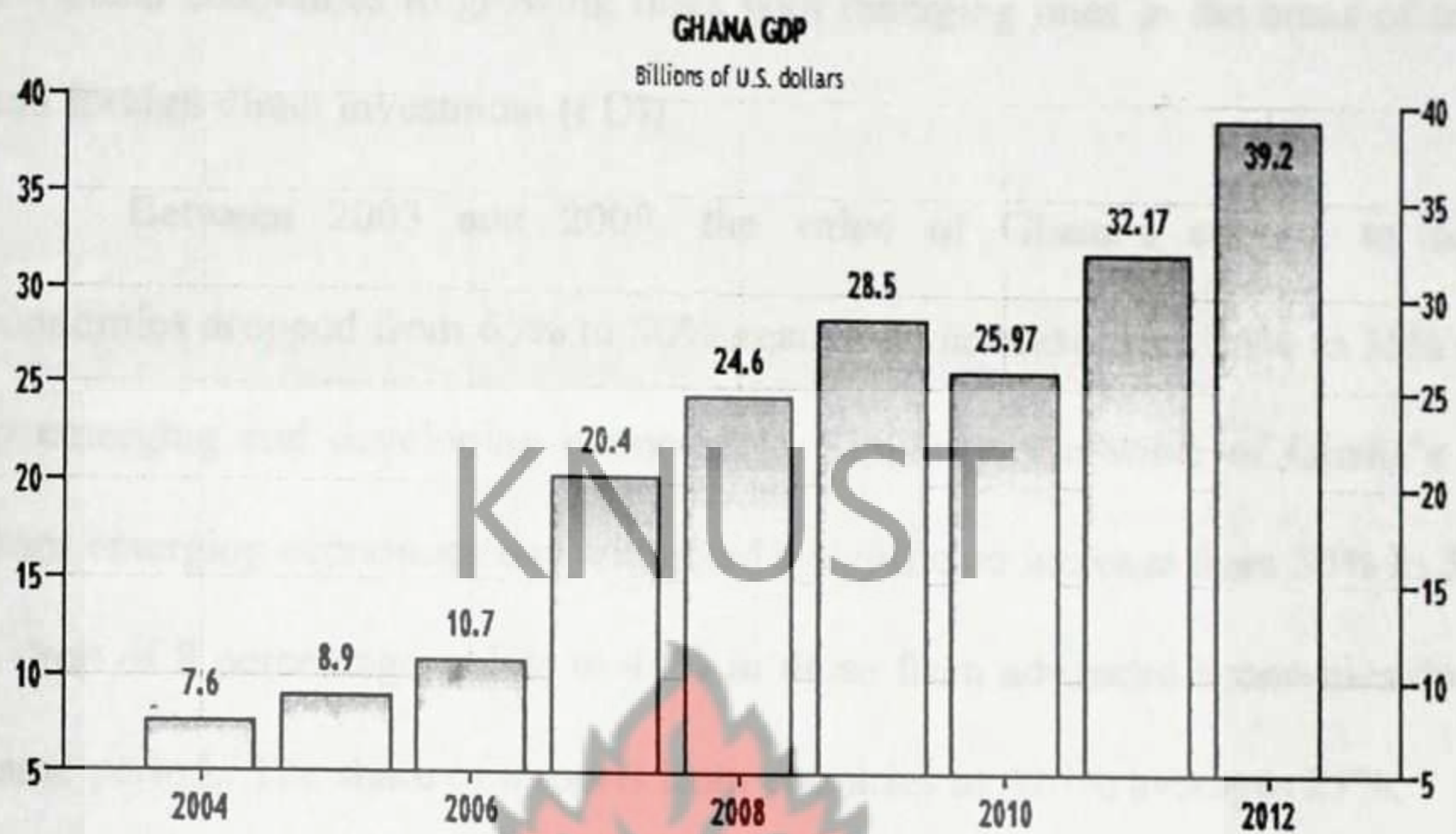
DDoS attacks are a potent, a relatively known but new type of Internet attack which have caused some biggest web sites on the world - owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon – to become inaccessible to customers, partners, and users, sometimes for up to twenty-four hours; some web sites have experienced several days of downtime while trying to restore services, the financial losses are very huge.

Financial loss is an expected effect of any significantly degradation of Internet performance or online business transactions. Furthermore, financial loss changes over time. Economic damage usually has not the same characteristics over time as technical problems have. Economic damage can still grow when technical problems have been resolved and the attack has stopped.

2.9.1 Ghana's Emerging Economy

The Gross Domestic Product (GDP) in Ghana was worth 39.20 billion US dollars in 2011. The GDP value of Ghana represents 0.06 percent of the world economy. Historically, from 1960 until 2011, Ghana GDP averaged 7.16 USD Billion reaching an all-time high of 39.20 USD Billion in December of 2011 and a record low of 1.20 USD Billion in December of 1960. The gross domestic product (GDP) measures of national income and output for a given country's economy.

The gross domestic product (GDP) is equal to the total expenditures for all final goods and services produced within the country in a stipulated period of time.



(Source: www.tradingeconomics.com)

Ghana has however rebased its national accounts, changing the base year from 1993 to 2006. According to the national authorities, following the rebasing, the size of the economy in real Gross Domestic Product (GDP) terms has been raised three fold and placed Ghana among the lower middle income group of countries.

Economic growth has remained strong with real GDP growth reaching an estimated 5.9% in 2010 compared to 4.7% in 2009. Growth prospects are even brighter as real GDP growth of 12.0% and about 11.0% are projected for 2011 and 2012 respectively, largely on account of the start of oil production in commercial quantities in December 2010. In addition, the country's increasingly democratic settlement and social stability have served to boost the confidence of investors, leading to rising investment in IT infrastructure.

According to African Economy Outlook, Ghana's economic relations with the rest of the world have seen a remarkable shift in recent times from close ties with advanced economies to growing links with emerging ones in the areas of trade, aid and foreign direct investment (FDI).

Between 2003 and 2009, the value of Ghana's exports to advanced economies dropped from 65% to 50% against an increase from 25% to 36% in those to emerging and developing economies. Similarly, the value of Ghana's imports from emerging economies has witnessed a significant increase from 50% to 59% and a drop of 8 percentage points to 40% in those from advanced economies during the same period. The share of imports from countries in Africa averages 25%.

The report goes on to state that, during the past decade the destination of Ghana's exports has increasingly shifted away from countries such as the United States, Belgium, France, Germany and Japan to India, Malaysia, Mongolia and Ukraine. At the same time, imports from India, China, Brazil, Nigeria and Côte d'Ivoire have risen considerably while those from the United Kingdom, the United States, Belgium and France have either stagnated or declined.

The major increase in imports value from emerging economies came from China which saw an increase in exports to Ghana from USD 354.2 million in 2003 to USD 1.78 billion in 2009 resulting in a rise in China's share of total import value to Ghana from 9% to 17%.

Furthermore, the report analysis on Ghana's investment prowess shows that in the area of investment, Britain remains the main source of FDI inflows (excluding mining) in terms of value of investment, accounting for about 37% of total FDI to Ghana between 1994 and 2009, followed by the United States, the United Arab Emirates, Nigeria, Malaysia and China in that order.

China, however, leads in the number of registered projects with 415 projects mainly in manufacturing and general trade. India comes next with 388 projects, mainly in the area of manufacturing, followed by Lebanon with 291 projects. In 2007 China ranked second to Britain in terms of value of FDI, indicating the increasing presence of China in Ghana's FDI. India is one of the top five foreign direct investors in Ghana (KPMG, 2012)

In 2010 Indian investments in Ghana included over 46 projects with an estimated total value of USD 277 million. In addition, within the health sector, Ghanaian pharmaceutical companies manufacture drugs in collaboration with Indian firms. Recently, Ghana's financial sector has attracted Indian investment. In 2010 the Indian Bank of Baroda opened a branch in Ghana (KPMG, 2012)

2.9.2 Telecoms Contribution To Ghana's Economy Vis-à-vis GDP

The Governments' proactive policy and regulatory interventions, combined with support from the World Bank Group and other development partners, has resulted in a competitive and vibrant industry.

As at December 2010, the telecommunications sub-sector had 2 fixed line operators plus 6 mobile cellular operators authorized to operate. Out of these, the 2 two fixed line operators and 5 of the mobile cellular operators were operational. Out of 84 Internet Service Providers (ISPs) authorized, 29 were in operation. The Sector also witnessed 18 DTH Satellite Service providers, 135 Data Operators, 65 Public/Corporate Data operators, 215 FM Stations and 48 TV Stations having authorizations to operate with 15, 60, 40, 185 and 15 of them respectively actually being in operation as seen in the Table 1.1 (KPMG, 2012)

	Category	No. Authorised	No. Operating
1	National fixed network operators	2	2
2	National Mobile cellular operators	6	5
3	Direct to Home (DTH) Satellite Services	18	15
4	Internet Service Data Providers	84	39
5	VSAT Data Operators	135	60
6	Public/Cooperate Data Operators	65	40
7	FM Stations	215	185
8	TV Stations	48	9 free-to-air 6 pay/view

Table1.1 Operators and Service Providers 2010 (Source: gipcghana.com)

A third party report, which gives an overview of the contribution of the telecom industry to Ghana's economy indicates in 2010 alone, telecom operators paid GHC598 million in taxes and levies, representing 10% of government income for that year. The report noted that market leader MTN alone paid a whopping GHC415 million, being 6.94% of government income for 2010, and 69.4% of taxes and levies from the telecom industry.

The telecom sector alone represents 7.0% of all investments in Ghana (5.1% from MTN alone) and is responsible for 2.0% of Gross Domestic Product (1.4% from MTN alone), while the sector also takes some 5.3 per cent of the total expenditure of consumers (MTN alone taking 3.6%). Meanwhile, as subscribers increase and mobile penetration goes up, average revenue per user – ARPU - (what telecom operators derive from each subscriber per month) decreased consistently from GHC14.6 a month, when penetration was 50%, to GHC9.4 when penetration rose to 67%. Currently, mobile penetration is above 80% and ARPU has dropped further to about \$3, and even though the operational costs of telecom operators keep going up with every passing day, the players keep absorbing inflationary trends on behalf of customers.

In July 2011, for instance, inflation on transport cost was 23.25%, on goods and services – 18.27%; on clothing and footwear – 13.78%; on beverages, narcotics and tobacco – 13.25%; furnishing/household equipment – 13.05%; hotels/cafes and restaurants – 11.91%; health – 8.15%; recreation and culture – 6.32%; housing, water, electricity, gas – 6.15%; food and non-alcoholic beverage – 3.25; education – 2.25% inflations, but for communication, inflation was zero, even though operational cost for telecoms went up.

According to the report the telecom industry has been transferring efficiency gains to the customer in clear contrast to other industries in Ghana. The telecom operators, for instance absorbed the communications service tax (talk tax) on behalf of customers, and they also absorb several exorbitant and arbitrary levies and charges by MMDAs on the installation of necessary infrastructure to provide service to communities.

The report also noted that for instance, the cost of mobile communication in Ghana, is one of the lowest in the world, and that has driven economic growth in the country to a large extent. Ghana has the 15th lowest cost for mobile communication on a list of 50 countries listed in a Nokia TCO (total cost of ownership) study in 2011 – and this included tariffs, taxes, and cost of handset.

Meanwhile, Telco operators also contribute one per cent each of their profits to the Ghana Investment Fund for Electronic Communications (GIFEC) mainly to extend co-located infrastructure to deprived areas. On the basis of these, telecom operators have been negotiating to get some of the arbitrary levies, fees and charges by MMDAs and some government agencies to be reduced so the operators can rather channel the resources into extending services to deprived areas.

This is in line with a most recent call by International Telecommunications Union (ITU) Secretary-General, Dr. Hamadoun Troure for some of those taxes, levies, fees and charges to be completely abolished to enable telecom operators and the ICT sector to contribute effectively to national development. (*myjoyonline.com, August 12, 2011, 23:22 GMT*)

2.9.3 Ghana's E-Commerce Readiness

Online business transactions open up many opportunities for emerging economy like that of Ghana, where ICT infrastructure is readily offering the private sector a safe and confidence trading environ for international trade and profit maximization. At the same time, it is also the lion's den for cyber-crimes that value way beyond USD250 million annually as in the case of United States (CNN, 2004).

The cost of Internet in Ghana has gone down and capacity has gone up by 65 times (GISPA, 2012) and the entry of two international bandwidth providers pushed the cost of Internet access in the country significantly downwards, and also resulted in enhanced internet-user experience (B&FT,2012).

The report indicated that, about 18 months ago Internet Service Providers (ISPs) bought E1 bandwidth for US\$4,500 but now buy the same bandwidth capacity at less than US\$1,000, which Internet providers expect to further fall as competition from other carriers such as the West Africa Cable System (WACS) – GLO has become operational and expected to be available for use throughout the country.

According to the two giant ISPs (Busy Internet and Internet Solutions), though the retail price of Internet access has not gone down in comparison to the percentage decline in wholesale price, Internet users are now having improved experience from Internet usage and more value for their money.

They also argued that the reduction in wholesale pricing has affected the retail pricing of Internet services to a considerable extent. Though prices have reduced, it is not as low as previously touted or expected due to the lack of adequate or extensive last-mile infrastructure in-country to link the capacity to the client site.

Thus, Service providers therefore have to incur additional excessive costs to provision last-mile infrastructure via fibre or wireless to enable clients' access. All of these recent improvements in the face of the recent oil discovery and Ghana's economy facilitate Ghana's readiness for e-commerce and e-business.

Ghana was ranked **number one** in Africa as the country with the highest Internet speed, according to a global internet speed report released March 5, 2012 by US-based, Ookla. Ookla is the global leader in broadband testing and web-based network diagnostic applications, and its report was based on millions of recent test results from Speedtest.net. Its Net Index compares and ranks consumer download speeds around the globe, and **reported** Ghana had an average broadband speed of 5.13 megabits per second.

The results for Ghana were obtained by analyzing test data between Feb 10, 2012 and Mar 14, 2012; tests from 31,183 unique IPs have been taken in Accra, and of 182,596 total tests, 10,624 were used for the current Index. According to the index, Ghana beat Kenya to second place with 4.49Mbps, South Africa to sixth place with 2.98Mbps, and near-by Nigeria to the eighth place in Africa with 2.3Mbps. Morocco, Angola, Tunisia, Zimbabwe, Rwanda, and Libya were all in the top ten, but obviously behind Ghana. (Ghanaweb.com, 2012)

Between the telecom operators in Ghana, professed broadband speeds range from 3.1Mbps (Expresso) to 14.4Mbps (Vodafone). But the index reported Ghana Telecom (Vodafone) had 6.13 Mbps, as per consumer experience; Zipnet/Broadband Home Ltd had 2.02 Mbps, and Scancom Limited (MTN) has 1.51 Mbps, and they constituted the major Internet service providers (ISPs) in country. Obviously, Vodafone has maintained its position from 2011 as the network with the highest internet speeds in Ghana. (Joyfm, 2012)

KNUST

2.9.4 Trade Partners

Ghana's trade partners are actively operators of e-commerce and e-business. From United States through Europe, Ghana shares export and import trade relationships. The major influence of Ghana's readiness is relationship with both China and India, both from Asia.

