Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya
Authors

Peterson Obara Magutu¹,
Gladys Monchari Ondimu¹
and Christopher Jilo Ipu²
Department of Management Science, School of Business, University of Nairobi, Nairobi – Kenya

Department of Political Science, Strategic Security Studies at Faculty of Arts, University of Nairobi, Nairobi – Kenya
Introduction

Background

Cybercrimes poses a great threat to the national security of all countries;
even technologically developed countries like the USA suffer from it (Darpan, 2008). These cyberspace crimes results in companies and government institutions to
lose billions of dollars, for example, the Russian organized crime groups were known to be involved in telecommunications fraud including cloning cellular phones, which cost
billions in lost revenues. The Russian groups also targeted bookmakers and online betting sites and made demands for ransom or threaten to shut down their network if they failed,
their activities costed the FBI, Interpol and other British and Australian authorities millions of dollars in trying to investigate and apprehend
such groups (Mallory, 2007).

Abuse and misuse of computer systems have existed nearly since mainframe computers were
first invented during the 1940s and 1950s as a means to improve military munitions and then rocket guidance systems. By the mid 1970s researchers began studying “computer
abuse” because in those days, harmful activities committed with computers were not prohibited by computer crime laws. By the 1980s all this began to change, with more and
more computers interconnected via the Internet, more abuses of computer systems drove state governments and the federal government to begin passing computer
crime laws. Initially these laws focused on the growing phenomenon of computer hacking, but were soon expanded into other types of criminal behaviors. In effect,
computerization made possible by inventions and innovations in computing and telecommunications technologies also made possible, if not inevitable, the concept of “computer
crime.” This concept, however, became outdated as computer technologies became smaller, more powerful, more affordable, and capable of performing many tasks including
uploading and downloading data files on the Internet (McQuade, 2009).

This social transformations wrought by Internet technologies has made the
future appear insecure and unpredictable, yielding public and political overreaction. Such ‘moral panics’, fuelled by the media, lead to an excessive and unjustified belief that
particular individuals, groups or events present an urgent threat to society (Critcher, 2003). Internet-related instances of such panics include those over the effects of pornography
in the mid-1990s, and more recently over threats to child safety from pedophiles (Littlewood, 2003). The emergence of the World Wide Web, along with a myriad of software
applications, online content, and the beginning of broadband internet connections, computer crime has evolved into computer-related crime and then what we refer
today as cybercrime. Today computer networks are more accurately referred to as information systems.

The largest information system in the world is the
Internet, although there are many regions and parts to this giant network. The Internet is seen as part of the globalization process that is supposedly sweeping away old realities.
and certainties, creating new opportunities and challenges associated with living in a ‘shrinking’ world. We are now said to be in the midst of a ‘new industrial revolution’, one
that will lead us into a new kind of society, an ‘information age’ (Webster, 2003).

Yet, awareness of and enthusiasm for these
changes have been tempered by fears that the Internet brings with it new threats and dangers to our well-being and security. Cyberspace, the realm of computerized interactions
and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities (Yar, 2006).
This has presented a challenge to information technology professionals who lack an awareness of an interest in the cybercrime phenomena. In many cases the law
enforcement officers have lacked the tools needed to tackle the problem; old laws haven’t quite fit the crimes being committed, news laws haven’t quite caught up to the reality of
what is happening, and there were few court precedents to look for guidance (Shinder, 2002).
The Concept of Cybercrime

The concept of cybercrime is not so much different from that of conventional crime as both include conduct, whether act or
omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Current definitions of Cybercrime have evolved experientially and differ
depending on the perception of both observer/protector and victim. The Council of Europe’s Cybercrime Treaty uses the term “Cybercrime” to refer to
offences ranging from criminal activity against data to content and copyright infringement. However, according to Zeviar-Geese (1998), he suggests that the definition
is broader including activities such as fraud, unauthorized access, child pornography, and cyber-stalking. Cybercrime is a subcategory of computer crime and it refers to
criminal offenses committed using the internet or another computer network as a component of the crime (Shinder, 2002).

