E-Crime; A Digital Syndromme That Needs To Be Cured

Virginiah Sekgwathe
Directorate on Corruption and Economic Crime
DCEC
Gaborone, Botswana
e-mail: veesek@gmail.com

***Abstract*—**The internet has weaved and knitted the geographical boarders together and is a powerful tool for development paradoxically it provides criminals an avenue to perpetrate crimes with relative anonymity simultaneously making investigations of these high tech crimes too complex and not easily decipher-able. E-crime affects our daily lives, more so that our lives today is ruled by technology and revolves around the internet. The tremendous increase in communication devices, the ease at which we virtually connect globally and the fact that business is now conducted online has been accompanied by an equal rise in the number and type of attacks against the security of these online systems, business and services. The practical implications of this paper is to remind the International community, government, business organization, academia, executives (policy makers and legislators), and of course individuals, that e-crime is a global syndrome requiring full participation, awareness and cooperation in order to find not just a sustainable cure and deterrence, but also to bring offenders to justice, consequently making the cyber space more virtually habitable and safe.

Keywords- *e-crime; online crime; internet perpetrated crime*

*****

I. INTRODUCTION

The ubiquity of computers, accessibility of internet everywhere, anytime and at affordable cost, furthermore the mobile phones capabilities to connect to the internet [Sekgwathe V. andTalib M] has resulted in the acceleration of its usage not only in promoting education, business growth, etc, but has also continually provide the criminal elements of the society, the greed motivated individuals the opportunity to also utilize this technology, to defraud, cause terror, revenge, steal identities, cause disrepute, extort, cyber bull and commit all sorts of crimes hence the rise in e-crime.

E-crime has become an International phenomena hitting all onlineindividuals, governments, business, industry etc, at the same time rendering the capability of the law enforcement, judiciary, and prosecution under uncertainty [Talib M. and Sekgwathe V.]. The successful detection, prosecution, tribunal and judgments of e-crime cases requires an extensive understanding of e-crime, technology used and artifacts of e-evidence. The escalation in the use of digital cash and credit cards of course aided by communication technologies and the internet endow with a greater incentive to digital criminals. The International community at large need to understand criminal activities that is prevalent and persistent in the digital world with a view to curtail attacks and encumber the success of attacks on individuals, governments, organisations, businesses etc. This obligates constant revamp of legislations internationally, ceaseless systems and infrastructure security audit and that the cyberspace be constantly regulated in order to achieve independent in depth analysis of this international phenomena and of course accomplish cyber justice and deterrence.

II. E-CRIME DEFINITION

Association of Chief Police Officer (ACPO) of England defines e-crime as the use of networked computers, telephony or Internet technology to commit or facilitate the commission of crime [ACP e-crime strategy]. For the purpose of this paper e-crime is defined as crimes committed through the usage of Internet and Communications Technology (ICT), aided, facilitated and/or directed towards the automated systems, these includes but are not limited to identity theft, E-commerce scams, salami attacks, cyber stalking, e-services scams, financial fraud, privacy, ICT networks attack, personal data intrusion etc.

III. PURPOSE AND SIGNIFICANCE OF STUDY

The purpose of this study was to investigate the nature and extent of e-crime, viewed for the purpose of this study as a syndrome, as its associated symptoms and characteristics are visible and experienced by all individuals, governments, business, industry etc., irrespective of their geographical location. The findings of this study are intended to assist in providing sustainable cure for this digital syndrome.

IV. RESEARCH METHODOLOGY

The study was carried out using secondary data, all sites that are specifically for cyber-crime incidents such as the Internet Complaint Centre (IC3), were visited and statistics collected therefrom, including some academic journals and news sites with a view to find statistics, the type of cyber-crime experienced by victims and the prevalent ones. The aim was to examine the nature, extent and the impact of the syndrome on the international perspective.