China is known of her widely use of ICT to promote trade and business, thereby dominating world trade and business environment. The country's influence or presence in Ghana is deepening Ghana's drive into e-business and e-commerce over the face of the internet (Ekow Quandzie, 2011).

India is known to be active in international trade and e-commerce. In 2009, India's e-Commerce industry was on the growth curve and experiencing a spurt in growth. It reported that the global revival of e-Commerce was having a ripple effect in India too where the B2B (Business to Business), B2C (Business to Consumer), C2C (Consumer to Consumer), G2B (Government to Business) and G2C (Government to Citizens) segments are showing rapidly increasing activity over the past few years (India Reports, 2009).

India's presence in Ghana may mean a strategic business relationship rather than exploitation. This means that, much of goods and services would not only exchange in trade relationship with Ghana, but much from participatory knowledge sharing and experience in ICT.

Evidence of experience sharing between India and Ghana is the Ghana-India Kofi Annan Centre of Excellence in ICT, Ghana's first Advanced Information Technology Institute working to stimulate the growth of the ICT Sector in ECOWAS.

Established in 2003, through a partnership between the Government of Ghana and the Government of India, this state-of-the-art facility provides a dynamic environment for innovation, teaching and learning as well as practical research on the application of ICT4D in Africa (AITI, 2009). The centre works with institutions located in six continents, Africa, Asia, Australia, Latin America, Europe and the United States.

A public sector institution run on private sector lines with a strong emphasis on social development, AITI-KACE represents the best in modern service delivery models. The AITI-KACE's Technology Transformation Seminars (TTS) are making an impact on the ICT sector in Ghana. These give stakeholders a platform to share experiences and technical know-how (AITI, 2009).

2.9.5 Current Infrastructure

The way businesses used to operate and daily lives were lead has in this modern times changed due to the advances in networks and by the way in which we all communicate. The Internet and E-mail services nowadays are being used to a much greater extent.

Ghana currently have 28 Banks, 43 Non-Bank financial institutions and 135 Rural Banks and most offer online banking including money transfers and account payments. Whiles the some schools and Universities are also allowing online registration, studying and written examinations, retailers double profits through online purchases. Families overseas can stay in touch with loved ones in Ghana on a daily basis via online chat facilities like Skype etc.

The problem is, there are loads of vulnerable systems especially in Africa connected to the Internet and any or all of these can be used as a launch pad for Distributed Denial-of-Service attacks, the effects of which could be devastating. The Internet is essentially a chain of networks and therefore only as strong as its weakest link. Distributed Denial-of-Service attacks are becoming extremely popular and common due to the effectiveness of this type of attack and the fact that the attackers are well hidden, therefore seldom caught.

Over time, the systems used by providers of Ghanaian critical infrastructure services have become increasingly interconnected. As this interdependence has grown, exposure to Denial of Service threats has increased, creating a need for best practice protection strategies in the area. Ghana has been recognized by the

International Telecommunication Union (ITU) to be among the countries with the highest growing telecommunication sector as seen in Figure 2 below.

Infrastructure development growth rate has been phenomenal over the years and this can be attributed to the country's good governance and the enabling policies as well as legislature introduced over the years (Iddrisu, 2010).

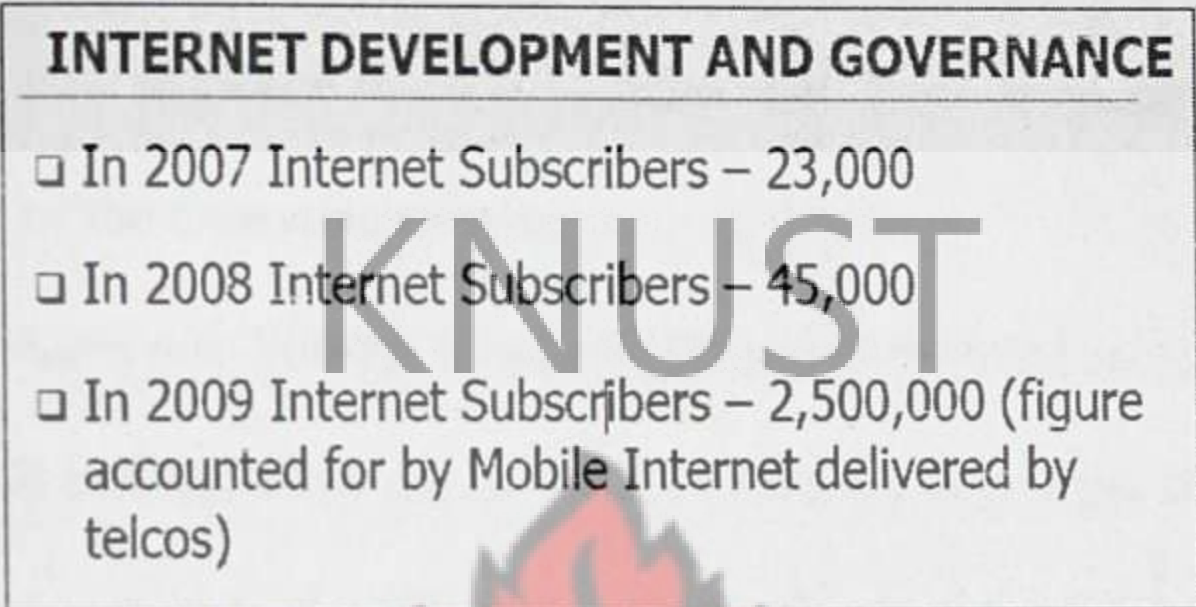


Figure 2.8: Internet Development and Governance (source: ITU, 2000)

With the framework of the government's development agenda to provide transparent and accountable governance, strong economy for real jobs, investing in people and expanding infrastructure for growth, the Ministry is situating ICT to provide the needed tools for good governance and support all activities of various sectors of the economy especially entrepreneurship. (Iddrisu, 2010).

In line with this objective, it has facilitated the existence of a resilient and advanced technology platform upon which solutions and strategies will be delivered to expand and improve education, health delivery, banking and agriculture, among others.

On the E-Government Network Infrastructure Development and to promote the use of ICT in governance, the Ministry of Communication has commenced the implementation of the E-government infrastructure project to provide a national

network for networking Ministries, Department, Municipal and District Assemblies as well as other public sector organizations.

To better the situation, efforts have been made to provide a universal, ever-present, unbiased and affordable access to ICT infrastructure services in Ghana. Honourable Haruna Iddrisu, however, entreated all stakeholders to preserve in the unrelenting task to ensure that the benefits of ICT for development are made to bear on the lives of the Ghanaian citizen.

An Audience Survey Research Project conducted in Ghana in 2009 (Inter-media, 2009) indicated that out of the 23.8 million, only 4 per cent of those that were sampled had access to the internet. Also, 80 per cent of the users are aged 15-29 years and 10% had access to computers.

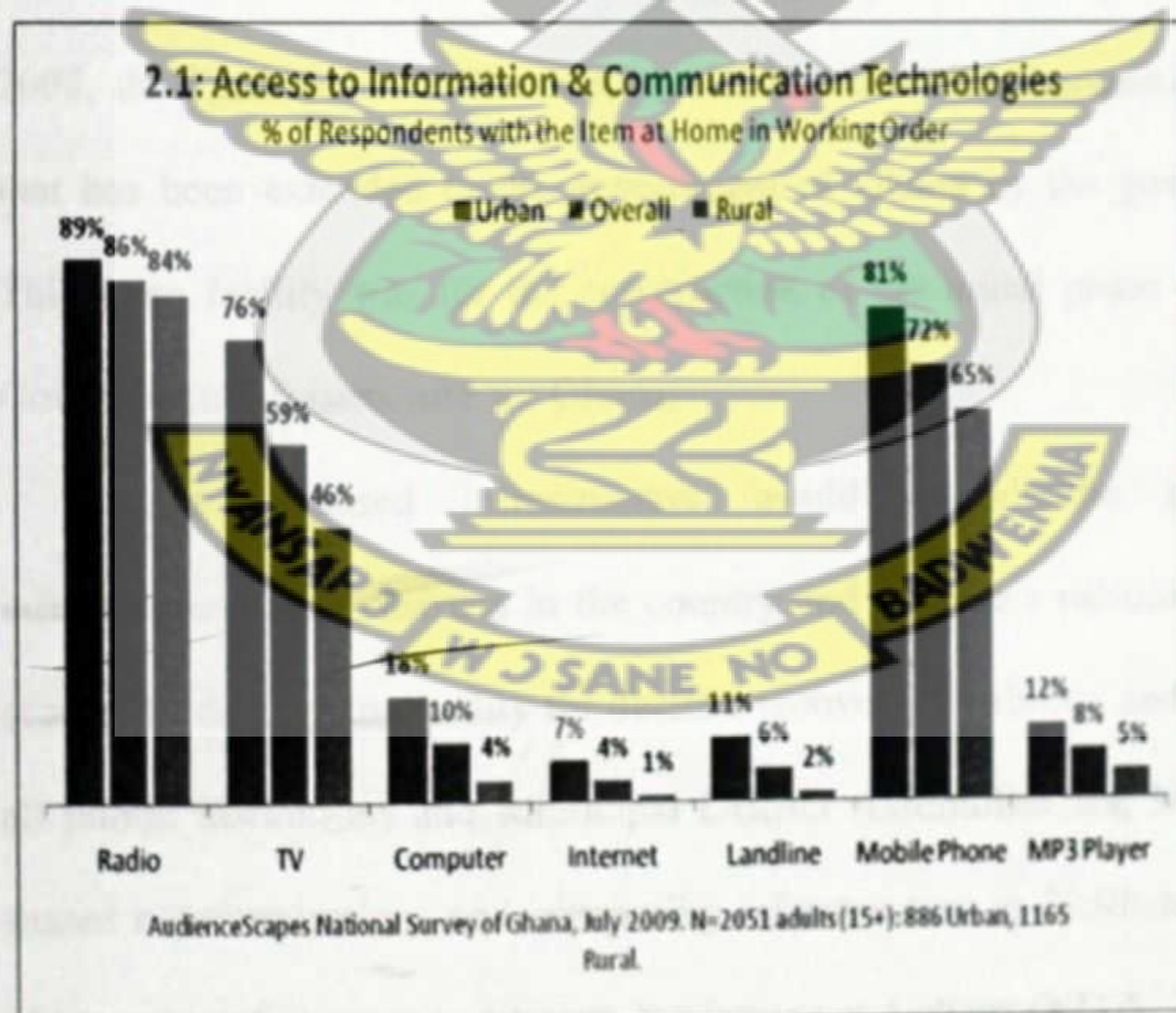


Figure 2.9 Access To ICT (Source: Inter-media, 2009)

Mobile Internet, which comes with cell phone subscriptions, offers many rural dwellers instant access to the web. Similarly, the recent mobile broadband

revolution sweeping through Ghana is welcome news as mobile telecom operators' line up their various data offerings in the competitive arena.

Mobile broadband has become the number one option for Ghanaian Internet users in both rural and urban areas. The government is also pushing its own initiatives through the introduction of the national Fiber optic cable, which would greatly boost access and reliability in the connectivity mix among rural Internet users.

Furthermore, computers and wireless Internet connections are being provided for many governmental institutions, such as schools and libraries, through the Ghana Investment Fund for Electronic Communication (GIFEC).

National Information Technology Agency (NITA), reports that in November 2008, the Parliament of Ghana approved a \$30 million concessionary loan facility that has been extended to the government of Ghana by the government of China. This Loan facility was for the construction of the initial phase of a nationwide e-Government infrastructure for Ghana.

The proposed infrastructure would extend the national backbone infrastructure to all districts in the country and provide a national data centre and a secondary data centre facility for disaster recovery capability, and ultimately connect all public institutions and Municipal District Assemblies and MMDAs to a single shared communications and computing infrastructure to facilitate effective delivery of government services to citizens, businesses and others (NITA, 2008).

Besides E-governance, almost all banking institutions in the country are wirelessly connected linking up with their head office and branches across the country. The Rural Banks are currently on ARB Apex Bank network across the country. These on-going network initiatives and infrastructure reforms in the country depict how much lost (i.e. in terms of cost) and how much damaged will be registered if all these heavily financed national developments will be subjected to threats such as DDoS attack.

2.9.6 Targets by Industry

Because of the motivations of attackers and the resources being supported by different industries, threat profiles of critical infrastructure organisations will be influenced by the industry in which they operate. The following provides an indication of the systems that could be subject to DDoS attack, within each key industry or segment.

Utilities: Utilities provide the fundamental supporting infrastructure for all other organisations in Ghana. While utilities are less susceptible to common forms of DoS and DDoS because of the use of closed networks and proprietary systems, they are at greater risk of a high-impact event. If a physical or otherwise non-network Denial of Service attack occurs, restricting access to a fundamental service such as electricity or water, could adversely impact human and organizational health. Potential targets would include:

- ✓ utility management buildings and facilities (e.g. Physical damage to a substation)
- ✓ billing systems; and
- ✓ Supervisory Control and Data Acquisitions (SCADA) systems.

Telecommunications: Telecommunications carriers may not only be the target of DDoS attacks but also the transport mechanisms for such attacks i.e., an attack on resources supplied by a carrier to another organisation may inadvertently or deliberately affect the carrier itself.

For instance, a Telecommunication supplier who provides access and bandwidth to clients can easily become a likely target for extortion and a disruption of service of a larger carrier may even cause an extensive damage to countless organisations.

Potential targets might include:

- top-level domain servers and ISP domain name servers
- core routers (public and private)
- corporate email servers
- intercontinental communications links
- billing systems and
- internet service providers

Governance: Government systems may as stated earlier be subject to DDoS attack for a wide range of political reasons. Various government bodies provide social and national services. Potential targets include

- electoral system services
- defence systems services
- Tax Systems (IRS)

Banking & Finance: Given that monetary gain is a prime DDoS motivator, banking and finance organisations are likely targets. They would be severely affected and open to extortion in the event of online services being unavailable for an extended period. Potential targets include:

- Online Banking
- Clearing systems
- Trading systems (e.g. Money transfers systems)

Transportation: Many public transportation systems are not sensitive to system-wide DDoS attacks but rather are sensitive at single points, such as traffic controller systems. However, even though Ghana's transport system is not that advanced like the developed countries, some systems are likely to be at risk because of the time sensitive services they provide. Additionally, with increased safety and security check requirements, many processes cannot be easily completed offline.