Schell (2004) defined
cybercrime as a crime related to technology, computers and the internet and it concerns governments, industries and citizens worldwide where cybercrime takes the
form of either piracy, phreaking (obtaining free telephone calls), cyberstalking, cyberterrorism and cyberpornography. Milhorn, (2007) on the
other hand, simply defines cybercrime as any activity that uses the internet to commit a crime.

According to Taylor (1999), when speaking about
cybercrime, usually it is about two major categories of offences. In one, a computer connected to a network is the target of the offence and this is the case of attacks on network
confidentiality, integrity and/or availability. The other category consists of traditional offences such as theft, fraud, and forgery which are committed with the assistance of/or by
means of computers connected to a network, computer networks and related information and communications technology.
Richards (1999) argues that to define cybercrime, it is important to understand the different types of crimes that can be linked to computers, for example, hacking into a telephone.
service to enjoy free telephone calls is a type of computer crime and pirating software is another. Whatever forms computer crimes take, the characteristics that make
computer systems, particularly computer banking systems, so attractive for legitimate purposes, that is, security, efficiency, anonymity make them similarly attractive
for illegitimate purposes such as money laundering. According to Wall (2001), the internet has impacted upon criminal or harmful activity in three ways; first, the internet has become
a vehicle for communications which sustain existing patterns of harmful activity, such as drug trafficking, hate speech, stalking and so on. Newspapers for example,
circulate information about how to bypass the security devices in mobile telephones or digital television decoders (Mann & Sutton, 1998).
Secondly, the internet has created an environment that provides new opportunities for harmful activities that are currently the subject of existing criminal or civil law, for
example, pedophile activity and fraud. Third, the nature of the virtual environment, particularly with regard to the way that it distanciates time and space, has engendered entirely new
forms of harmful activity such as the unauthorized appropriation of imagery, software tools and music products (Giddens, 1990). These three levels invoke different policy responses
and require quite different bodies of understanding. Jurisdictional dilemma is one factor that makes the definition of cybercrime difficult as laws in different jurisdictions define the
terms differently and the lack of concrete statistical data on these offences imposes another major problem. As from the above definitions, Cybercrime can be defined as any crime
that is facilitated or committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or
the target of the crime. The crime can take place on the computer alone, or in other non-virtual locations.

Unauthorized access of hosts more commonly
known as hacking, can take various forms some of which might not always involve deep technical knowledge. It involves using a computer or terminals to crack the
security of some computer systems. Cybercriminals use sniffers or just by guessing passwords to breach security greatly diminishing the effectiveness of passwords.
when users do not select wisely (Adomi, 2008).

Spamming involves flooding the internet with many copies of the same message to multiple
addresses. A spammer sends millions of emails in hope that one or two percent will find their way into inboxes and that a further one or two percent will generate a response.
Spam messages are always sent with false return address information and they are also referred to as junk mail (Milhorn, 2007).
All stages of computer operations are susceptible to criminal activity, either as the target of fraud, the instrument of fraud, or both. Input operations, data processing, output
operations and communications have all been utilized for illicit purposes. The more common types of computer fraud include, fraud by computer manipulation
where intangible assets that are represented in data format such as money-on-deposit or hours of work, are the most common targets of computer related fraud. Modern business is
replacing cash with deposits transacted on computer systems, creating an enamours potential for computer fraud. The organized criminal community has targeted
credit card information, as well as personal and financial information about clients. The sale of this information to counterfeiters of credit cards and travel documents
has proven to be extremely lucrative (Siegel, Saukko, & Knupfer, 2000).

Viruses, Trojans and Worms all fall into a similar category as they are
software designed to infect computers or install themselves onto a computer without the users permission, however they each operate very differently. A typical virus
does two things, first, it creates itself into previously uninfected programs and secondly, it executes other instructions that virus creator has included in it. Some viruses do not have
any harmful instructions at all, instead they cause damage by replicating and taking up disk space (Adomi, 2008). Malicious code is any software program designed to move
from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator. It includes viruses, Trojan
horses, worms, script attacks and rogue Internet code. Computer viruses have been around for almost as long as computers (Grimes, 2001).
Another major element of cybercrime is piracy, which refers to the illegal copying of software and games, movies, music and other digital media. Piracy is relatively easy to undertake
quite often requiring not more than a CD-RW or DVD-R/RW drive that can replicate the original CD's or DVD's on which a particular application is stored. Applications, games,
and music can also of course be simply copied onto the internet for download (Bell, 2004).

