The International Information & Library Review (2005) **37**, 11–17

The International Information & Library Review

www.elsevier.com/locate/iilr

The evolving sophistication of Internet abuses in Africa

Ayoku A. Ojedokun

University of Botswana Library, Gaborone, Botswana, Box 70130, Gaborone, Botswana

KEYWORDS
Internet abuse;
World Wide Web abuse;
Information technology abuse;
Cyber crime;
Internet crime;
Computer crime;
Internet fraud

Summary This paper discusses the evolving sophistication of the Internet and the World Wide Web abuses in Africa. It begins by reviewing known abuses worldwide. It also reviews the various technology solutions in place to reduce the abuses. The paper notes that the various security measures and protocols identified require human intervention based on trust. It argues that human behaviors are unpredictable, and that human trust cannot always be absolutely guaranteed as they can at any point in time compromise their integrity. The paper also notes on-going efforts of some African countries at updating their country laws. The author proposes the creation and enforcement of new international laws that would compliment country laws and preserve basic civil rights in the electronic environment as a way of bringing sanity into the use of the Internet and the World Wide Web. Such laws must particularly incorporate measures that would prevent governmental abuses. The paper also suggests the formation of a separate international court with exclusive jurisdiction over the Internet.

Introduction

The term information technology (IT) comprises a rapidly expanding range of equipment, applications, services and basic technologies that process information, as well as telecommunications, and multimedia devices. These are also sometimes referred to collectively as information and communication technologies (ICTs). Today, emerging technologies such as the Internet, and the World Wide Web (WWW) are enabling faster access to useful information and services from remote locations. The Internet is a sprawling network of networks used to communicate digital information. In other words, users are no longer constrained by distance; however, one wonders whether the developers realized the potential destabilizing effects that these information technologies could have. One feature of the Internet is that it is largely unsupervised and unregulated. Thus, in spite of the many benefits, which these technologies offer, current happenings show the many abuses to which they have been used.

Computer and related criminality has become the phenomenon of the end of the twentieth century, and is expected that its further rapid

E-mail address: ojedokun@mopipi.ub.bw.

1057-2317/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.iilr.2005.01.002

development will follow in the 21st century. This is caused, according to Ministerstvo vnitra (2002), by vast expansion of computers in the global economy, quick increase of their use in households and especially by developments of computer networks, in particular, the Internet. For example, approximately 10% of the Czech population seems to use the Internet. The numbers are however higher in the highly developed countries. The Ministerstvo vnitra report states that the percentage of the population that are Internet users is estimated at 59% in the USA, 56% in Canada, 53% in Sweden, 46% in Australia, 45% in Switzerland, 33% in Japan, 33% in Great Britain, 29% in Germany, 22% in France, and 11% in Poland. A report credited to Netsizer by Case and Young (2002, p. 355) also indicated that there are more than 350 million Internet users worldwide, representing 105% increase from the estimated number of users in 1999. The estimated number of Internet users worldwide rose nearly 80%, from 171 million in March 1999 to 304 million in March 2000 (Haskins, 2000). Thus, indicating that the Internet is showing no signs of slowing in growth. Indeed, globally, according to Ministerstvo vnitra this number of the Internet users is expected to grow to 1 billion by the end of 2005.

In Africa, as of mid 2002, the number of dialup Internet subscribers was close to 1.7 million, 20% up from 2001, mainly bolstered by growth in a few of the larger countries such as Egypt, South Africa, Morocco and Nigeria. Of the total subscribers, North Africa and South Africa are responsible for about 1.2 million, leaving about 500,000 for the remaining 49 Sub-Saharan African countries (The African Internet—a status report, 2002).

This paper discusses the evolving sophistication of the Internet and the WWW abuses in Africa. It begins by reviewing known abuses worldwide, and reviews the various technology solutions in place to reduce these abuses. It then suggests ways of bringing sanity into the use of the Internet and the WWW. Abuses in this paper refer to non-accidental and non-negligent mis-use of the Internet and the WWW to engage in unwholesome and criminal activities.

Internet abuses contribute to productivity losses, unnecessary burdens on networks, data security problems, and potential risks of civil and criminal liability. They also increase Internet security costs and are, above all, detrimental to economic growth. However, the Internet does not itself cause the various abuses; rather it is simply the conduit for the abuses. The Internet serves as but one form of information source among many other sources that influence these abuses. Other IT-related influences apart from print sources include radio broadcasts, and public access cable television. But its ease, speed, and the economy of use, and the anonymity it affords are major factors that contribute to its abuses.

Internet abuses are a manifestation of human weakness as well as the level of sophistication of the environment, and usually stem from selfish motives, curiosity, envy, terrorism, and greed. Perpetrators usually include a broad range of persons: students, terrorists and members of organized crime groups. What distinguishes them is the nature of the abuse. They range from novice to experts, with information technology employees representing the largest threat.