Potential targets include:

- airline ticketing systems
- Airline/control tower signalling
- security checking processes (e.g. by creating false alarms)
- shipping inventory and queuing systems and
- Customs support systems.

Health & Emergency Services: While typical motivations behind DDoS attacks suggest health and emergency services are unlikely targets in Ghana despite the NHIS, a catastrophic event may occur if the communications or database systems of health and emergency services become ineffective.

Potential targets include:

- SOS emergency reporting systems;
- patient record databases
- Dispatch processes (e.g. hoax phone calls).

Law Enforcement: Now attacks on law enforcement are basically motivated by the two least-common motivations – revenge and information warfare.

Potential targets include:

- criminal databases, and
- Law enforcement communication networks

2.9.7 Cyber Crime and Combat Readiness

Minister of Communications, Hon. Haruna Iddrisu on Monday, 3rd October 2011, issued Statement during a forum where the Ministry of Communications and its Agencies interacted with the media and the general public on the developments and progress made in the ICT sector. In his statement, he emphatically stressed on Ghana's readiness in deploying full cyber-crime counter measures and ICT infrastructure development (Iddrisu, 2011).

Ghana Government is to set up an emergency Cyber Crime Response Team, to review existing legislature governing the Information and Communication Technology (ICT) activities and strengthen the country's cyber security. The Communication Minister expressed concern that Ghana is ranked among the world's top 10 countries in cyber-crime because of sakawa and other related online crimes and added that it is a disincentive to investment in the country's ICT sector.

He further expressed worry that use of credit cards in the country is restricted because of the growing incidence of cyber fraud popularly termed *sakawa*, adding that the act is endangering the safety, use and growth of ICT in Ghana (Iddrisu, 2011). Speaking on the possible negative social impact of cyber-crime at the same forum, The Minister further stated that the Ministry will monitor and facilitate the development of the following bills;

- Electronic Signature Regulations,
- Electronic Investigations & Interception Regulations,
- he Electronic Payment Medium Regulations,
- Quality of Service Regulation and
- Electronic Regulation on Dumping of Electronic Waste to address issues relating to the increasing cyber-crimes in the country.

He said the Data Protection Bill is already before Parliament. The Minister also stressed on Provision of Modern ICT Infrastructure for Growth. He said that the Ministry, through the National Information Technology Agency (NITA) has commenced the implementation of the e-Government infrastructure project that will provide a national network for the networking of Ministries, Departments, Metropolitan, Municipal and District Assemblies and other Public Sector Organisations, and also extend broadband to the District Assembly areas.

To enable the efficient delivery of converged ICT services for development, the Ministry is implementing the e-Government infrastructure project under the cooperation agreement with the Government of China. The focus is to extend fibre optic infrastructure to all district capitals and provide broadband capacity to facilitate

e-governance activities. He also clarified that so far the Ministry through the NCA has provided WIMAX licence for the provision of wireless access to 550 locations.

Currently, the National Information Technology Agency (NITA) has facilitated the installation of the e-Government network, comprising of a fibre optic network within Accra connecting all MDAs with 10 Gbp/s core fibre and 29 WIMAX Base Stations connecting all the 10 Regional Coordinating Councils and selected Districts. The stage has been set for the utilization of shared and secured interoperable architecture to provide better support for e-government and other e-applications. The Ghanaian government is indeed ready for e-commerce and e-business environment for the private sector as well.

Research studies have indicated several factors responsible for the sudden spurt in growth of e-Commerce in developing countries such as Ghana (India Reports, 2009):

- Rapidly increasing Internet user base
- Technology advancements such as VOIP (Voice-over-IP) have bridged the gap between buyers and sellers online
- The emergence of blogs as an avenue for information dissemination and two-way communication for online retailers and e-Commerce vendors
- Improved fraud prevention technologies that offer a safe and secure business environment and help prevent credit card frauds, identity thefts and phishing
- Bigger web presence of SME's and Corporate Institutions because of lower marketing and infrastructure costs.
- Longer reach – rural areas fast realizing the potential of the phone and Internet as transacting media
- The young population find online transactions much easier

This further illustrates that ease of Internet access and navigation are the critical factors that will result in rapid adoption of Net commerce. Safe and secure payment modes are crucial too along with the need to invent and popularize innovations such as Mobile Commerce.

In comparison to Ghana's situation, until a comprehensive research is conducted to ascertain the fixtures and strength on Ghana's readiness for cyber-crime, it will be only to accept what authoritative informer may say. Counter measuring DDoS attack and other cyber-crimes are the only means to be sure of readiness.

Mr. Raymond Codjoe, a legal practitioner, has cautioned that if the situation is not properly addressed, software and computer viruses may in the future mutate data and alter Internet Protocol addresses in the same manner that AIDS does to the human immune system (Ghana Districts, 2009).

This research study, will seek to study effects, preventive measures and counter-measures available to protect Ghana's economy and investments against cyber-attacks such as DDoS.

2.9.8 Estimating Losses Due To DDoS

Estimating the probability of different types of DDoS attacks is no easy tasks. Estimating the time needed to stop such an attack, if the attacker has designed the attack system in a way that the attack is robust against basic traffic filtering, is currently pure guesswork. Cleanup-durations in the range of several weeks seem possible for sophisticated malicious Internet worms.

Many researchers have developed models to estimate financial losses caused by cyber-attacks (crimes) such as DDoS attacks. (Thomas D'ubendorfer, et al, 2004) developed a model and methodology to provide a universal tool that can be used to calculate the expected financial loss for a wide variety of scenarios involving Internet DDoS attacks.

Since the effects of a DDoS attack are complex, they took several steps in order to analyze interdependences involved and financial loss incurred by this type of attack. Specifically, they used graphical plots representing damage versus time in a qualitative fashion, mathematical formulae that can be used to calculate the financial loss for the different types of damage, and example scenarios that demonstrate how to calculate financial loss for concrete settings.

Measure of Impact of DDoS Attack (MIDAS) was also developed from a network service provider's perspective (Rangarajan Vasudevan et al, 2006). We would like to gauge the actual impact of DDoS attacks to rank the relative importance of attacks which could then be used, for instance, to determine priority for mitigation strategies.

Our approach is to estimate the actual or potential economic impact of DDoS attacks to an ISP to derive our relative MIDAS metric estimation. Rather than absolute values, it is believed that a relative metric provides an intuitive indication of the severity of impact regardless of provider size. Thus, the same MIDAS metric can represent the same relative economic impact across different providers. Their scale is applicable to ISPs of all sizes and diverse tiers. They present models to calculate the MIDAS scale using comprehensive economic and network data.

However, obtaining the necessary data to calculate them precisely is in general infeasible. Therefore, they also indicate how the MIDAS scale can be estimated in practice especially in the case of Ghana -thus, an attempt to estimate the economic value of losses that DDoS attack may affect the nation's economy.

According to the Secretariat of the Ministry of Communications of Ghana, the Government of Ghana is committed to the transformation of the services sector of the economy to become the largest source of employment and contributor to the GDP of Ghana (ITES, 2012).

These pursuits of the Government of Ghana are in line with the national ICT Policy blueprint which identifies the need for Government to promote the development of a regional competitive advantage in the Business Process Outsourcing (BPO) industry to enable the private sector meaningful support value added product and services development in Ghana's economic transformation. This referral was made with ICT sector in mind.

However, there is no clear statistics that evaluates the GDP contribution from the ICT sector. It is obvious, that more than 90% of corporate institutions use Information Technology in one way or another to get work done. However, it's not clear whether internet or wide area network has been the "must be" platform for conducting business in Ghana.

This research study will also collect data in this respect to aid in estimating economic losses that may be caused by DDoS attack, review and evaluate the motives and finally ascertain whether DDoS is actually a threat to Ghana economy.

CHAPTER THREE

METHODOLOGY

The purpose of this research was to examine whether a DDoS attack in Ghana, is really a threat vector and how much of economic damage it can beand evaluate the motives behind such threats.

Interview questions were designed and validated by experts in the field of study. The analysis of data collected was done qualitatively via an attempt to compare the findings from the primary data with the meanings derived from secondary data and published text for the purpose of using it to optimize the conceptualization of DDoS as a threat vector in the Ghanaian perspective.

3.0 Research Phases

To get an understanding of the current state of affairs as to industry awareness of DDoS, research proceeded in phases. Some ISPs as listed on Ghana Chamber of Telecommunications Website where randomly selected and questions informally administered to technical personnel.

In the *First Phase*, a survey questionnaire was prepared and technical questions were examined. This part of the survey had two purposes;

- i : Firstly, to determine the current level of awareness of network security vis-à-vis DDoS in a typical ISP setting.
- ii : the survey was used to get an idea of what threats Service Providers are protecting themselves against or which threats have already been realized in Ghana's case as a developing country.

In the *Second Phase*, an ISP was selected and ‘informally’ questions were administered in the form of an interview for necessary data for estimating the Cost of Downtime and due to the sensitive nature of the questions being asked, responses were kept completely anonymous and, keeping the responses anonymous help ensure that answers and figures given were honest and was not artificially inflated.

Table 3.1: Motives

In the *third phase* and using the data in phase two, the results were analyzed and evaluated orestimated using an economic damage model (MIDAS Model). The model comprises the following steps;

Table 3.0: STEPS

Step 1	Targets Categorization (Investigate motives, etc by potential attackers’ to launch DDoS attacks (in Ghana)
Step 2	Calculations (Estimate Economic damage/losses using economic damage model calculation)
Step 3	Analysis and Evaluation Eyaluate Defense

STEP 1: TARGETS CATEGORIZATION (Investigate motives by potential attackers)

The various potential targets were categorized into groups according to attackers' motives as follows;

Table 3.1Motives

	Motive	Target (Victim)
1	Monetary Gain (Extortion, blackmail etc.)	Business Entity with massive public services. Financial Institution with online transactions.
2.	Cyber Terrorism	Attack on ISPs. Attack on education and examinations council web sites and networks.
3	Political Motivation	Ghana: destabilization of government information technology structure. E.g. E-Governance project, National Health Insurance Scheme, etc. Electoral Commission information system. Attack on Political party web site. Attack on Ghana government web sites and servers by foreign nationals.
4	Phishing Attacks	1. Banks, financial institutions, and their networks (e.g. E-Zwich).
5	Revenge	1. IT security companies (e.g., anti-spam and anti-virus developers). 2. ISPs with strong security against online hackers and spammers.

STEP 2: CALCULATIONS (Estimate Economic damage/losses using economic damage model).

The questionnaire and interviews were evaluated according to the method explained below. This was expected to yield total economic loss and enabling the inference and analysis in relation to the GDP of Ghana.

STEP 3: ANALYSIS AND EVALUATION (Evaluate Defense)

With estimated value of each motive, by means of a graph the research work may be able to determine which motive is likely to cause more damage and extent of damage in monetary terms. This information may lead to proper identification of precise mitigation method for any DDoS attack in Ghana.

3.1 Calculating Financial Loss

In this section, the method this research intend to apply is based on a new comprehensive model and methodology, which allows a company to qualitatively and quantitatively estimate possible financial losses due to partial or complete interruption of Internet connectivity (Vasudevan, et al, 2006)

The model further subdivides financial damage (as the result of the interruption of connectivity and Internet services) into four categories:

1. Downtime Loss
2. Disaster Recovery Loss
3. Liability Loss
4. Customer Loss

Calculation of **Total Economic Loss** will be sum of all the four classes of the economic damage. Thus;

$$\text{Total Economic Loss} = \text{Downtime} + \text{Disaster Recovery} + \text{Liability} + \text{Customer}$$

Although this model was used and tested withsome Swiss Telcos, ithas been modified and translated into Ghanaian context. These changes primarily affect the following factors;

Table 3.2: Local Values

Factor	Modification
Working time per employee and year	To be based on 8am to 5pm commonly as applied in Ghana
Productivity degradation during outage	To be estimated according to prevailing charges by outsourcing from business and communication centers.
Total annual revenue	To be based on enterprise under review prudent projections.
Cost per hour for a recovery team member	To be evaluated according to previous fees/charges incurred by the enterprise review, or request for pro-forma invoice from “recovery team” company.

3.1.1 Downtime Loss

The downtime costs can be split further into *Productivity Loss* (employees can no longer do “business as usual” and have to use less efficient ways to fulfill their duties; certain tasks can only be done later) and *Revenue Loss* (lost transactions by customers that cannot access a service or due to the inability of a company to fulfill customer requests).

Productivity Loss

$$= \frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po}$$

Revenue Loss

$$= \frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o$$

Total downtime related loss (L_D) is the sum of Productivity and Revenue loss;

Downtime Loss (L_D)

$$= \frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o$$

Table 3.3: Downtime Loss

Factor	Symbol	Unit
Working hours overlapping outage time	d_o	h(hour)
Service operation time affected by outage	ds_o	h(hour)
Degree of service degradation	S_o	%
Annual cost per employee	E_{ca}	GH¢/yr
Working time per employee and year	d_a	h(hour)/yr
Number of Employees affected by outage	E_{no}	
Productivity degradation during outage	E_{po}	%
Total annual revenue	R_a	GH¢/yr
Service operating hours per year	ds_a	h(hour)
Part of the revenue affected by full outage	R_o	%
SUM for Downtime	L_D	GH¢/yr

3.1.2 Disaster Recovery Loss

This is the costs of the time that employees and external staff have to spend on recovery from an incident. Additionally, material costs can arise.

The loss due to disaster recovery is the sum of the cost for work and material to get the system up and running again. It arises during the downtime [t0; t1]. Given by;

$$\text{Disaster Recovery Loss } (L_r) = E_r \cdot E_{Gh} \cdot d_r + M_c$$

Table 3.4: Disaster Recovery Loss

Factor	Symbol	Unit
Number of employees in the recovery team	E_r	
Cost per hour for a recovery team member	E_{Gh}	GH¢/yr
Recovery work hours outside office hours	h	h(hour)
Cost of material needed	M_c	GH¢/yr

3.1.3 Liability Cost

Many companies offer Service Level Agreements (SLAs) to their customers. In case that their service quality deviates from an SLA, the customer can claim compensation payments. Liability related losses can be partially insured and typically arise several days after the incident.