Cyberstalking and cyberharrassment has been
described by Yar (2006), as the persistent and targeted harassment of an individual via electronic communication such as email. Cyberstalking has been defined as the
repeated use of the Internet, email or related digital electronic communication devices to annoy, alarm, or threaten a specific individual (D’Ovidio and Doyle, 2003).
Cyberstalking, also called online stalking or online victimisation, shares important characteristics with offline stalking. The similarities are that, first, the majority of cases
involve stalking by former intimates, although stranger stalking certainly occurs in the real world and in cyberspace; second, most victims are women and most stalkers are men.
Third, stalkers are believed to be motivated by the desire to control the victim. Cyberterrorism which has become a very emotive topic partly because of the
dramatic imagery that it evokes using computers to attack the physical infrastructure to generate mass fear and anxiety and, in theory, manipulate the
political agenda (Wall, 2007).

Cyberterrorism is the convergence of terrorism and cyberspace. It has been defined as premeditated,
politically, motivated attack against information, computer systems, computer programs, and data which result in violence against non combatant targets by sub
national groups or clandestine agents. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be
examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact (Khosrowpour, 2004).
The Development of the Internet Service in Nairobi, Kenya

Development of the Internet in Kenya took place in three broad phases.
The first phase, which ran from 1990 to 1998, witnessed the introduction of the Internet largely by Kenyans returning from studies overseas, western expatriates, and personnel
of Inter-governmental Organizations and NGOs. Commercial ISPs entered the Internet market by the mid 1990s, primarily offering dial up and content services. The early adopters
of the Internet included import/export sector, industries with overseas clients and the academic sector. Most of the Internet users then were confined to the Capital City, Nairobi. As
the number of ISPs and Internet users increased, the need for an Internet backbone became evident and the defunct Kenya Posts and Telecommunications
Corporation established one in 1998. The key challenges in the 1990s included limited and high cost of international Internet bandwidth; the high cost of both dial-up
and domestic leased lines; the limited penetration of PCs; lack of policy and regulatory environment; and the lack of appropriate IT skills (Njoroge, 2009).
As described by Njoroge, the second phase took place from 1999 to 2004 with the Government of Kenya restructuring the communications sector with a view to introducing
competition and to pave way for private sector participation. As a result, an independent ICT sector regulator, the Communications Commission of Kenya
(CCK), was established to spearhead sector reform. A number of positive developments took place during this phase, the most notable were the establishment of an
Internet Exchange Point (IXP) by the private sector and the successful re-delegation of the administration of dot KE ccTLD through a public private partnership. The
elapse of Telkom Kenya’s exclusivity in June 2004 in the provision of various services including Internet bandwidth marked the grand entry of the third
phase of Internet development in Kenya.

The ICT industry had been anxiously waiting for the lapse of the exclusivity to have a share of the services
hitherto reserved for the incumbent. The most notable features of the post-exclusivity regime was introduction of competition in all business segments previously reserved for the
incumbent, including internet backbone, Voice over IP, satellite and international voice gateway services. In addition, the regulator expanded competition in the cellular
mobile telecommunications market from two to four networks, triggering off the deployment of a wide range of innovative products and services, including mobile Internet and a host of value
added services such as, M-Pesa. As a result of this new wave of reforms, coupled with increase in the penetration of PCs and in the level of IT skills, the number of regular Internet
users in Kenya increased to the region of 3 million out of a total population of 35 million.

The deployment of national broadband fibre
optic connectivity to take advantage of the three submarine cables competing to land at our coastal city of Mombasa is expected to lower the cost of Internet access and thus spread the
digital dividends to a bigger proportion of Kenyans. The projects will also make e-government a reality in the country. Today, a number of mobile companies are providing 3G mobile
Internet services at very competitive rates and with the recent adoption of the Unified Licensing Regime, there is no doubt that Kenya should have close to
50 per cent Internet penetration by 2013.

Statement of the Problem

The research intended to establish the types, impact
and mitigations of cyber crime with the deployment of fibre optic cable in Kenya security.