V. AN ANALYSIS OF E-CRIME AS A SYNDROMME

A syndrome is defined in medicine and psychology as "association of recognizable features, signs…or phenomena or characteristics that often occur together". E-Crime is a syndrome in the sense that it has recognizable features and signs, for instance leaked automated and confidential information is a sign that there has been an intrusion and probable theft of information or simply an internal system security compromise. Whether the intrusion is internal or external it mandates expedited investigation to find out how it occurred, extent, cost and remediation. It is used in this paper to refer to a combination of phenomena seen in association as outlined by figure 1. E-crime has a number of essential characteristics that require to be studied and analyzed and well understood ultimately its economic impact, and its cause and effect well established. This study found that not all countries have appropriate legal and regulatory frameworks to address this syndrome and its impact on the economy, national security and the populace at large.

In this Information and Communication Technology epoch, where data is viewed as the zeros and ones, crime has revolved and crime that prevails is of high tech, and constantly torments security and safety of online users and transactions. The pervasiveness of computers has resulted in the inescapable human interaction with them, sometimes even unaware, this translates into the fact that our lives are ruled by the zeros and ones, we live in the digital world, the virtual community. In this man-made space, the cyber space, all things are man-made, to a level that even the very nature of crime has revolved, unlike conventional crimes these type of crimes are committed within the virtual place and law enforcers need to be cyber savvy. The victim and the perpetrator may not know each other and may not be in the same locality, as e-crime has no respect for geographical boarders. In the cyber world anonymity may be guaranteed and mostly there are no eye witnesses to testify about what they actually saw happening, hence this brings about challenges of admissibility of digital evidence in a court of law. The crime scene in this phenomena is not just virtual but highly technical requiring expertise to reconstruct this seriously transformed, digital crime scene, the crime scene made up of chips and wires. It requires an expert to testify of what really occurred in the virtual space, within the chip, this has brought about devastating challenges to all stakeholders concerned that is the Judiciary, Law enforcement, prosecution, business industry etc [Sekgwathe V. and Talib M.]. For centuries law enforcement agencies have been dealing with the physical crime scene, where evidence and exhibits are visible, vibrant and straight forward, for instance when there is a case of theft it is evident to the reporter that the thing reported stolen is in fact missing, this is not the case with the zeros and ones, as information stolen doesn't necessarily mean the physical/manual file or automated records are missing or have been deleted, rather some confidential information may have been leaked and worst case scenario it may be publicised. Cyber criminals decide where and how to commit the high tech crime on the basis of the value of the target and ease of attack, just like conventional crimes their main aim is to get wealthier and evade arrest and prosecution, so their main target is lax security. There are several questions that need to be answered:

- What is the nature of e-crime?
- To what extent does e-crime affect Individuals, governments, business and the International community at large?
- How does these governments, business?
- How do Individuals, governments, business and the International community guard against e-crime?

While e-crime requires application of forensic techniques in data extraction for those investigating, prosecuting and those ultimately passing judgments in regard to disposition of offenders and the redress of offenders. The e-criminals are mostly technologically advanced and the law enforcement have resorted to the aid of the forensic tools, though in most countries the academia, prosecution, judiciary and business have been left behind, consequently impeding on the success of this battle. On the other hand there is yet another challenge brought about by the e-criminals who are always abreast in researching current technologies and how they can use technology to enrich themselves. This necessitates the academia, prosecution, judiciary and business to fully understand the syndrome as needing partnership as such keep abreast with the cyber forensic tools, the legislation, their capabilities and limitations.

The framework below (Figure 1) depicts the nature and characteristics of e- crime glimpsed through uniqueness of the internet as the study concludes that it is through the internet that e-crime has become so invasive and ubiquitous, it is a lethal but invisible weapon compelling that prior to its usage, and during the course of its utilization, individuals need to be sensitized on how to be safe online.