This loss class describes cost incurred because contracts with third parties cannot be fulfilled and these third parties may demand financial compensation. The loss is incurred during [t1;1] and equals the sum of all demands:

$$\text{Liability Cost } (L_c) = \sum C_c + \sum C_l$$

If a claim is in dispute, substantial legal costs may arise in addition. Notice that this type of loss can often only be quantified when the affected third parties make their claims known. It is hard to estimate how much an affected third party was actually damaged by the outage without asking it. ISPs typically reimburse their customers for the time they were unable to provide service.

Table 3.5: Claim

Factor	Symbol	Unit
Claims from contractual penalties	C_c	GH¢/yr
Claims from other liabilities	C_l	GH¢/yr
SUM for Liability	L_c	GH¢/yr

3.1.4 Customer Loss

Customers being unhappy by ruined service quality might terminate their contract. The rate of new customers joining a service can substantially drop if the reputation of a company suffers. These opportunity costs arise typically weeks to months after an incident.

If a service is unavailable for some time, customers might move to another service provider or no longer use the service. This type of loss is incurred over a very long time $[t_2;1]$ and also includes loss of potential new customers. Given by

Customer Loss $(L_{CL}) = [C_A(\Delta t) + C_P(\Delta t)] \cdot R_C(\Delta t)$

If the revenue per customer varies significantly, the above expression may be inaccurate and would be replaced by a detailed analysis focused on the most important customers.

Table 3.8: Customer Loss Table

Factor	Symbol	Unit
Time interval	Δ_t	yrs
Number of actual customers lost	C_A	
Number of potential customers lost	C_P	
Average revenue per customer	R_C	GH¢/yr
SUM for Customer Loss	L_{CL}	GH¢/yr

3.2 The Questionnaire Format

The questionnaire was designed to include the following factors required to be filled for the calculations (Table 3.9).

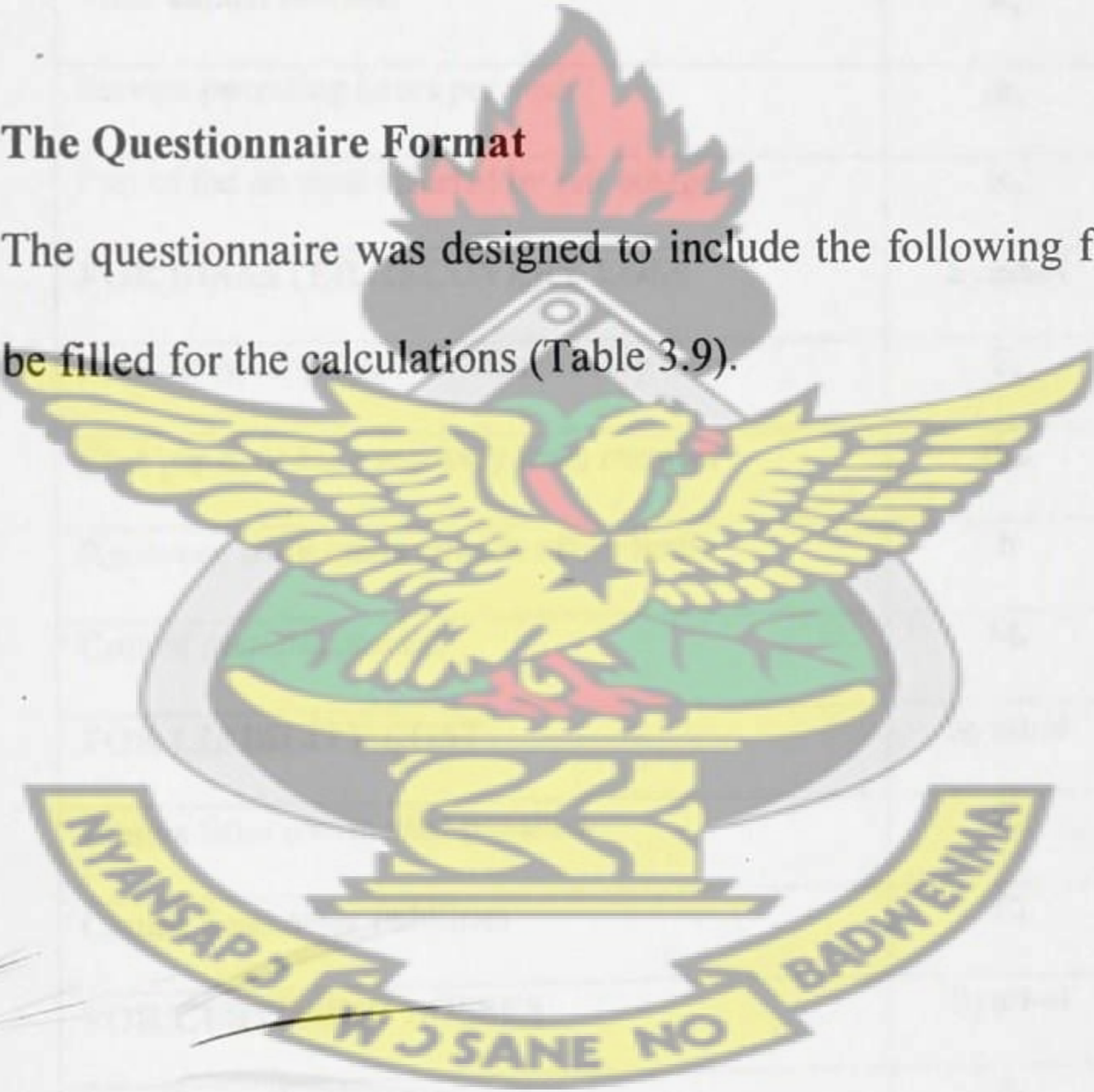


Table 3.9: Questionnaire Table

FOR DOWNTIME LOSS	Symbol	Unit
Working hours overlapping outage time	d_o	h(hour)
Service operation time affected by outage	ds_o	h(hour)
Degree of service degradation	S_o	%
Annual cost per employee	E_{ca}	GH¢/yr
Working time per employee and year	d_a	h(hour)/yr
Number of Employees affected by outage	E_{no}	
Productivity degradation during outage	E_{po}	%
Total annual revenue	R_a	GH¢/yr
Service operating hours per year	ds_a	h(hour)
Part of the revenue affected by full outage	R_o	%
FOR DISASTER RECOVERY LOSS	Symbol	Unit
Number of employees in the recovery team	E_r	
Cost per hour for a recovery team member	E_{gh}	GH¢/yr
Recovery work hours outside office hours	h	h(hour)
Cost of material needed	M_c	GH¢/yr
FOR LIABILITY COST	Symbol	Unit
Claims from contractual penalties	C_c	GH¢/yr
Claims from other liabilities	C_l	GH¢/yr
FOR CUSTOMER LOSSES	Symbol	Unit
Time interval	Δ_t	hrs
Number of actual customers lost	C_A	
Number of potential customers lost	C_P	
Average revenue per customer	R_c	GH¢/yr

The next chapter will provide the results of the survey including pie and bar charts showing the actual number of responses from the various ISPs as well as the overall percentages.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

This chapter presents the analysis and discusses the study findings in relation to the research questions. Later after the descriptive results it will continue with the description of the variables used in the study and concludes with the discussion of cost of downtime in relation to the contribution of the ICT sector to the GDP of Ghana. Data from the questionnaires and interviews were collated, organized and analyzed qualitatively and descriptively.

4.0 Descriptive Results

After collecting the data and analyzing it, a number of themes became clear. As the literature suggested would be the case, most of my hypotheses were strongly supported by the data. Therefore, the question this research seeks to answer; Whether a DDoS attack in Ghana is really a threat vector, and how much of economic damage it can be to the economy was strongly supported by the data.

High percentage of the results shows that most of the institutions are aware of DDoS and have had an experience in their institutions before. In their opinion DDoS was one of the largest Threat Vectors perceived by their network. HTTP flooding was however an attack vector used mostly against their Infrastructure.

A wide range of anti-DDoS mechanisms were in use in the survey respondents' organizations, including on-premise detection/prevention and ISP anti-DDoS services.

All data have been anonymised and is presented with permission from the respondents. Each ISP was represented by a single respondent - most often a senior network/security administrator. However, standard mathematical methods to weigh responses have been applied where there are incomplete responses.

4.1 Research Results

After collecting the data and analyzing it using SPSS (Statistical Product for the Social Sciences), a number of arguments become clear. As the literature suggested would be the case, most of my hypotheses were strongly supported by the data. The first hypothesis *Are you aware of DDoS*, had a 100% response (Table 4.0) showing that DDoS is known in Ghana as is represented in Figure 4.0 below from the responses from the ISPs' point of view. Consequently DDoS is not a strange term to any of the ISPs at all but for when it would strike and cause damages to them and the national economy is a matter of time.

Table 4.0 : Are you aware of DDoS

	Frequency	Percent
Yes	6	100.0

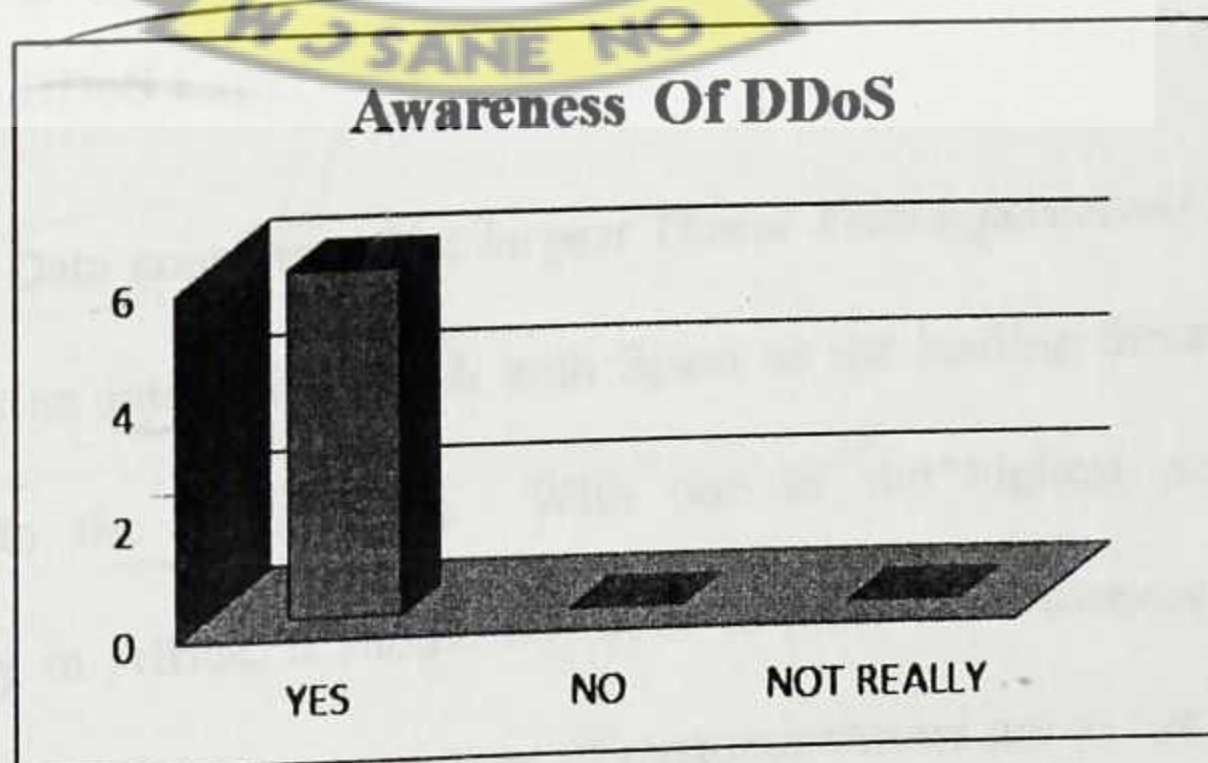


Figure 4.0: Awareness Of DDoS

However, as regards my second query, *have you ever experience any in your institution*, 66.7% of the respondents responded YES with 33.3% saying No. So technically speaking this affirms my objective that DDoS have actually been experienced by or to over half of the ISPs in Ghana.

Table 4.1 **Have you ever experience any in your institution?**

	Frequency	Percent
Yes	4	66.7
No	2	33.3
Total	6	100.0

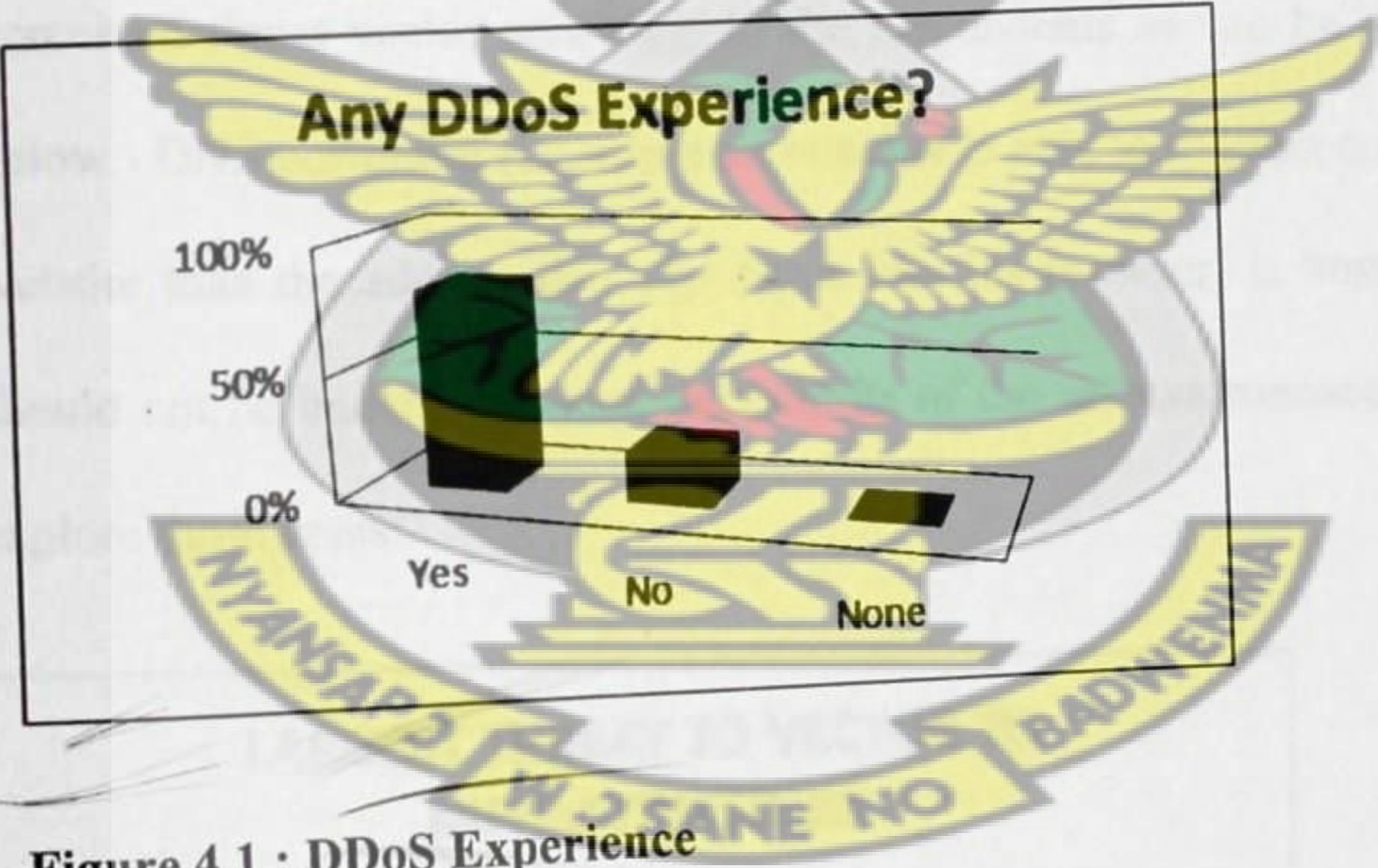


Figure 4.1 : DDoS Experience

The Data concerning the *largest Threat Vector perceived by any network or ISP* showed an interesting graph with Spam as the leading threat vector with 50% according to the respondents. With one of the highest penetration rate for connectivity in Africa, it should not be a surprise for a technocrat to come to the realisation that a higher percentage of customers/users are at the lowest level of the

literacy ladder and hence would click anything that is catchy which in-turn leads to subscriptions to schemes causing spams in return as can be seen in Table 4.2