Kenya had not attracted this sort of cyberspace
crime largely because of the slow Internet connectivity which had been available only in selected urban centers. The recent emergence and development of the
broadband fibre optic connectivity will certainly and inevitably expose Kenya to high levels of Cybercrime. This research intends to study the forms of cybercrime in Nairobi
and the emerging threats brought about by the recent internet development through the fibre optic cable.
Although cyber-crime has been around for nearly 30 years, research in the area has been sparse (Chandler, 1996). A major problem for the study of cybercrime is the absence of a consistent
current definition even among those law enforcement agencies charged with tackling it (Yar, 2006). As Wall (2001) notes, 'the term has no specific referent in law', yet
it is often used in political, criminal justice, media, public and academic discussions.

Research of cybercrime is in its infancy, this is
because knowledgeable individuals and institutions both in the public and private sectors may for commercial, political or national security reasons be disinclined to share their
wisdom with researchers (Roderic, 2005). According to Yar (2006), our awareness of the Internet’s criminal dimensions has certainly been cultivated and heightened by mass
media representations. The news media have played their part in identifying and intensifying public concerns, and hardly a day goes by without some new
report of an Internet-related threat.

According to one of the studies by Tushabe and Baryamureeba (2005), cybercrime was found to be
silent but common in East African countries and concluded that cybercrime is a serious threat to the security of cybercitizens and all countries should take it seriously. Their
study realized that cybercrime instances are mainly discussed socially and the victims suffer in silence, while the perpetrators continually hide under the invisibility
of the cyber world and it is hard to convict cyber criminals because of two major reasons. Firstly, few countries have enacted e-laws and the existing ones are not sufficient in
convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime
that would stand in courts of law is lacking in many countries since the field of computer forensics is still relatively new and
lacks sufficient literature and expertise.

Although a number of researches had been done on the cybercrime, none had focused in Kenya,
particularly Nairobi. The Kenyan internet structure has seen a revolution with the emergence of the fibre which will place Kenya at the same level as first world economies and will
certainly drive growth especially after a time that Internet in Kenya has been referred to as being inadequate, inefficient and of high cost. The advent of high speed connectivity will
draw the attention of local and international hackers who were previously put off by the amount of time it took to break into local websites using slower satellite connections, this is
because Nairobi is slowly being recognized as a regional hub for internet connectivity not only in Kenya but regionally and this is largely being driven by affordable and reliable
Internet connectivity projected from the emergence of the fibre optic cable. (Kinyanjui, 2009). Recently, Hewlett Packard (HP) made Nairobi the regional hub for East
and Southern Africa for its Personal Systems Group, where The Nairobi office will serve 18 sub-Saharan countries (Ngunjiri, 2008).
At this moment, the most serious threat to the economy is seen as the lack of security online. This study therefore seeks to identify the different forms of cybercrime prevalent in
Kenya, with Nairobi as the case study and the effects of these threats on security. Also the study sought to identify the emergent threats imposed by the recent internet
development through fibre optic and its probable implications on security. The research questions were:
• To determine the types of Cybercrime prevalent in Kenya;

• To investigate the impact of cybercrime on Kenyan security.
• To assess the security employed by ISP’s & other organizations to curb cybercrime as imposed by the recent fibre optic development in Kenya
Research Strategy

The guiding principles here were the objectives of the study. A survey research design sought information about the effects of
Cybercrime on state security in Kenya. This study had the privilege of providing in-depth analysis on the recent internet development in Kenya and
the challenges it imposes on state security.

The population of the study consisted of the fifty one (51) ISP’s in Kenya registered by the CCK, it
will consist also of the CID who hold vital statistics to cybercrime reported in Nairobi, and the CCK who enforce regulations on all registered ISP's in Kenya, currently there're 51 ISP's
registered by the CCK (See Appendix I). The research targeted the IT staff in the above selected study population (both in the Senior and low level management). The sample
frame constitutes of both the Senior and Junior management level where simple and stratified sampling was employed to select the respondents in this study. Stratified
sampling was used to ensure that the various entities in the population are well represented in the sample and to ensure accuracy. With Simple Random Sampling, a
random sample was selected such that every element in the population will have an equal chance of being included into the sample and the respondents selected will
each be interviewed discretely.