VI. IMPACT OF E-CRIME

E-crime is not just a menace of the 21st century, it is here to stay mainly due to its anonymity and less riskier nature, coupled with its success rate and high lucrativeness, this was also noted by Stephen Trilling "*Today's criminals are using more sophisticated attack such as ransom ware and spear phishing which yield them more money per attack than ever before"* The findings from Norton 2013 reports are that *" 49% of consumers use their personal mobile device for both work and play, this creates entirely new security risks for enterprises as cybercriminals have the potential to access even more valuable information."*

According to a study conducted by Ernest and Young their finding were that the exact impact of e-crime is often underestimated or unknown hence the disastrous economic impact of these attacks is not well established. Several questions are left unanswered, how do countries, law enforcement agencies, business etc protect their nations and clients, how do they develop strategies to tackle this digital syndrome if they don't quite understand this phenomena. Then how do countries plan, estimate,and allocate the resources to fight the battle they don't quite comprehend, hence this is a vicious cycle.

However there are estimated loss [IC3, InfoSec, 2013]. For instance the US Federal Deposit Insurance Corporation reported that in cybercrime trend news, businesses lost $120m in the third quarter of 2009 to phishing and Trojan-based online banking scams, and that small businesses lost $25m as part of these scams. Norton 2013 report reveals that global direct cost of cybercrime (US$113 billion; up from $110 billion) and the average cost per victim of cybercrime ($298; up from $197) increased in 2013. According to statistics for reported and recorded cyber-crime statistics from the Internet Complaint Centre (IC3), they received 2013, 262,813 consumer complaints which according to their report has an adjustment dollar loss of $781,841,6111, which is a 48.8 percent increase compared to the losses reported losses in 2012 which is $581,441,110. In 2012, according to the IC3 report 289,874 complaints were receivedand processed, which averages more than 24,000 complaints per month [IC3 2013 report, 2013 cyber-crime impact report by InfoSec]. In accordance with the Norton 2013 report, there is an unverified intensification of 8.3 percent losses reported to IC3 over the previous year, which is 2011. This clearly indicates a very significant and distressing augmentation that mandates not just attention by the International community, but also exhaustive and systematic understanding, planning and research in this area.

E-crime phenomena prompted the International community to come up with several international assistance programs such as International Cyber Crime Assistance Program [www.icspa.org] and initiatives such as International Telecommunications Union (ITU) Online child protection initiative [www.impact-alliance.org] with a view to promote international cooperation and joint effort and protect children online respectively and aiming at continuing and possibly winning the fight.

E-Crime Framework: This is an analysis of e-crime as a syndrome with visible features and signs