Table 4.2 What in your opinion is the largest Threat Vector perceived by your network today

	Frequency	Percent
Spam	3	50.0
DDoS	2	33.3
DNS Poisoning	1	16.7
Total	6	100.0

However DDoS took the second position with 33.3% as the 2nd most perceived threat vector according to the respondents as can be seen in Figure 4.3 below. DNS poisoning (i.e. when an attacker is able to redirect a victim to different website than the address that s/he types into his browser) is however a threat that should not be underrated since the culprits of the sakawa menace might try to also explore those areas.

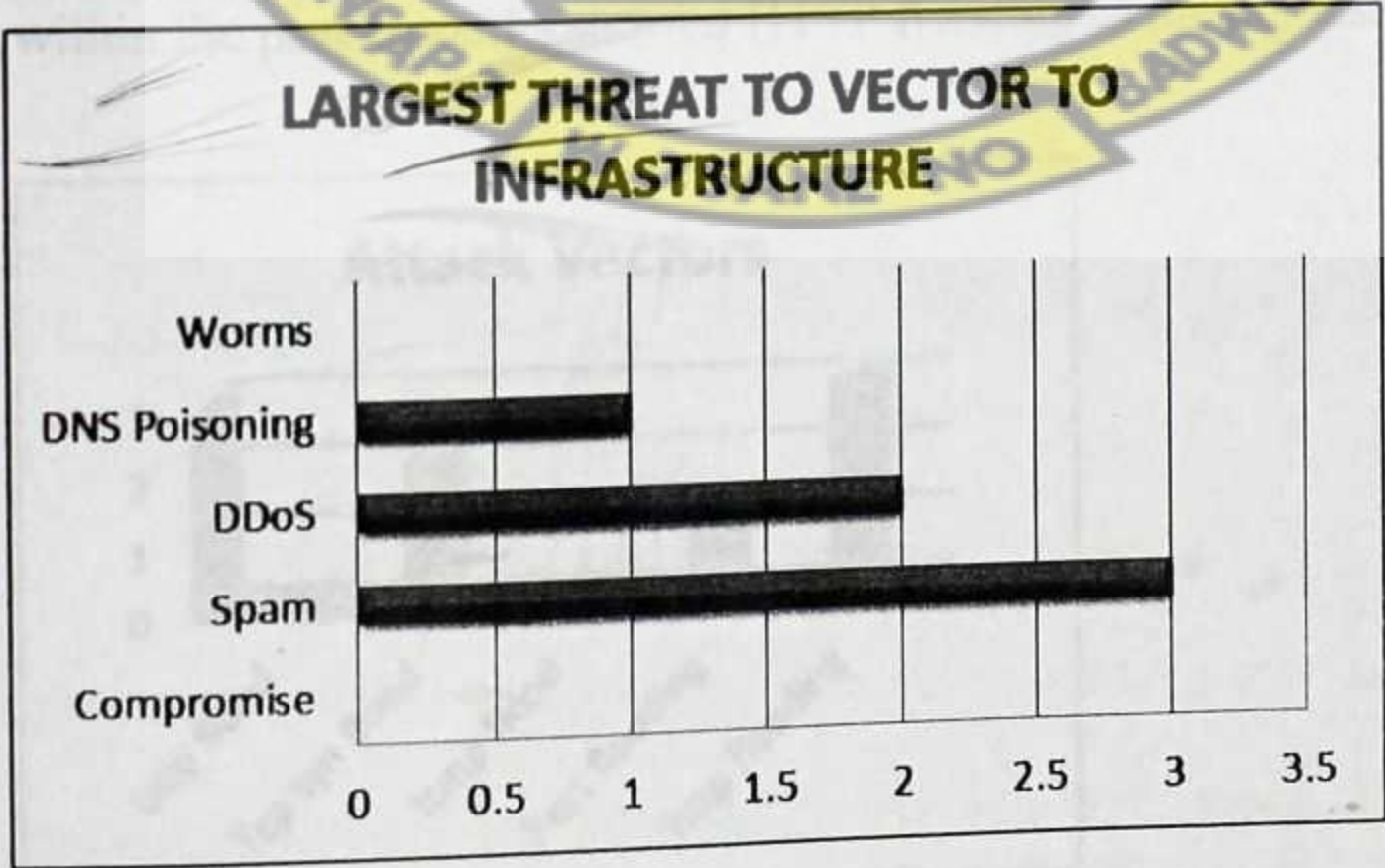


Figure 4.2: Infrastructural Threat Vector

TCP SYN With this percentage of DDoS attacks on an infrastructure, a target on any branch of a networked bank, or Municipal District Assembly on E-government network, or even ISP who offers e-commerce services to many subscribers would certainly cause havoc. This might be possible due to the increasing consumer adoption of the ALWAYS-ON nature of these connections.

A distributed denial of service attack on a small IT infrastructure-based country such as Ghana, would therefore register an enormous economic damage across the economic landscape of the nation.

Table 4.3 Which of the following attack vector was observed within the past 6months

	Frequency	Percent
TCP Syn Flood	2	33.3
Port Flood	1	16.7
HTTP Flood	3	50.0
Total	6	100.0

The highest attack vector against any infrastructure observed (Table 4.3) within the past 6months showed HTTP flooding as the highest attack with 50%.

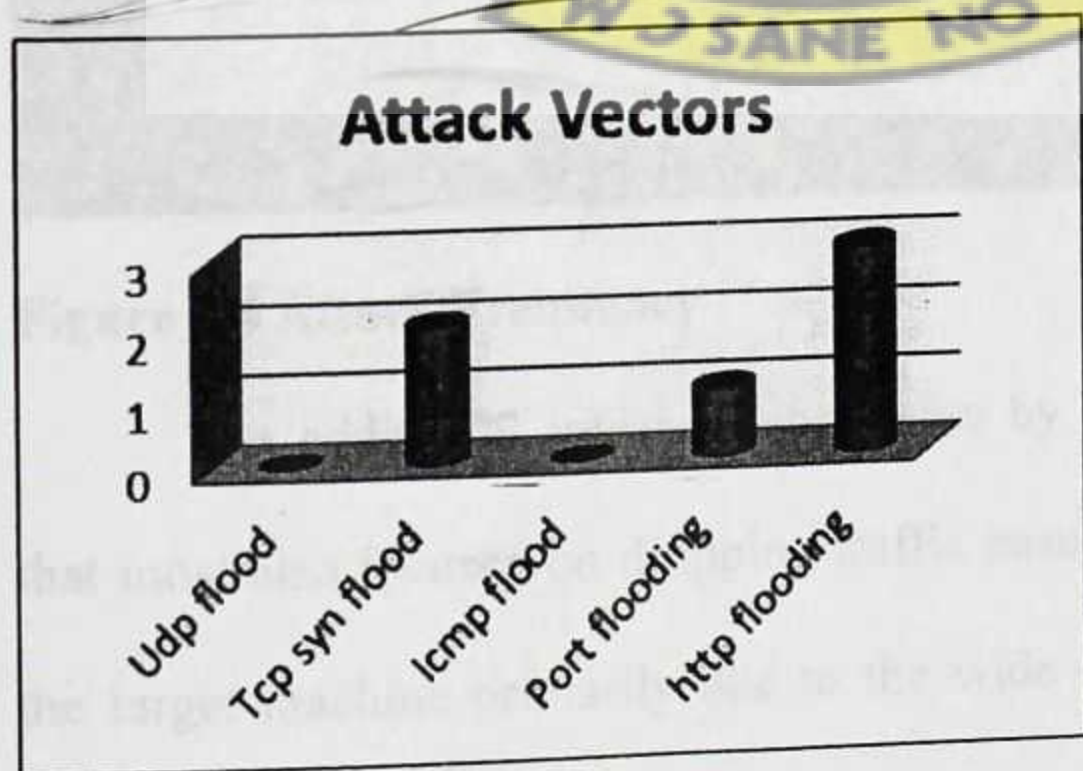


Figure 4.3 : Attack Vectors

TCP SYN flood attacks however followed closely in 2nd place to HTTP flooding. These two most treacherous attack vectors were the most experienced within a month on an Infrastructure. This can cause a lot of damage if that infrastructure is not adequately protected.

In terms of Infrastructure capacities, Virtual economy is vulnerable to DDoS attacks or any other online attack. Servers forming the basis of the Ghanaian online economy may be overloaded in a matter of minutes if spare resources are not employed.

KNUST

In *Attack Detection Per Month*, more than 10 attacks in a month contributing about 50% were experienced by most of those networks interviewed (Figure 4.5)

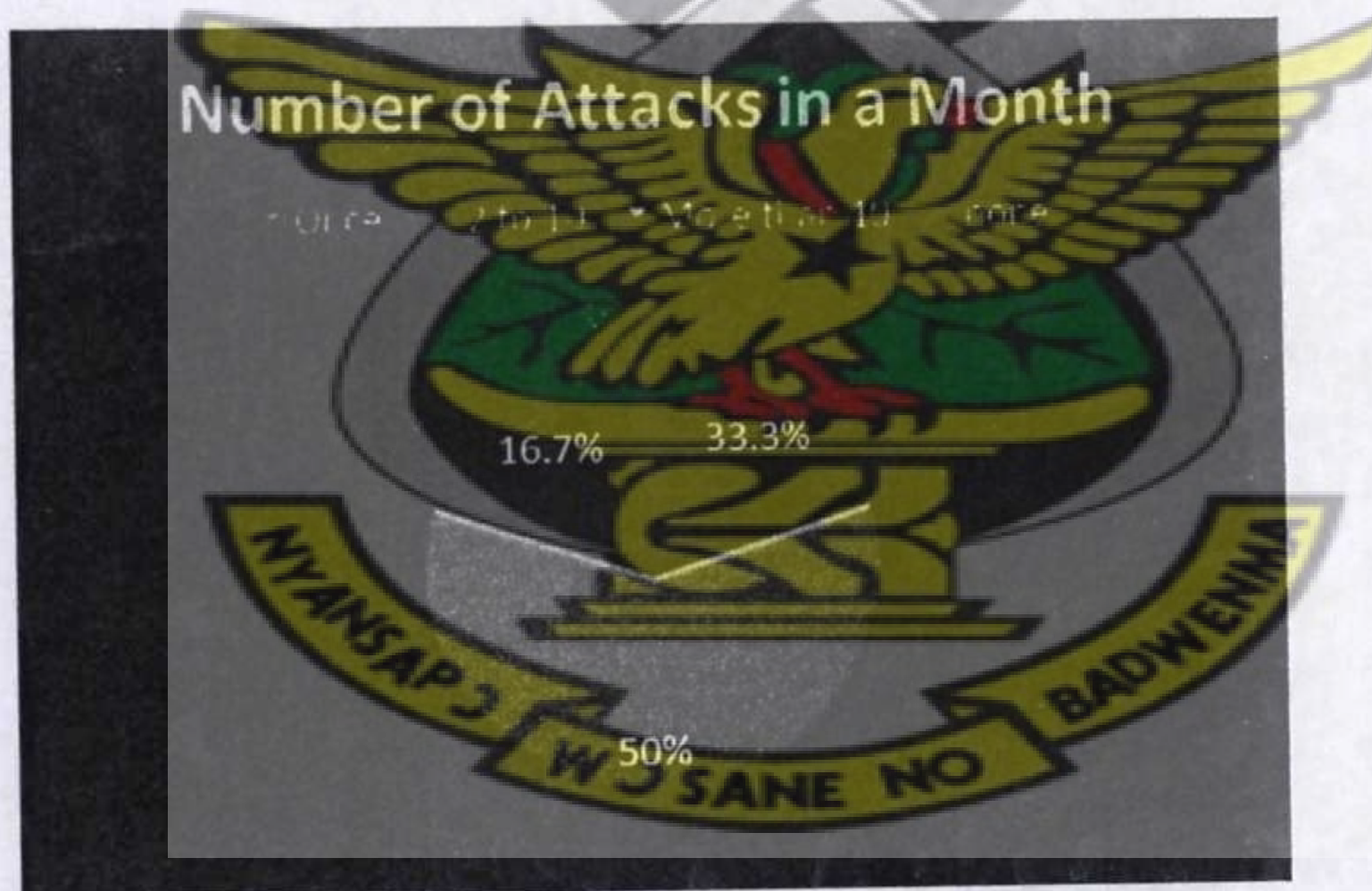


Figure 4.4 Attack Frequency

The additional informal comments by the respondents, however, indicated that most also focused on dropping traffic based on a service—port and protocol on the target machine primarily due to the wide distribution of attack sources, which may or may not have been spoofed.

Regarding *Attack Detection Tools And Techniques* as indicated, a number of respondents (66.7%) indicated that they resorted to commercial detection tools but however indicated that they also employ multiple mechanisms to detect and trace attacks back through their network. Because of these most of the respondents also indicated using intelligent filtering systems to reduce and to detect and handle an attack.