The mechanisms employed in data collection included the use of both questionnaires and
interviews (See appendix II). The questionnaires were preferred in this study because those who took part in this study were considered to be literate and capable of answering
the questions sufficiently. For quicker response the use of email to administer the questionnaires was employed, apart from personal visits to the respondents where a drop
and pick later approach was employed. Interviews were conducted with the use of both structured and semi-structured modes of interview. Telephone interviews were hereby
preferred to facilitate the research especially for areas where physical access to respondents was limited, for example, the Criminal Investigation Department (CID). The questions were
structured in such a way that for fixed response questions were rated against five points scale, from extremely significant (5) to not significant (1). Room was provided for
personal responses not captured in the fixed response-questions. The responses that were obtained were compared to the literature review to establish the significant
implications of cyber-crime on security.

The data from respondents was analyzed using descriptive statistics such as means, percentages and
tables. SPSS (Statistical Package for Social Scientists) was used to analyze the data.
Data Analysis and Findings

Data was collected from (51) institutions with only 35 of them responding.
Cybercrime is simply as any activity that uses the internet and computers to commit a crime. All the IT staff interviewed consented to their knowledge and
existence of Cybercrime in Kenya.
Forms of Cybercrime Prevalent In Kenya

There are a number of forms of cybercrime. The respondents were asked to indicate the forms of
cybercrime prevalent in Kenya, on a five likert-scale where Very Great Extent = 5; Great Extent = 4; Average extent = 3; Small Extent = 2; Very Small Extent = 1. The
results are shown on table 4.1
Table 4.1 Forms of Cybercrime in Kenya

Please see table 4.1 in full PDF version
From the results in table 4.1, it was found that, Spam, virus and trojan attacks, hacking and piracy, were the leading cyberspace crimes experienced by IPSs. Most of the reports to the
given data were reported to the system administrators where victims hoped to recover lost or damaged data. Otherwise most victims preferred to keep quiet because they do not
think reporting would help them since preserving evidence is unknown to them. These statistics show that Kenyans and internet users are initiating and falling victim of cybercrime,
although the public are not reporting to the relevant authorities either because of non-existent sensitization programs or hopelessness due to the
unavailability of e-laws that would bring them justice.

Other cyberspace crimes that are emerging include; Cyberespionage, Denial of Service attacks,
Cyberterrorism and Cyberstalking. These can be explained to be at the bottom of the table largely as a result of the fact that, internet in Kenya is still developing where internet
is still expensive and limited but once the fibre connectivity is fully operational these threats are feared to be escalated, since internet will be readily available at cheaper
rates and bandwidth connectivity will compare to first world economies. Cyberterrorism the most feared of them all poses a great danger especially as the government plans to
inter-connect all its ministries through e-governance. It faces a deadly threat where its operations may be interrupted through denial of service attacks that could
cripple vital services. Again, cyberespionage may be used to steal or expose critical information by covert organizations intending to sabotage the state.
According to the Criminal Investigations Department (CID), in January 2005 [11], a multi-million dollar scam involving a fraudulent intranet bank transfer between Standard Charted
Bank, Nairobi and Barclays Bank, Kampala was unveiled. A prominent Ugandan businessman and construction magnet, Andrew Zzimwe Kasagga together with two
Congolese nationals were wanted by Interpol (Kenya) over accusations of masterminding the bank fraud that saw Kenyan Standard Chartered Bank staff wiring to them $5
million in three installments to separate bank accounts and recipients in Kampala. Suspected conmen got the Nairobi based bank to wire one million dollars to
Zzimwe’s Barclays Bank account in Kampala and another $2 million from Kenya was intercepted at Crane Bank. It had allegedly been sent to another suspect, Kampala lawyer,
Paul Kalemera. Further investigations and trial are being conducted. Another $3 million being swindled from Kenya was detected before it was sent to forex
bureaux via the DFCU bank in Kampala.