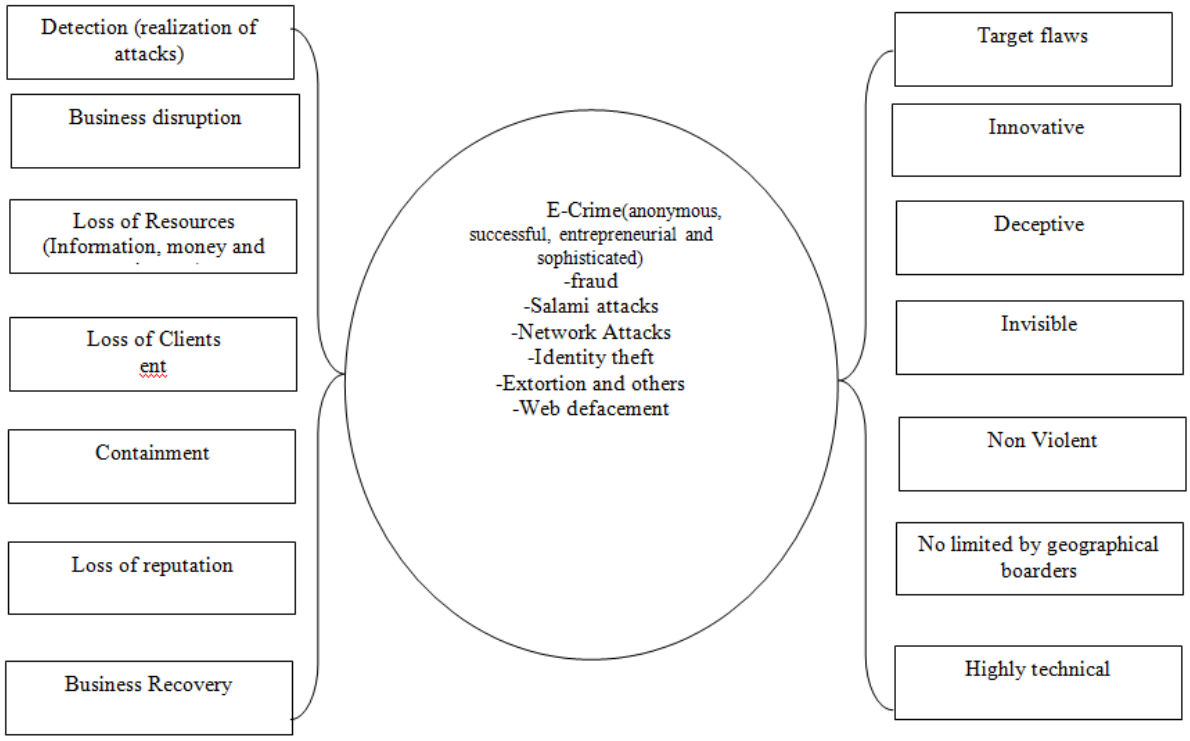

Fig. 1- E-Crime Framework

VII. BOTSWANA SCENARIO

This study emphasizes that no country can afford to place a blind eye on this phenomena, and all countries just like Botswana experienced this, for instance Botswana recorded and reported incident of this syndrome in 2000.In this particular incident, a Bank of Botswana employee electronically transferred over P2million to an account outside the country from the Bank that he was an employee in [Botswana Daily News]. This was the first incident of its kind and the country back then did not have any cyber-crime act or Information and Communications act subsequently, the country was left with no alternative but to use the penal code [Fombard CM and Quansah EK; Penal Code Act of Botswana] despite the fact that technology aided the accused to commit fraud. This prompted the country to come up with a cyber-crime bill, which ultimately became the cyber-crime act of 2007.

VIII. DISCUSSIONS

This study revealed that the actual statistics is unavailable, this unmistakably means the battle against this phenomena is

far from over, it is just beginning and it will be difficult for the International community to fight a battle that is not quite understood, as Lord Kevin stated "*When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot express it in numbers your knowledge is of meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely advanced to the stage of science"*– [Quoted by Jeanne MagerStellman]. All nations, all countries irrespective of their economic status, both developed and developing countries, need to understand the nature, extent and impact of this phenomena. Nocountrycan afford to place a blind eye on this phenomena, and all countries just like Botswana experienced this, therefore partnership is required in order to win the war.

E-criminals are characterized by showier personae for their rambles as they can stride past law enforcement without any fear of being arrested, mainly due to the anonymity of e-crime and the availability of third party anti-forensics software [Marcella A and Doug Menendez] that are freely available for download and may easily be used to cover the criminals tracks consequently assisting them to evade prosecution [Sekgwathe V. and Talib M.]. Their non-violent and deviant nature has contributed to most countries tight-lipped in coming up with legislation to impede e-crime and regulations to control the cyber space and these high tech and sophisticated criminals.

The Cyberspace has illuminated the truth of the zeros and ones reflection of intelligence, and its virtual locality makes it not just a virtual reality and transcend physical limitation of deceptive appearance but also a criminal harboring place in possession of a lethal weapon known as the internet.

E-crime is omnipresent, omniscient and omnipotent and its impact is felt by individuals who have been victims of identity theft, governments who lost information [Europol] due to cyber-crime.

The findings from this study concludes indeed there is a serious digital syndrome that comes in different sizes, dimensions, complexity, sophistication and its quite deceptive due to its imperceptible nature, it is not well quantified [IC3 2013 report] due to the fact that most organisations do not report these crimes. However this requires methodical and in depth understanding hence need to be studied with a view for countries, communities, business etc not only to protect their nations, individuals, clients but also to understand and examine future threats and come up with informed strategies and probably develop countermeasures.

E-crime has become entrepreneurial since e-criminals can now sell their services such as hacking services, malicious code [InfoSec, Impact of cyber-crime report, 2013] to other criminally minded individuals or syndicates to conduct criminal activities online and defraud, hack, attack systems, steal information utilizing these hired products or services.