Table 4.4 How do you Detect an attack?

	Frequency	Percent
Manual	1	16.7
Commercial	4	66.7
In House	1	16.7
Total	6	100.0

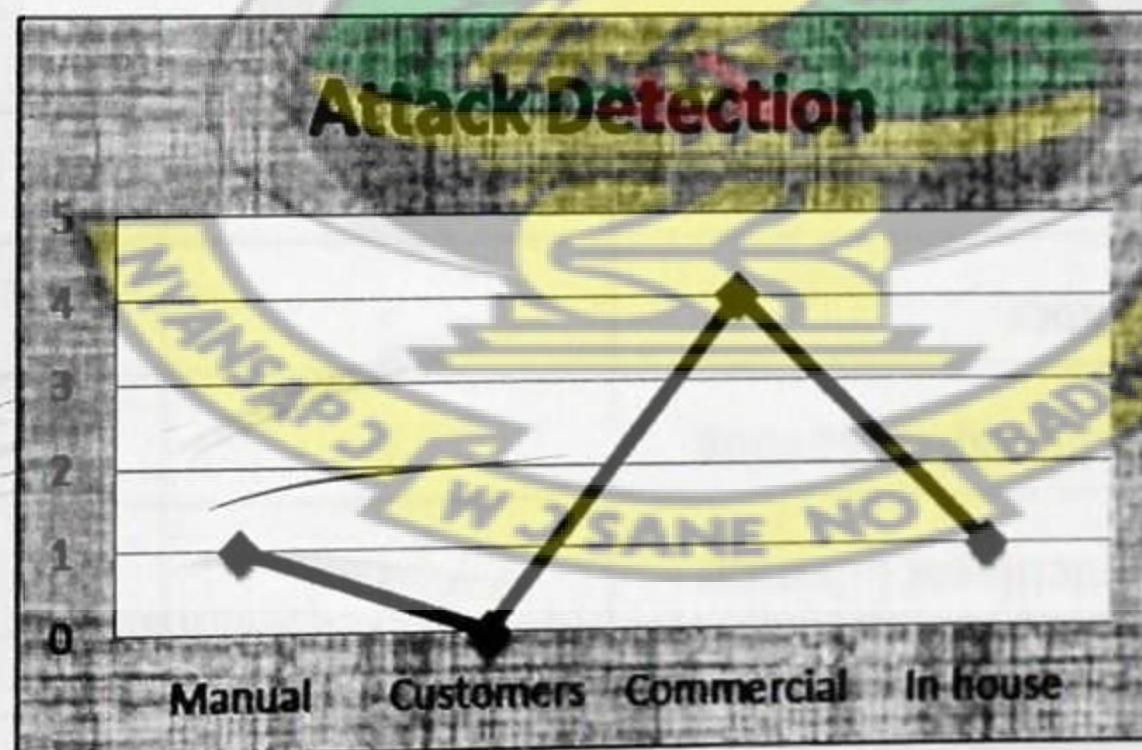


Figure 4.5 Attack Detection

Finally, the hypothesis about the motives of a DDoS attack, then it will be politically motivated and hacktivist in nature was not fully supported with only 16.7% of the data.

This might be due to the fact that the information technology terrain in politics in Ghana is not as developed as those in the advanced countrieslike the US and UK where political parties have an online or web presence.

This does not mean an attack on a political party's website would not wreck havoc but the likelihood that if there is a way it might be used is marginal. It can however cause destabilization of government information technology structure e.g.E-Governance project, National Health Insurance Scheme, Electoral Commission information system and to an extent an attack on the ruling political party's website.

Table 4.6 What do you think would be the motives behind a DDoS attack if it is to happen to Ghana?

	Frequency	Percent
Monetary Gain	1	16.7
Political	1	16.7
Phishing	4	66.7
Total	6	100.0

The data regarding Monetary Gain as a motive showed that 16.7% of attacks might hit a business Entity with massive public services and Financial Institution with online presence. The number of *Might-be* attacks with a solely Phishing motive was quite interesting in that it was not expected to be the highest.

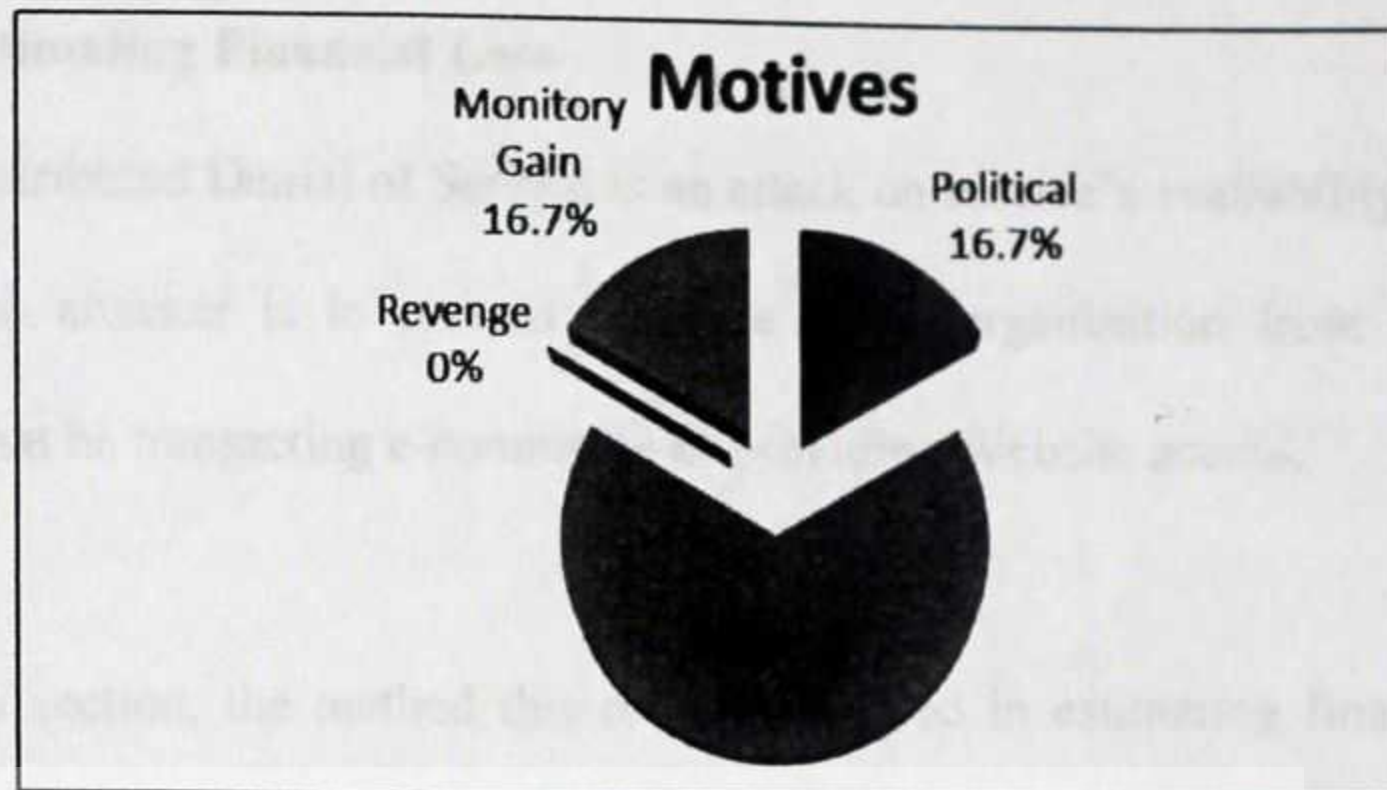


Figure 4.7: Motives

Phishing had 66.7% of the data analysed indicating the attackers could target those in the Banking industry in Ghana which is the fastest growing sector.

Phishing however according to the respondents topped with 66.7% of the motives that can be behind an attack due to the fact that much of this attack activity can be as a result of a scoundrel attempting to still money from individual and organizations that are highly reliant upon Internet availability and are likely to be vulnerable from a bandwidth and network capacity perspective

With the downward demise of the sakawa scheme in Ghana, most hacktivist and extortionist might consider going into phishing to steal innocent banking details for their nefarious activates.

4.2 Estimating Financial Loss

Distributed Denial of Service is an attack on service's availability. The main aim of the attacker is to prevent the core of an organisation from functioning, whether that be transacting e-commerce or providing Website access.

In this section, the method this research applied in estimating financial loss is based on a new model and methodology (MIDAS), which allows a company to qualitatively and quantitatively estimate possible financial losses due to partial or complete interruption of Internet connectivity.

The model further sub divides financial damage (as the result of the interruption of connectivity and Internet services) into four categories:

- Downtime Loss
- Disaster Recovery Loss
- Liability Loss
- Customer Loss

Hence,

$$\text{Total Economic Loss} = \text{Downtime} + \text{Disaster Recovery} + \text{Liability} + \text{Customer}$$

4.3 Scenario

The Information and telecommunication technology sector in Ghana is one of the largest contributors to the country's GDP. Telecom companies suffer primarily from productivity loss of its employees that can no longer do work during an attack. Financial loss is an expected effect of any significant degradation of Internet performance.

Furthermore, financial loss changes over time and economic damage usually has not the same characteristics over time as technical problems have. Economic damage can still grow when technical problems have been resolved and the attack has stopped.

For this research an ISP/Telecommunication company (hereafter called TELCO-M) was chosen in Ghana for the estimation. The Telecommunication sector is one of the fastest growing sectors and most of them operate both telephone and internet services.

The Annual revenue of Telco-M for 2011 contributed was just a little over US\$784.093 million (i.e. GH1528.9814 million) and the total employees as of the end of 2011, was 2314 according to secondary data.

As of the time of writing this research, the Exchange rate of the Cedi (¢) to the Dollar (\$) was $\text{GH}1.95 = \$1.0$ and all figures would be in thousands of Cedis.

Table 5.1 shows a summary of data collated to be used for the estimation of the four concrete scenarios that would sum up to be the Cost of Total Economic Loss.

Table 4.7: Questionnaire Data Table

FOR DOWNTIME LOSS	Symbol	Unit	Actual	Estimated
Working hours overlapping outage time	d_o	h(hour)	8	56
Service operation time affected by outage	ds_o	h(hour)	24	168
Degree of service degradation	S_o	%	20	100%
Annual cost per employee	E_{ca}	GH¢/yr	2000	24000
Working hours per employee per day		h(hour)/yr	8	56
Working time per employee per year (235 working days per year)	d_a	h(hour)/yr	8	1880
No. of Employees affected by outage	E_{no}	No.	2324	2,314
Productivity degradation during outage	E_{po}	%	20%	100%
Total annual revenue (2011)	R_a	GH¢/yr/mil		1528.9814
Service operating hours per year	ds_a	h(hour)	8760	8760
% of revenue affected by full outage	R_o	%	15%	40%
FOR DISASTER RECOVERY LOSS	Symbol	Unit		
No. of employees in the recovery team	E_r		4	8
Cost per hour for a recovery team member	E_{Gh}	GH¢/yr	8	56
Recovery work hours outside office hours	H	h(hour)	16	112
Cost of material needed	M_c	GH¢/yr		40000
FOR LIABILITY COST	Symbol	Unit		
Claims from contractual penalties	C_c	GH¢/yr	0	0
Claims from other liabilities	C_l	GH¢/yr	0	0
FOR CUSTOMER LOSSES	Symbol	Unit		
Time interval	Δ_t	yrs	1	1
Number of actual customers lost	C_A		1	20
Number of potential customers lost	C_P		1	5
Average revenue per customer	R_c	GH¢/yr	7	84

4.3.1 Downtime Loss

For an outage of 24 hours the research assumed that about 20% of workers would be affected in the company.

The total downtime related loss is the sum of productivity and revenue loss. This type of loss is incurred during the actual downtime interval. This is given as

Productivity Loss = $\frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po}$

Revenue Loss = $\frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o$

Hence, Downtime Loss = Productivity Loss + Revenue Loss

Downtime Loss (L_D) = $\frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o$

Table 4.7.1: Down Time Loss Data

FOR DOWNTIME LOSS	Symbol	Unit	Actual	Estimated
Working hours overlapping outage time	d_o	h(hour)	8	56
Service operation time affected by outage	ds_o	h(hour)	24	168
Degree of service degradation	S_o	%	20	100%
Annual cost per employee	E_{ca}	GH¢/yr	2000	24000
Working hours per employee per day		h(hour)/yr	8	56
Working time per employee per year (235 working days per year)	d_a	h(hour)/yr	8	1880
No. of Employees affected by outage	E_{no}	No.	2324	2,314
Productivity degradation during outage	E_{po}	%	20%	100%
Total annual revenue (2011)	R_a	GH¢/yr/mil		1528.9814
Service operating hours per year	ds_a	h(hour)	8760	8760
% of revenue affected by full outage	R_o	%	15%	40%

Item	Figure		
Eca	24000	GH	
da	1880	hrs	
do	16	hrs	
Eno	2324	no	
Epo	50%	%	
Ra	1528.981	GH (Billion)	
dsa	8760	hrs	
dso	24	hrs	
Ro	40%	%	
So	20%	%	

$$= ((D7/D8)*(D9*D10*D11)+(D12/D13)*(D14*D15*D16))$$

$$Ld = 237,345.02$$

From the results, this indicates a Downtime Loss of GH¢237.345.02 and this is what Telco-M could suffer when its infrastructure is attacked over a period 24hrs.

4.1.2 Disaster Recovery Loss

The loss due to disaster recovery is the sum of the cost for work and material to get the system up and running again. It arises during the downtime [t0; t1].

Table 4.7.2 Disaster Recovery Loss Data

FOR DISASTER RECOVERY LOSS	Symbol	Unit	Actual	Estimated
No. of employees in the recovery team	E_r		4	8
Cost per hour for a recovery team member	E_{Gh}	GH¢/yr	8	56
Recovery work hours outside office hours	d_r	h(hour)	16	112
Cost of material needed	M_c	GH¢/yr		40000

Disaster Recovery Loss
$$(L_r) = E_r \cdot E_{Gh} \cdot d_r + M_c$$

Er	5	No	
Egh	8	hrs	$L_r = (H8*H9*H10)+H11$
dr	16	hrs	$L_r = 40640$
Mc	40000	gh	

From the data collated, the above Disaster Recovery cost to the company of GH¢40,640 would be experienced. And this indicates the challenge to any ISP to always be on the guard to avoid such huge losses

4.3.3 Liability Loss

This loss class describes cost incurred because contracts with third parties cannot be fulfilled and these third parties demand financial compensation. The loss is incurred during $[t_1;1]$ and equals the sum of all demands:

$$\text{Liability Cost } (L_C) = \sum C_c + \sum C_l$$

Table 4.7.3 Liability Loss Data

FOR LIABILITY COST	Symbol	Unit	Actual	Estimated
Claims from contractual penalties	C_c	GH¢/yr	0	0
Claims from other liabilities	C_l	GH¢/yr	0	0

Liability Cost to the company is assumed to be negligible since structures in Ghana are not equipped to deal with such issues at the Courts. This type of loss could have often been quantified when the affected third parties make their claims known.