Also according to an article published in the Nation newspaper on 8th August 2009, child pornography is
on the high increase, where internet development in Nairobi has enabled criminals to promote this vice. According to the article, pornography materials are easily
downloaded from the internet and burned using DVD/ Writers and the DVD's sold for as little as 300, what is alarming is the fact that children as young as nine years were watching
the movies that were also openly advertised on the Nairobi streets.
Challenges Curbing Cybercrime

There are a number of strategies employed by various organizations some specific to particular
cybercrime forms and some general for instance, antispam which is specific to preventing the proliferation of spam mails into client accounts which is also a part of CCK
requirement to ensure that clients are protected. General strategies against cyber crime include use of firewalls and bandwidth shaping tools, for instance, the Canadian developed
Sandvine equipments which limit bandwidth choking and efficient way of controlling piracy. To satisfy one of the specific objectives outlined on the first chapter, on the
challenges faced by ISP's in curbing cybercrime, it was necessary to query the respondents further on the specific challenges they face in fighting cyberspace crime. On an interview with
a senior management staff at Orange Telkom staff observed that the use of bandwidth shaping tools allowed them to control how users on the cyberspace downloaded
media files such as movies and music, this strategy not only prevented the users from starving other users from bandwidth but also controlled to some extent
the piracy of copyright materials.

The respondents, therefore, were queried on a number of challenges they are facing in fighting
cybercrime in Nairobi. This was on a five likert-scale where Very Great Extent = 5; Great Extent = 4; neither agree nor Disagree = 3; Small Extent = 2; Very Small Extent = 1 where the
higher values represented the extent to which the challenges had been overcome, on the other hand, the lower values represented the challenges that were still difficult to
eradicate. The results are shown below on table 4.3
Table 4.2 Challenges Curbing Cybercrime

Please see table 4.2 in full PDF version
From table 4.2 it was found that to a great extent (mean>4), most of the ISP’s in Kenya had employed skilled personnel who were knowledgeable in combating cybercrime, also
there was low resistance to change when strategic measures were being implemented, there was also satisfactory software evaluation that also ensured there were
minimum compatibility issues experienced. Finally the ISP’s had also invested in conducting management training that presented the staff with the relevant knowledge of cyberspace
crime that was constantly changing and the means necessary to combat them.

On the other hand, from the table 4.2 we draw conclusions that the cost of
combating cybercrime in terms of purchasing the necessary equipments and applications, employment of skilled personnel and other strategies constituted a large portion of ISP
budget. Apart from purchasing software firewalls the respondent revealed that it was becoming necessary to also purchase hardware firewalls together with
bandwidth shaping tools to minimize the emerging crime such as piracy which also choked the network, that is, it prevented other users from accessing bandwidth. Ignorance by
both staff members and the public was also a great hindrance to the fight against cybercrime which to a great extent was as a result of lack of awareness that this type of crime
exists, thus, users of the internet will fail to employ the measures required in order to safeguard themselves when on cyberspace, it is important to note that a single client
infected by a virus is enough to infect other clients and servers on the network. Therefore, individual responsibility is a challenge that great
undermines the fight to eradicate cybercrime.

According to the Criminal Investigations Department (CID) there are a number of challenges that have largely
constituted to the poor control and eradication of cybercrime in Nairobi. Table 4.2.1 outlines the results as provided by the CID.
Table 4.2.1 Challenges Curbing Cybercrime

Please see table 4.2.1 in full PDF version
According to table 4.2.1 the greatest to challenge to cybercrime include, poor legislations presently in Kenya that are essential in combating cyberspace crime, authorities cannot
obtain permission to search and prosecute offenders of this crime without proper laws that will enforce them, for this reason, cybercriminals do not have the fear of being
apprehended and continue to commit this crime. The issue of jurisdiction also makes on one country irrelevant for instance, a crime committed in Uganda where cybercrime laws are
ineffective or non-existent makes apprehension almost impossible.

The lack of sufficient resources for instance, funds which would enable
authorities purchase equipments and applications, necessary to collect evidence and also applications and instruments to detect and prevent such crime from
happening are quite limited. Finally, lack of awareness to this type of crime and also lack of relevant skills constitute to the remainder of these challenges, where
legislators who are responsible for enacting laws cannot enforce into law what they do not understand. Authorities on the other hand, lack necessary skills that afford
them the capacity to employ efficient strategies in detecting and in collecting digital evidence crucial in prosecuting cyberspace offenders.
Preventing Cybercrime