The study therefore recommends;

A. Mandatory Reporting Internationally

The cure of this syndrome may not be found until and unless the statistics, nature and extent of the syndrome are well understood and documented [Sekgwathe V. and Talib M]. This calls for mandatory reporting and guaranteed protection of victims (attacked organization, individuals etc) to guard against revealing vulnerabilities and inducing further attacks and of course credibility and loss of business [Talib M. and Sekgwathe V.].

B. Implementation of Analysis of Intrusions

An obligatory enforcement of the implementation of intrusion detection systems [Talib M. and Sekgwathe V]. There is a need for governments and the International community at large irrespective of their geographical location, to endeavor for earlier detection of intrusion and response, which may also be used as a control measure.

C. Private Public Partnerships (PPP)

The effects and impact of e-crime, its deceptive nature calls for partnership or rather joint effort in the fight against this phenomena. If companies, government, individuals, industry, business can have platforms to discuss,share information regarding e-crime as well as find ways to fight e-crime, definitely this battle may be won. PPP will ensure harmonious relationship and working together to understand the exact nature, level and impact of e-crime on all sectors (private, government industry), by sharing, reporting and recording information, which may be the basis of how to tackle the battle against e-crime. This will also bring together organisations, businesses, public sector etc affected and infected by this phenomena and assist those not yet experiencing the effects of e-crime to prevent, hence contribute towards detection and prevention of this digital syndrome.

Public Private Partnership will also ensure information sharing as depicted by figure 2, which will guarantee that all reported cases of cyber-crime are automated by the local agency in the reporting countries and escalated to a central depository where all e-crime cases and reports will be captured, examined and attended to with the assistance of other law enforcement agencies for technical support. This centralized depository will assist all countries, of course that have become members of the Public Private Partnership to

have access to relevant information statistics and these countries will be able to draw full facts and figures in regard e-crime thus appreciate the nature, extent and impact of e-crime. This will enable members to analyze volumes of reporting, reported loss, impact of e-crime on trust of online transactions, international trends, details of cyber criminals and or organized crime and of course be adept in profiling these cyber criminals and sharing their information. This will act as a deterrence to cyber criminals.

Policy makers must include a clause that criminalize failure to include and enforce security inclusion in business decision. This will ensure action by organizations, governments and business throughout the world intertwine preventative and detection measures and weave these on the fabric of their daily operations and decision making.

D. Research and Development

Joint forums of the industry, business and of course the academia in researching on criminal behavior, monitoring and evaluation of implemented security systems, and coming up the best feasible solutions may also alleviate this international problem.

It is palpable from the success of cyber criminals that they spend sleepless nights devising means to compromise security no matter how organizations have put in place to secure their critical asserts. For the international community to triumph experts from all discipline need to form forum that convene annually to discuss real issues surrounding e-crime in order to address this issue from diverse perspectives such as the criminal, the internet, the legal, technological, system/processes, programming and business/industry.

E. Cyber Security Education based on International Framework

Internationally there is a need for education, training and awareness to all cyber citizens, to equip them with knowledge and skills of how to live safely in the world made of chips and wires, known as the cyberspace. An Internationally acclaimed training and awareness programs tailored to different levels of online users will undeniably assist in winning this battle, though this will not disarm the opponent (cyber criminals). This will assist in the prevention of e-crimes since online surfers will be well informed to make decision to surf the internet safely, also legitimate consumers will not become unwitting accomplices, in regard e-crime.