It is however hard to estimate how much an affected third party was actually damaged by the outage without asking it. ISPs typically reimburse their customers for the time they were unable to provide service.

Another major challenge is the issue of jurisdiction and the ability of existing legal frame works to prosecute such companies if there is such a challenge.

4.3.4 Customer Loss

If a service is unavailable for some time, customers might move to another service provider or no longer use the service. This type of loss is incurred over a very long time [t2;1] and also includes loss of potential new customers.

Customer Loss $(L_{CL}) = [C_A(\Delta t) + C_P(\Delta t)] \cdot R_C(\Delta t)$

As discontented customers cannot instantly cancel a contract, the damage resulting from *customer loss* might occur weeks or even months after the actual technical incident. A sudden surge of customers terminating their contracts is likely to happen at the end of the current service period

Table 4.7.4 Customer Loss Data

FOR CUSTOMER LOSSES	Symbol	Unit	Actual	Estimated
Time interval	Δt	ys	1	1
Number of actual customers lost	C_A		1	20
Number of potential customers lost	C_P		1	5
Average revenue per customer	R_C	GH¢/yr	7	84

t	1	Lcl	=(19+110)*111
Ca	20		
Cp	5		
Rc	84	Lcl	= 2100

The assertion that if a service isn't available for some time customers of any company might switch to another company is not true as portrayed above by the

negligible figure above of GH2100. If the revenue per customer varies significantly, the above expression would be inaccurate and should be replaced by a detailed analysis focused on the most important customers.

Hence, the **Total Economic Loss** is given as

$$\text{Total Economic Loss} = \text{Downtime} + \text{Disaster Recovery} + \text{Liability} + \text{Customer Loss}$$

$$\begin{aligned} \text{Total Economic Loss} &= 237345.02 + 40640 + 2100 \\ &= \text{GH¢}280,085.02 \end{aligned}$$

So, our telecommunications giant under this case study Telco-M, would be losing at least Two Hundred and eighty thousand and eighty five Ghana Cedis and 2 pesewas (GH280, 082.02) within the first 8hour working period when the system/infrastructure is attacked and it goes offline.

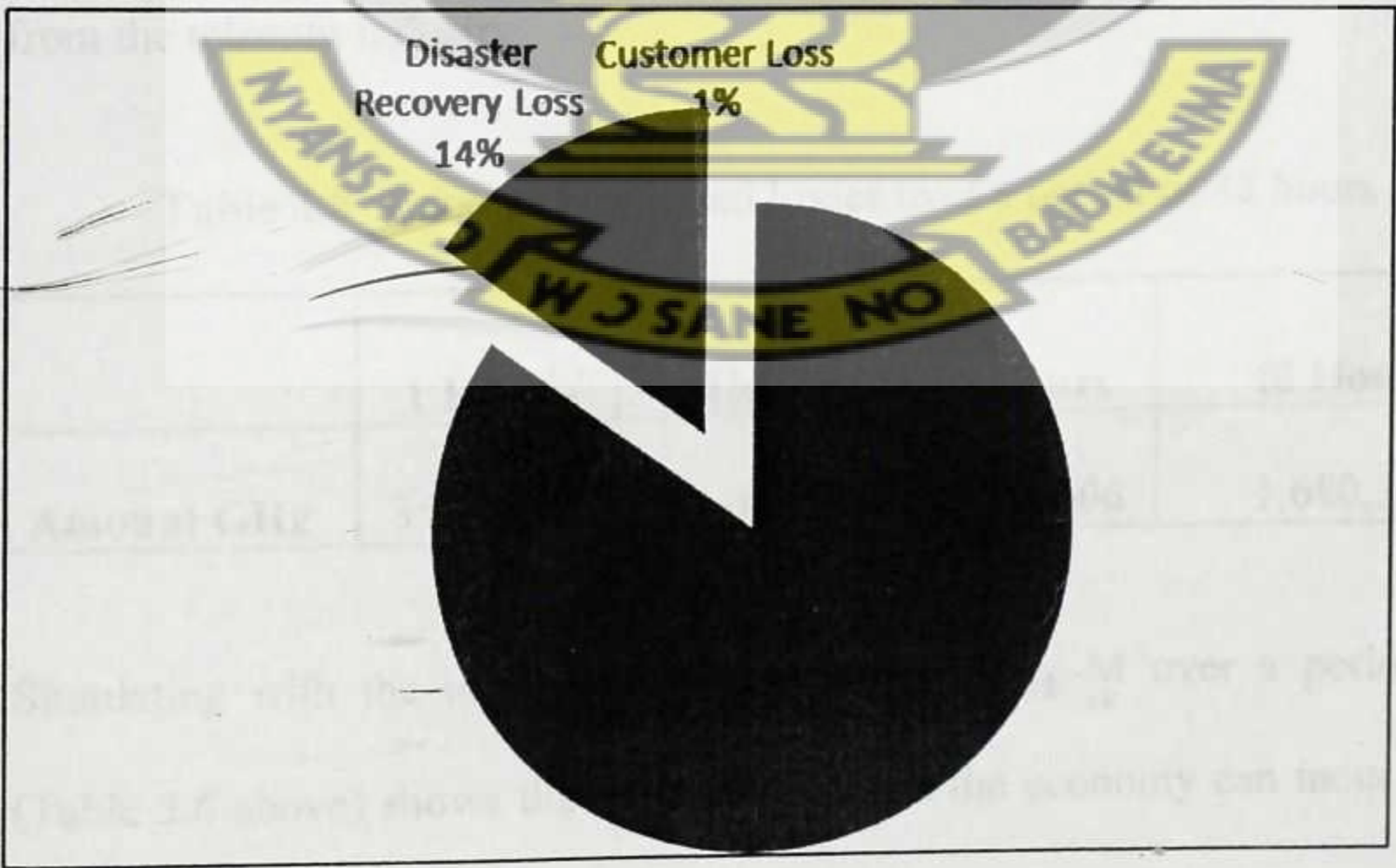


Figure 4.8: Total Economic Loss

From figure 4.7 above the Downtime Loss contributes the highest loss to a company if it is to happen but also depends on the technical infrastructure of the company.

However, customer loss being negligible depends on revenue per customer and competitors. The threat potential of a massive DDoS attack on critical Internet infrastructure elements can no longer be ignored. The possible direct and indirect financial loss for many Internet dependent companies must be considered in each complete business risk analysis.

4.4 Final Analysis

According to an independent report, the contribution of the telecom industry to Ghana’s economy indicates in 2010 alone, telecom operators paid GHC598 million in taxes and levies, representing 10% of government income for that year. The report noted that market leader Telco-M alone paid a whopping GHC415 million, being 6.94% of government income for 2010, and 69.4% of taxes and levies from the telecom industry.

Table 4.8 Telco-M Estimated losses over a period of 48 hours

	1 Hours	8 Hours	24 Hours	48 Hours
Amount GH¢	35,010.63	280,085.02	840,255.06	1,680,510.12

Simulating with the total Downtime Loss of Telco-M over a period of 48hours (Table 5.6 above) shows the depth of loss that the economy can incur over a period of 48hours.

Hence, assuming all ICT related companies especially those with online presence are to be also attacked simultaneously over the same period considering the contribution of the ICT Sector to the GDP of the Ghana which is estimated to be about 8 percent demonstrates what impact an attack would have.

However, despite most of these attacks happening none of the Telcos and ISPs seem to be firmly aware of cyber crime Laws in Ghana for prosecution of offenders and culprits.

Table 4.9 Are you aware of any Cyber Crime Laws in Ghana?

	Frequency	Percent
Yes	2	33.3
No	3	50.0
Not Really	1	16.7
Total	6	100.0

According to the respondents only 33.3% seem to be aware of cyber crime laws in Ghana with over 50% (Table 5.6above) being ignorant about cyber crime laws in Ghana.

Interestingly, the number of not sure of (Not Really) was the highest with 50% and none have never ever taken any culprit to the Law Court (Table 5.7 below).

Table 4.9.1 Have your Institution ever taken any culprit to a Law Court before?

	Frequency	Percent
No	6	100.0

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

This chapter presents a summary of the main findings, conclusion drawn and recommendations emanating from the study. The limitations of the study are discussed and finally suggestions are made for future research.

5.1 Summary

This research sought to technically analyse whether a DDoS attack in Ghana is really a threat vector to the economy, how much of economic damage it can have and the motives that might be behind it. To get an understanding of the current state of affairs as to industry awareness of DDoS, research proceeded in phases. Some ISPs as listed on Ghana Chamber of Telecommunications Website were randomly selected and questions informally administered to technical personnel.

According to the results, 100% response from the respondents showed that DDoS is known to them however as regards the second query, *have you ever experience any in your institution*, 66.7% of the respondents responded YES with 33.3% saying No.

The Data concerning the *largest Threat Vector perceived by any network or ISP* showed an interesting graph with Spam as the leading threat vector with 50% according to the respondents. However DDoS took the second position with 33.3% as the 2nd most perceived threat vector according to the respondents

The highest attack vector against any infrastructure observed within the past 6months showed HTTP Flooding as the highest attack with 50%.

TCP SYN flood attacks however followed closely in 2nd place to HTTP flooding. These two most treacherous attack vectors were the most experienced within a month on an Infrastructure. In attack detection per month, More than 10 attacks in a month contributing about 50% were experienced by most of those networks interviewed.

Regarding attack detection tools and techniques as indicated, a number of respondents (66.7%) indicated that they resorted to commercial detection tools but however indicated that they also employ multiple mechanisms to detect and trace attacks back through their network.

According to respondents, intelligent packet filtering (50%), and alternative routing (16.7%) and other (33.3%) mitigation means are marginally deployed by network operators to secure them against any attack

Finally, the hypothesis about the motives of a DDoS attack, then it will be politically motivated and hacktivist in nature was not fully supported with only 16.7% of the data.

The data regarding Monetary Gain as a motive showed that 16.7% of attacks might hit a business Entity with massive public services and Financial Institution with online presence. The number of *Might-be* attacks with a solely Phishing motive was quite interesting in that it was not expected to be the highest. Phishing had 66.7% of the data analysed indicating the attackers could target those in the Banking industry in Ghana which is the fastest growing sector.

In estimating the financial loss that might result as a result of a DDoS attack a formulae based on a new model and methodology (MIDAS), which allows a

company to qualitatively and quantitatively estimate possible financial losses due to partial or complete interruption of Internet connectivity (Thomas D'ubendorfer *et al*, 2004) was used. This model subdivides financial damage (as the result of the interruption of connectivity and Internet services) into four categories: Downtime Loss, Disaster Recovery Loss, Liability Loss, and Customer Loss

For this research an ISP/Telecommunication company called TELCO-M was chosen in Ghana for the estimation. The Annual revenue of Telco-M for 2011 contributed was just a little over US\$784.093 million (i.e. GH1528.9814) and the total employees as of the end of 2011, was 2314 according to secondary data.

From the simulation, a Downtime Loss of GH¢237.345.02 was suffered by Telco-M when its infrastructure was attacked over a period 8 working hours. Disaster Recovery Loss cost Telco-M GH¢40,640 and Liability Loss to the company was however assumed to be negligible since structures in Ghana are not equipped to deal with such issues at the Law Courts but most ISPs typically reimburse their customers for the time they were unable to provide service.

On economic level loss of consumer loyalty, causing indirect financial losses and a shift in customers' preferences, investors' withdrawal, cash flows decrease, additional costs of security and information technology audits, infrastructure resources expansion and public relations costs in a strategic perspective aren't farfetched. As discontented customers cannot instantly cancel a contract, the damage resulting from *customer loss* might occur weeks or even months after the actual technical incident. The assertion that if a service isn't available for some time customers of any company might switch to another company is not true as portrayed by the negligible figure of GH2100 (i.e. the amount Telco-M will loose in the event

of a customer leaving the network). The Total Economic Loss to be incurred by Telco-M if it was attacked by a DDoS was GH¢280, 85.02. However, despite most of these attacks happening none of the Telcos and ISPs seem to be firmly aware of cyber crime Laws in Ghana for prosecution of offenders and culprits. According to the respondents only 33.3% seem to be aware of cyber crime laws in Ghana with over 50% (Table 5.6 above) being ignorant about cyber crime laws in Ghana.

Interestingly, the number of not sure of (Not Really) was the highest with 50% and none have never ever taken any culprit to the Law Court

5.2 Conclusions

DDoS attacks are a difficult challenge for the Internet community. The reality of the situation is that only the biggest attacks are fully investigated, the smaller ones that happen every day slip through the cracks and while a bevy of products exist, most are not practical for smaller networks and providers.

With the wide variety of tools available on the Internet and the lessening degree of technical knowledge and effort necessary to launch DDoS attacks it seems that, indeed, we haven't seen anything yet. The potential risk to a developing critical infrastructure organisation in Ghana being subjected to a DDoS attack is too great to ignore.

From this research it can be predicted that there would be potential growth in scale and sophistication of these attacks. The number of financially motivated online attacks will grow in Ghana and online businesses and indeed any organizations with a Web presence need to be aware of the growing threat from DDoS and the other kinds of attacks.

Furthermore, effective and efficient countermeasures require operational awareness, speed, precision, experience, appropriate security protocols summarizing and alleviating potential consequences in case of failure to contain as well as proactive detection algorithms in place.

The online security plans of any organization in Ghana must include deep consideration of this type of threat, and organizations must familiarize themselves and their system administrators on the current motives and methods of DDoS attackers. The losses in productivity, money and reputation can be significant. A well documented plan to deal with the threat is a necessity.

Finally, the contribution of the telecom and ICT sector to the GDP of the Nation is significant and cannot be toyed with. The over 1% damage to GDP of a developing country such as Ghana for every one week of Internet blackout is a reflection of how reliant modern business and society have become on Internet technologies.

5.3 Recommendations and Suggestions for Future Research

This research is essentially interdisciplinary and draws on work in computer security, microeconomics, and social network analysis. This approach was necessary in order to adequately understand and evaluate the impact of DDoS attacks on the economic and financial impact in relation to the GDP, network and critical infrastructure of Ghana.