Presently in Nairobi, Kenya, local ISP’s are adopting a number of measures as directed and required by the CCK in order to
establish client or user security and also ultimately reduce cybercrime. These measures vary and they are primarily instituted to control cybercrime from the public as much as
possible, who largely are not aware that this crime exists. The ISP’s also find themselves going a notch further than CCK’s standard requirements to adopt different other strategies to
curb cybercrime. The advent of the cyber optic cable also symbolizes a new information revolution age in Nairobi as internet is expected to be much more affordable and internet
bandwidth will be offered at much more faster speeds, competitive with those of the first worlds. The respondents were asked to identify the various strategies they had
employed in order to curb cybercrime. This was on a five likert-scale where Very Great Extent = 5; Great Extent = 4; Average extent = 3; Small Extent = 2; Very
Small Extent = 1. The responses are as table 4.3.
Table 4.3 Preventing Cybercrime (Descriptive Statistics)

Please see table 4.3 in full PDF version
From the results in table 4.3, it was found that to a great extent (mean > 4) the ISPs have focused on employing antivirus applications, software and hardware firewalls,
antispam applications, data recovery and staff training in an effort to control cybercrime in Nairobi. Although there is an indication that ISPs have tried to focus on ways of
preventing cybercrime, other important areas such as parental control which can be an effective measure against cyberpornography and also penetration testing to identify loop holes that
can be exploited by cybercriminals, haven’t yet been optimized. From the statistics gathered on prevalent forms of cybercrime in Nairobi, it was observed that
Cyberpornography which also encompassed childpornography was steadily on the increase, the use of parental control or enforcement of this feature could mean that this
emerging crime can be controlled before it becomes a grave concern.
Summary and Conclusions

Conclusions

In line with the general objectives of the study, the
following conclusions were arrived at. Based on the results from data analysis and findings of the research, the study has revealed that cybercrime is silent but
common even in developing countries like Kenya and the following conclusions were arrived at, based on the objective of the study; Firstly, it was observed that a number of
cybercrime forms were prevalent in Nairobi most notably spamming, hacking, use of malicious code through viruses or trojans and lastly piracy. These ultimately pose a more
security risk with the emergence of the submarine optic fibre which promise faster internet speeds through higher bandwidth and most importantly at cheaper and
affordable rates, giving cyberspace criminals and added advantage at perpetuating there crimes. With the country and the government on the verge of instituting e-commerce to
all its ministries in Kenya, it means that if strategies will not be put in place then there is a National Security risk posed through hacking, and cyberespionage where the government may stand
to lose vital information or by having their websites denied access for instance, through denial of service bombs.
Secondly, the major focus on cybercrime employed by organizations in Nairobi was on providing means of curbing cybercrime that exist rather than finding ways of preventing them.
from occurring. As observed, currently spamming, hacking and piracy are at the forefront common forms of cybercrime employed by
cyber criminals. ISPs especially, are purchasing expensive antivirus applications and firewalls to remove virus infections while ignoring preventive solutions such
as, blacklisting specific IPs that are related to crime, which could be either pornographical websites, phishing sites or even sites that are known to host viruses. In some first world
countries, torrent sites that proliferate the piracy of copyrighted material are blacklisted as a government directive, through tough legislations.
Thirdly and most importantly is that organizations in Nairobi, that is, both ISPs, the CCK and the CID use a lot of resources in an effort to curb cybercrime. The
Communications Commission of Kenya has set out on an exercise to educate consumers on cybercrime and other threats posed by the expected increase in
Internet usage as a result of cheaper bandwidth. Expensive connectivity has limited the region's Internet penetration and electronic commerce is nonexistent, so,
cybercriminals have not targeted that area as much as South Africa. The lack of awareness, ignorance and poor legislations have greatly contributed to slow
progress against the fight against cybercrime.

Furthermore, it is hard to convict cyber criminals because of two major reasons. Firstly, few
countries have enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends
international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries since the field of computer forensics is still
relatively new and lacks sufficient literature and expertise. Cyber crime is a serious threat to the security of cybercitizens and all countries should take it seriously.
From the above it is clear, beyond reasonable doubt that if proper strategies are not put in place to curb cyberspace crime especially with the recent internet
development, then Cybercrime posses a great threat on Security in Nairobi.
Recommendations, Limitations and Suggestion for Further Research

Prevention is best solution to curb the increasing...
number of security violations on the net. However, it may not be feasible to prevent all incidents, and that is when two major factors come in play. Firstly, forensic
knowledge and expertise, followed by the relevant laws that would empower victims to seek justice. This can be achieved through a number of measures discussed below.
There is a need for setting up a public facility (preferably with a presence on the internet) where victims can report incidences. The public need a lot of sensitization and
training on what computer crimes are, in which forms they can manifest, how to detect them, what to do after detection and how to prevent and minimize them. The Police should
also endeavor to build trust and confidence in the population by using the media and otherwise, so that more such incidents are reported to them for
proper and unified record keeping.