 ISSN: 2321-8169
3859 – 3865

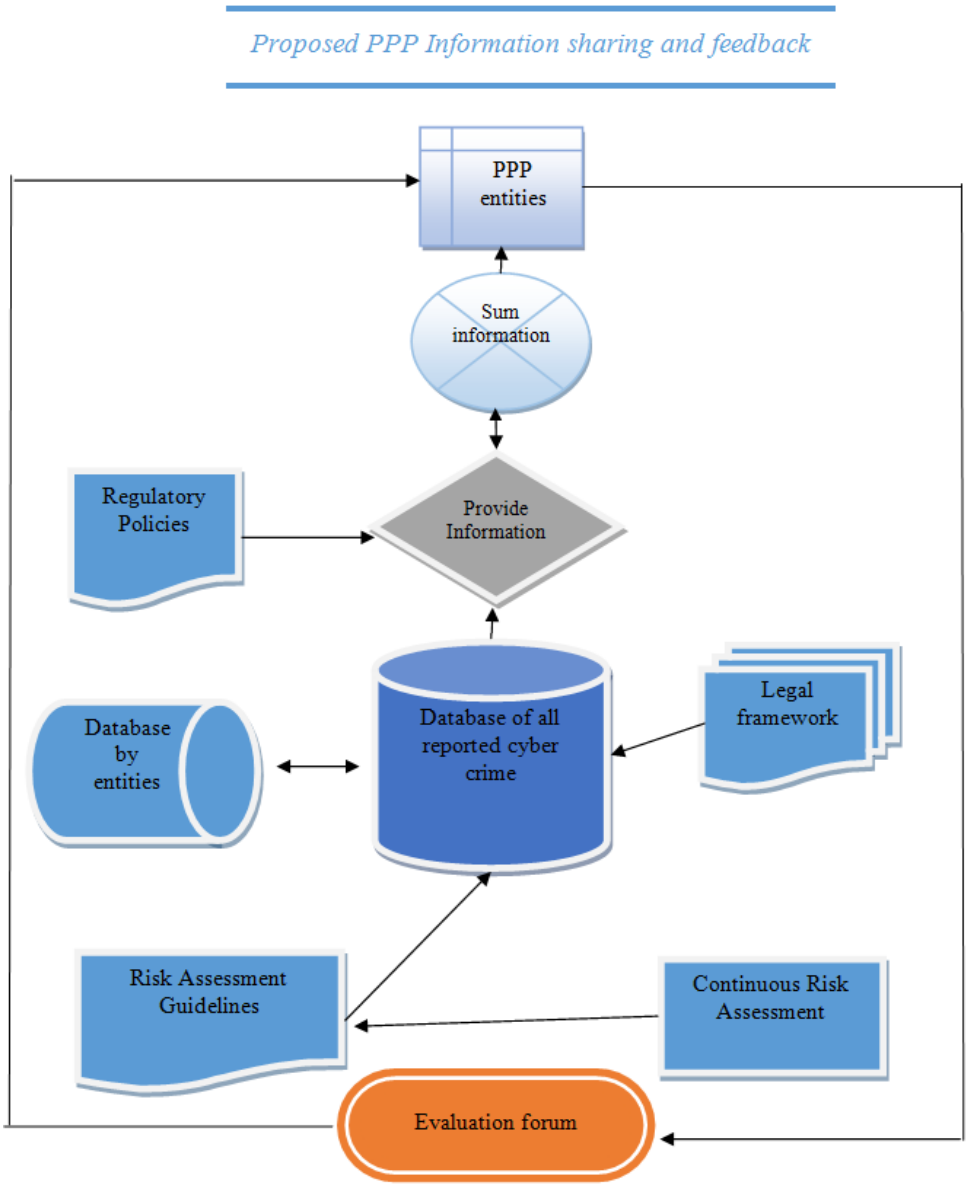

Figure 2: Proposed Information sharing in a PPP setting

VIIII. CONCLUSIONS

This study provided an insight into this omnipresent phenomena. There is a dire need to develop models, come up with new paradigms to cure this syndrome. It is evident that technology, legislation, secure infrastructure and cyber security awareness cannot afford the cyberspace security. These coupled with research and development, new models and continuous testing of the ICT infrastructure security, including the international cooperation of all stakeholders, may provide long term and sustainable cure and protection of the Cyber Space. For e-crime to be prevented and online transactions, activities, shopping, e-government and all online services to succeed, there is a need not just for large bandwidth and best connectivity but these must be coupled with regularly updated systems security, stiffer legislation, education and public awareness to support it. Consequently countries and their academia, businesses, nations, and the international community as well, need to understand this 21st century peril, and the fact that almost all crimes in this era are either aided or targeted towards technology. This calls for international cooperation of all sectors, nations, countries with the constant aims and objectives of jointly fighting this battle with a view to come up with strategies on how to fight and win the battle against e-crime.