The results obtained are encouraging and leave a broad avenue to explore for further research works. Therefore, the following recommendation should be considered in future studies:

- ❖ There is a need to develop a better, simple and accurate model that predicts the financial implications of cyber attack. A complex evaluation model would usually make its application unbearable to institutions.
- ❖ Analysis of institutionalized defence structures and their inter-cooperation in light of a spontaneous DDoS attack using widely available tools.
- ❖ There is a need to develop a better, simple and accurate model that predicts the financial implications of cyber-attack to enable institutions and companies to easily calculate their own economic loss.

5.4 Limitations of the Study

- The study considered only a single Telco/ISP due to lack of data to estimate the cost of downtime etc.
- Most institutions were not willing to divulge information pertaining to correct data for the research and sometimes respondents had to be coaxed into giving scanty data.
- In Ghana, most Companies and Institutions do not keep records of the inputs and outputs. This study suffered from the weakness associated with survey interviews when data accuracy depended heavily on the respondent's ability to recall past information and to answer survey questions accurately.
- High material cost (stationary, transportation and secretarial)
- Relatively short period for the study which is very involving

REFERENCES

AFRICAN ECONOMY OUTLOOK, "GHANA"

(<http://www.africaneconomicoutlook.org/en/countries/west-africa/ghana/>), Accessed on 22/06/2012.

AITI-KACE, (2009). Ghana-India Kofi Annan Centre of Excellence in ICT (AITI-KACE),

"What We Do". (<http://www.aiti-kace.com.gh/?q=Node/2>). Accessed on 4/5/12.

APEC, (2005). APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment [Denial Of Service / Distributed Denial Of Service MANAGING Dos ATTACKS].

APEC, (2005). APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment.

ARBOR NETWORKS, (2005). "Worldwide ISP Security Report" September 2005.

AURA, T., Nikander, P. and Leiwo, J. (2000). "DOS-resistant Authentication with Client Puzzles," Lecture Notes in Computer Science, Volume 2133, revised from the 8th International Workshop on Security Protocols.

AURA, T. and Nikander, P. (1997). "Stateless Connections," Proceedings of the First International Conference on Information and Communication Security.

BENNAHUM, D. (1996). "PANIX ATTACK", MEME 2.12.
(<http://memex.org/meme2-12.html>). Accessed on 9/4/2012.

BORGLUND, J. (2009) *Top 5 Most Costly Viruses of All Time*.
<http://anti-virus-software-review.toptenreviews.com/top-5-most-costly-viruses-of-all-time.html>. Accessed on 7/7/2011.

B&FT, (2012). "Cost of Internet goes down ...capacity goes up 65 times".
http://www.thebftonline.com/bft_subcat_linkdetails.cfm?prodcartID=6&tblNewsCatID=77&tblNewsID=10654. Accessed on 5/3/2011.

CARL, G., Kesidis, G., Brooks, R.R. and Rai, S. (2006). "Denial-of-service attack-detection techniques", *IEEE Internet Computing*, Vol 10, No. 1, January/February, pp 82-89.

CERT, (1996). "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", September 1996.

CHESWICK, W. and Bellovin, S. (1994). "Firewalls and Internet Security", (ISBN: 0201633574, January 1994).

CNN Money, (2004). MyDoom costs seen up to \$250 million - Jan. 30, 2004.
(http://money.cnn.com/2004/01/28/technology/mydoom_costs/index.htm)

DANCHODANCHEV. "GoDaddy hit by a DDoS attack."
(<http://www.zdnet.com/blog/security/godaddy-hit-by-a-ddos-attack/2391>).
Accessed on 1/1/2012

DENNING, D. (2000). "Reflections on Cyber weapons Controls." *Computer Security Journal* 16(4): 43-53.

DENNING, Dorothy E. "Barriers to Entry. (2012)." *IO Journal*, April 2012: 6-10.

—. "Cyberterrorism Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S House of Representatives." Washington, DC.

D'UBENDORFER, T., Arno Wagne, Bernhard Plattner. (2004). "An Economic Damage Model for Large-Scale Internet Attacks". *Computer Engineering and Networks Laboratory (TIK). Swiss Federal Institute of Technology, ETH-Zentrum, CH-8092 Zurich.*

EKOW QUANDZIE, (2011). *Ghana Business News*. "African countries told to partner new economic giants as China is leading trading partner".
(<http://www.ghanabusinessnews.com/2011/06/27/african-countries-told-to-partner-new-economic-giants-as-china-is-leading-trading-partner/>).

FBI, (2012). *FBI Warns: Game Over*". (<http://infosecisland.com/blogview/19295-FBI-Warns-GameOver.html>). Accessed on 10/1/2012

FOROUZAN, B. (2006). *TCP/IP Protocol Suite*, McGraw Hill, 1221 Avenue of the Americas, New York, third edition.

GARBER, L. (2000). "Denial-of-Service Attacks Rip the Internet", *Computer*, Vol 33, No. 4, April, pp12-17.

GHANA DISTRICTS, 2009.

<http://www.ghanadistricts.com/districts1on1/ama/?arrow=nws&read=28121>.
Accessed on 11/8/2012

GISPA, 2012. Ghana Internet Service Providers. "Cost of Internet goes down ...capacity goes up 65 times". (<http://www.gispa.org.gh/news/?p=525>). Accessed on 9/9/2012.

GRALLA, P. (2009). *CIA: Hackers have already attacked the electric grid*.
<http://www.greenercomputing.com/blog/2009/03/26/cia-hackers-have-already-attacked-electric-grid>.

HANG, C.(2004). <http://msdn.microsoft.com/en-us/library/ee798408%28v=cs.20%29.aspx>).
"Network Security – Defence Against DoS/DDoS Attacks". Resource Starvation Attacks.

IDDRISU, H. (2010). Statement By Minister Of Communications Hon. Haruna Iddrisu on 6th April 2010 [<http://www.ghana.gov.gh/documents/meetmoc.pdf>]. Access on 2/9/2012

IDDRISU, H. (2011). Statement by Minister of Communications, Hon. Haruna Iddrisu On Monday, 3rd October 2011.
<http://www.ghana.gov.gh/index.php/information/meet-the-press/7853-statement-by-minister-of-communications-hon-haruna-iddrisu-on-monday-3rd-october-2011>).
Accessed on 2/9/2012

INDIA. India Reports. (2009). "eCommerce in India-A Review": Overview and Reasons for Growth. (<http://www.india-reports.com/articles/ecommerceinIndiaGrowth.aspx>).
Accessed on 10/11/2012

ISO/IEC. 2000. Basic Reference Model: The Basic. Open Systems Interconnection. (www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=20269&ICS1=35&ICS2=100&ICS3=1). Accessed on 3/8/2012.

ITES, (2012). Information Technology Enabled Services [<http://www.ites.gov.gh/>].
Accessed on 20/10/12.

JOYFM. <http://business.myjoyonline.com/pages/news/201203/82958.php>, Accessed: August 12, 2012, 23:22 GMT

KARATZOGIANNI, Athina. (2002). "The Politics of "Cyberconflict".

KAUFMAN, C., "Internet Key Exchange (IKEv2) Protocol," RFC 4306, December 2005.

KESSLER, G. (2000). Defences against distributed denial of service attacks.

<http://www.garykessler.net/library/ddos.html>. Accessed on 2/5/2012

KIM, D., Solomon, M. (2012). Fundamentals of Information Systems Security, Jones & Bartlett Learning.

KPMG, 2012.

www.kpmg.com/GH/en/Documents/Doing%20business%20in%20Ghana%20-2012.pdf. Accessed on 10/12/2012

LEWIS, James A. (2008). *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies.

LEWIS, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic and International Studies.

MATOS, Luis Camarinha 2012. Scientific Research Methodologies and Techniques. <<http://www.uninova.pt/~cam/teaching/SRMT/SRMTunit1.pdf>>. Accessed 30/3/2012

MIRKOVIC, J., PRIER, G. and REIHER, P. (2003): Alliance formation for DDoS defence, in *Proceedings of the New Security Paradigms Workshop, ACM SIGSAC, Ascona, Switzerland*, 11–18.

MIRKOVIC, J., PRIER, G. and REIHER, P. (2002): Attacking DDoS at the source, In *Proceedings of ICNP 2002, Paris, France*, 312–321.

MIRKOVIC, J., Dietrich, S., Dittrich, D. and Reiher P. (2004) *Internet Denial of Service: Attack and Defence Mechanisms*, Prentice Hall, New Jersey.

MIRKOVIC, Jelena, and Peter Reiher. (2004). "A Taxonomy of DDoS and DDoS Defense mechanisms." *ACM SIGCOMM Computer Communication Review*, : 39-53.

MOORE, D., Voeker, G.M. and Savage, S. (2001). "Inferring Internet Denial-of-Service activity. IN *Proceedings of the USENIX Security Symposium*, pp. 9–22.

MTN, MTN Gives Away 21 Million Minutes of Calls. (2012).

<http://business.peacefmonline.com/news/201208/127070.php?storyid=100&Joyfm>,
Accessed on 8/9/2012.

NAGPAL, R. (2002). "Cyber Terrorism in the Context of Globalization." *II World Congress on Informatics and Law*. Madrid, Spain.

NETWORK, Solutions. (2011). <http://dos-attacks.com/2011/06/22/network-solutions-bounces-back-after-ddos/>. Accessed on 2/8/12.

NITA, 2008. eGovernment Network Infrastructure. www.nita.gov.gh/pages.aspx?id=5.
Accessed on 4/6/2008.

SARGA, Libor, Jašek, R. (2011). Distributed Denial of Service Attacks as Threat Vectors to Economic Infrastructure: Motives, Estimated Losses and Defence Against the HTTP/1.1 GET and SYN Floods Nightmares.

SCARFONE, K., Grance, T., and Masone, K. 2008. Computer security incident handling guide. Special Publication 800-61, National Institute of Standards and Technology (NIST). March.

SHACHTMAN, Noah. (2012) *Top Georgian Official: Moscow Cyber Attacked US-We Just Can't Prove It*. <http://www.wired.com/dangerroom/2009/03/georgia-blames/>.
Access 3/9/2012

STALLINGS, W. (2007). *Network security essentials*. Trenton, NJ: Pearson Education, Inc.

STALLINGS, W. (1995) *Network and Internetwork Security*, Prentice Hall, Upper Saddle River, NJ, 1995.

STEWART, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, (2000). "Stream Control Transmission Protocol," RFC 2960.

STONEBURNER, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>, Accessed 3/5/2011

TISN (2006). (Trusted Information Sharing Network) for critical infrastructure protection. "Denial of Service / Distributed Denial of Service MANAGING DoS ATTACKS, June 2006" (ISBN 0 642 75362 8, Commonwealth of Australia 2006).

VACCA, R. J., 2006. Practical Internet security.

VASUDEVAN, R., Morley, Z., Mao, Spatscheck, O and Van der Merwe, R. (2006). Reval: A tool for real-time evaluation of ddos mitigation strategies in *USENIX Annual Technical Conference*.

VERISIGN, 2008. Distributed Denial of Service (DDoS) Attacks: Latest Motivations and Methods, July 11, 2008

VRIZLYNN L. Thing, I. Morris Sloman, Naranker Dulay. (2007). "A Survey of Bots Used for Distributed Denial of Service Attacks". Department of Computing, Imperial College London.

WALDEGGER, T. (2006). Mozilla Firefox HTML Parsing Null Pointer Dereference Denial of Service Vulnerability". (www.securityfocus.com/bid/17499). Accessed on 6/6/2012

WESLEY, M. Eddy, Verizon Federal Network Systems, "Defences Against TCP SYN Flooding Attacks", The Internet Protocol Journal - Volume 9, Number 4.

APPENDIX A: QUESTIONNAIRE

- Q1. Are you aware of DDoS?
- Yes
 - No
 - Not Really
- Q2. Have you ever experience any in your institution?
- Yes
 - No
 - None
- Q3. What in your opinion is the largest Threat Vector perceived by your network today
- Compromise
 - Spam
 - DDoS
 - DNS Poisoning
 - Worms
- Q4. Which of the following attack vector was observed within the past 6months?
- UDP flood
- TCP SYN flood
 - ICMP flood
 - Port flooding
 - http flooding
- Q5. How many times in one month do you experience an Infrastructural attack?
- Once
- 2 to 10
 - More than 10
 - none
- Q6. How do you detect an attack?
- Manual
 - Customers
 - Commercial
 - In house
- Q7. How do you mitigate an attack?
- Intelligent filtering
 - Source-based black holing
 - Alternative routing
 - Other

Q8. What do you think would be the motives behind a DDoS attack if it is to happen to Ghana?

- a. Monetary Gain
- b. Terrorism
- c. Political
- d. Phishing
- e. Revenge
- f. Extortion
- g. None

Q9 Are you aware of any Cyber Crime Laws in Ghana?

- a. Yes
- b. No
- c. Not Really

Q10 Have your Institution ever taken any culprit to a Law Court before?

- a. Yes
- b. No



APPENDIX B: QUESTIONNAIRE DATA TABLE

Distributed Denial-Of-Service (DDoS) Attacks as Threat Vectors to Ghana's
Economic Infrastructure
(Case Of Ghana's Emerging Economy Vis-À-Vis Network Infrastructure)

Name of ISP.....
Address.....
Supervising Technical Personnel (Position).....
Name.....
Signature.....Date.....

ESTIMATING DOWNTIME LOSS

		Estimate	Actual
1	How many working hours overlapping outage time		
2	How much service operation time affected by outage		
3	Percentage degree of service degradation		
4	Annual cost per employee		
5	How much working time per employee		
6	How many Employees affected by outage		
7	How much productivity degradation during outage		
8	Every total annual revenue		
9	How much service operating hours per year		
10	Part of the revenue affected by full outage		

Comments.....

ESTIMATING DISASTER RECOVERY LOSS

		Estimate	Actual
1	No. of employees to be in the recovery team		
2	Cost per hour for a recovery team member		
3	Recovery work hours outside office hours		
4	Cost of material needed		

Comments.....

ESTIMATING LIABILITY COST

		Estimate	Actual
1	Claims from contractual penalties		
2	Claims from other liabilities		

Comments.....

ESTIMATING CUSTOMER LOSSES

		Estimate	Actual
1	Time interval		
2	Number of actual customers lost		
3	Number of potential customers lost		
4	Average revenue per customer		
5	Time interval		

NOTE

Entries under "Estimate" column are for events that have not actually occurred but estimated value can be made based on current market values. The "Actual" entries must be based on events that actually. Year or date of the events must be mentioned under space for "Comments".