Countries implementing Internet filtering at client, Internet Service Provider (ISP) and government
levels would prevent access to illegal websites like those promoting concepts like drug use, gambling, immorality, pornography, bomb making recipes, terrorism and the like.
Legislative organs can mandate a body to filter all incoming web traffic before it is accessed by Internet users in that country and block away websites that pose security threats to the
users. Internet Service Providers are also in position to protect their clients against most cyber attacks like distributed denial of service attacks, email spoofing, spam and
the like if they were only allowed to do it. Enacting global cyber laws that deal with harmonization and standardization of computer crime would
bring us closer to attaining total justice to cybercrime victims. Although a number of countries have enacted cyber laws and have punished criminals within their jurisdiction, they are
dominated by the developed countries. Most developing countries have not yet enacted e-laws. Harsh punishments should be given to defaulters so that people fear to commit
these acts and victims be motivated to report them. This would prevent escalation of cases and further loss of money, time, data and equipment.
On the other hand, Third World countries like Kenya which already have laws related to cybercrime should have their legislations revised to keep up with the emerging
cyberspace threats, as criminals are coming up with new tricks to evade the law and process of prosecution.
The greatest constraint in carrying out the research was time factor. Some of the respondents had little information hence giving out data which was not satisfactory and needed
more input. Due to poor means of communication it took long to visit all branches and this led to arriving when some of the managers had left for meetings and others home,
again because of shortage in time the research had to rely on telephone interviews. It also took a while when collecting the questionnaires because some of the respondents
kept them or even failed to reply to the questionnaire sent via email. There was also poor coordination and assistance from government organizations that were critical to this
study, especially the CCK (Communications Commission of Kenya) and also the Criminal Investigations Department (CID) who failed to present the research with vital
statistics on cybercrime, the organizations insisted on a letter signed by the Commissioner of Police in order to access the materials which time could not allow.
Areas of further research that were identified include a similar study to be carried out on other sectors of the ICT sector, for instance cybercafés where cybercriminals identify to
carry out their criminal activities. Other areas of study should include law enforcement and the fight against cybercrime that they employ in Nairobi, Kenya, a vivid statistical
data is vital in order to understand the dynamics of cybercrime and their threat to security. Crucially further research should be done to explore new techniques and procedures
that will combat the rate at which cyber crime spreads and the ease at which they can be conducted.
References


Coleman, J. W. (2002). The Criminal Elite:

Council of Europe. Octopus Programme, (2004). Organised crime in

Buckingham: *Open University Press*.

Journal of management studies.


Debra Littlejohn Shinder, Ed Tittel. (2002). "Scene Of
The Cybercrime: Computer Forensics Handbook,

FBI law enforcement bulletin.


Cybterterrorism,' *The International Library of Essays in Terrorism.*

Acquisition in Cyberspace, "Cambridge University Press.


Idea Group.

Available: http://www.businessdailyafrica.com/-


Press, Westport USA.

Office of Investor Education and Assistance

Organizations, Cybercrime, and money laundering,’ CRC Press LLC, New York.

Roderic, G. Et al. (2004). ‘Cyber-crime: The Challenge in Asia,’”
University of Washington Press, USA.


Sylvester, L. (2001). ‘The Importance of Victimology in Criminal Profiling,’

Sublime,” Routledge, London

The Kenya Communications (Amendment) Act,
Available: http://www.cybercrimelaw.net/

About the Internet,” No starch Press.


Yin, R. K. (1994). Case Study Research: Design and


Cyberjurisdiction and Cybercrime on the Internet," Gonzaga University.
Appendix I: Telecommunications licensed service providers

Appendix II: Questionnaire
Please see Appendix I and II in full PDF version