REFERENCES

[1] Amol Vyavhare, Cyber Forensic tools http://www.articleswave.com/computerarticles/top-cyber-forensic-tools.htmllast accessedon 02/11/2009

[2] Ernest and Young (2009 E-Crime: An increasingly sophisticated menace to businesses and consumers available from http://ey.mobi/Publication/vwLUAssets/e-Crime/$FILE/EY_E-crime.pdf last accessed 23/09/2013

[3] Computer Forensics, Cybercrime and Steganography http://www.forensics.nl/links/ Accessed 02/11/2009

[4] Cyber crime losses almost doubled, available from http://www.theregister.co.uk/2010/03/15/cybercrime_complaint_surge/ last accessed on 30/02/2011

[5] Cyber Crimes and Computer related Crimes Act, of Botswana, 2007, available from http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/Botswana/CYBERCRIMES.pdf last accessed 20/03/2012

[6] Fombard CM and Quansah EK, The Botswana Legal System, LexisNexis Interpak Books, Pietermaritzburg, 2008

[7] Norton 2013 report News dated available from http:www.semantic.com/about/news/resources/press_kits/detail.jsp?pkid=Norton-2013-report last accessed 10th March 2014

[8] IOLScitech 2011, Top five cyber threats facing consumers, available from http://www.iol.coza/scitech/technology/security/top-five-cyberthreats-facing-consumers-1.1009335 last accessed on 22/04/2011

[9] Lecture on "Electrical Units of Measurement" (3 May 1883), published in Popular Lectures Vol. I, p. 73; quoted in Encyclopaedia of Occupational Health and Safety (1998) by Jeanne Mager Stellman, p. 1992 available from http://zapatopi.net/kevin/quotes/ and http://en.wikiquote.org/wiki/William_Thomson last accessed on 23/02/2011

[10] Marcella A and Doug Menendez, Cyber Forensics, A field Manual for Collecting, Examining, and Preserving Evidence of M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[11] Electronic Publication: Digital Object Identifiers (DOIs):

[12] Article in a journal:

[13] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[14] Article in a conference proceedings:

[15] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.

[16] Muller Robert, Statement to Senate Judiciary Committee, December 2, 2006, available from http://www.fbi.gov/congress/congress06/mueller200606.htm accessed on 30/03/2011

[17] Report on Progress of MP's e-strategy dated 25/01/2007, available from www.mpa.gov.uk/committees/mpa/2007/070125/10/, last accessed 05/03/2012

[18] Research Centre For Educational Technology (RCET), Ubiquitous Computing, available from http://www.rcet.org/ubicomp/what.htm, last accessed 02/02/2012

[19] Sekgwathe V. and Talib M, Cyber Forensics; Computer Security and Incident Response, available from http://www.sdiwc.net/digital-library/web-admin/upload-pdf/00000149.pdf

[20] Talib M. and Sekgwathe V., E-Crime: An analytical study and Possible Ways to combat, International Journal of Applied Information Systems, 2012

[21] Temane's over P1million case heard at the magistrate court, Botswana Daily News dated 19th February, 2002, available from http://www.dailynews.gov.bw/cgi-bin/news.cgi, last accessed 10th March 2011

[22] The World Bank Group, Financial Intelligence Units, An Overview,

[23] International Monetary Fund Publication Services, Library of Congress Cataloguing- in Publication Data, 2004

[24] EUROPOL Cybercrime presents a major challenge for law enforcement, EUROPOL, January 3, 2011

[25] InfoSec, Cyber crime Impact report 2013, available from http://resources.infosecinstitute.com/2013-impact-cybercrime/ last accessed 01/03/2014

[26] International Cyber Crime Assistance Program available from www.icspa.org last accessed 18/03/2014

[27] International Telecommunications Union, ITU Child Online protection initiative-E- crime expert available from http://www.impact-alliance.org/resourcecentre/ITU-COP-ecrime-expert.html