Review of known abuses

A number of Internet abuses have already become widely known. These include: *Privacy infringement* e.g. unauthorized acquisition of data, and subsequent usage of the data for crime commission, unauthorized reading of another person's e-mail, and revealing the information obtained through the e-mail to the third party with the aim of causing damage to another person or gain property benefits, intrusion of privacy of employees by organizations—for example, surveillance is frequently imposed as a condition of employment, while some demand the right to spy on almost every detail of a worker's performance (Human Studies Center, 2004), government retention of data about people's e-mail traffic and Internet activities, government establishment of rules that do not necessarily apply to them, etc.; *dysfunctional e-behavior* e.g. sending harassing e-mail (racist and sexual), managing spam (unsolicited bulk electronic mail), posting pornographic materials on the net, gambling, etc.; and *Hacking* i.e. unauthorized penetrations into computer networks and unauthorized reading, correction or destruction of data. Hacking is becoming particularly threatening. For example, there have been cases in which hackers have infiltrated hospital computers and altered prescriptions for patients. In one such case according to Steele (1997), a hacker prescribed a potentially lethal drug to a 9-year old boy who was suffering from meningitis. The boy was saved only because a nurse caught the deviation prior to the drug being administered. According to Steele, the same hacker had also prescribed unnecessary antibiotics to a 70-year old woman, scheduled a patient to have an unnecessary X-ray, and recommended that another patient be discharged. Ironically, the hacker was also a nurse, and the motive was to directly contact

and harass the patients. In what could be considered a 'prank', Steele also reported a school boy hacking his way into a world-famous cancer research center. The boy overloaded and shut down the entire computer system by causing it to call over 50,000 long-distance telephone numbers. The 'prank' resulted in the hospital being presented with a 980-page phone bill for over $20,000 in addition to the serious problems that such a shut down inevitably caused.

Another rapidly growing form of abuse of the Internet is the use of the Internet for graphical and verbal crime such as publishing instructions on how to commit violent crime (e.g. instruction for manufacture of explosives, weapons, such as reported by the AntiDefamatory League (2001)), for committing crime against morality (e.g. child pornography) or for verbal crime (e.g. extremism, threatening, etc. such as hate groups espousing racial supremacy or separation) (Ministerstvo vnitra, 2002).

Internet abuses have also found their way into the realm of business. For example, forgery, counterfeiting, misrepresentation, repudiation, embezzlement, and theft are the common abuses now associated with Electronic Data Interchange (EDI). Fraudsters use the Internet for scams and frauds as a way to profit economically. Fraudulent e-mails (spam emails) claiming to be from reputable companies designed to entice recipients into divulging sensitive credit card information, in order to steal the recipient's identity and bank account details abounds. Some also advertise non-existent businesses with the aim of defrauding the recipients. The Internet is also making it possible to carry out quick financial operations in practically unlimited quantities in a very short period of time. The Internet has made life amazingly easy for money launderers by ensuring speed and anonymity. There is no audit trail, no face-to-face contact, and no need to go to the bank (Marshall, 2002), as they can operate entirely in the virtual world. Marshall described money laundering as an age-old practice of taking "dirty" money obtained through criminal enterprises like narcotics trafficking and organized crime, and "cleaning" it i.e. getting it into circulation without attracting the attention of bank regulators and other officials on the lookout for sudden deposits of large amounts of cash. According to Marshall, although the Internet does not make it much easier to get large sums of dirty cash online and into circulation, once criminals place the money there through other means, the Internet makes it much easier to manipulate the money. Such funds can be moved around and managed quickly and anonymously from virtually anywhere in the world. A common technique is to access the web either from a laptop or a personal computer (PC), surf to an Internet bank, open a dozen accounts and then transfer the money with the press of a keyboard button. Others use dirty money to bankroll a debit card, inserting it into a card reader linked to a PC, and programming the computer to transfer funds to a web-based business, claiming the clean money as legitimate profit.

Another dimension is the incidences of baby and/or attempted baby sales over the Internet. The UK Sky News in an article titled Surrogate mum jailed (2004), reports that a woman made 2500 pounds by selling her unborn baby over the Internet to two different couples. The deal was struck via a surrogacy website. A similar attempt was reported in Australia in an article by '*smh.com.au*' titled Magistrate dismisses Internet baby sale (2004).

Internet abuses in Africa

Many cases of Internet abuse are being reported in Africa. Cyber swindles is one such abuse. These are committed through hacking, email letters, or establishment of phony websites. Many of the cyber swindle cases have been linked to South Africa and Nigeria. For example, Makhanya (2001) reports that hackers are siphoning off millions of rands (South African currency) from KwaZulu Natal companies every year in South Africa. According to a report in IOL: South Africa (2001), one such hacker allegedly transferred money electronically from a number of international and South African financial institutions by hacking into their Internet databases. He also allegedly defrauded these institutions by creating false documentation such as financial statements and credit cards.

Similarly, in South Africa, Internet fraud has been linked to the use of the Automated Teller Machine (ATM) customer transaction slips, which has resulted in thousands of rands being stolen using the bank's Internet service. Allen (2001) reports an incidence in which a security guard stationed at an ATM machine watched as customers entered their PIN numbers, and then supplied this information as well as the customers' transaction receipts (retrieved from the wastepaper basket next to the machine) to a fraud syndicate. The ATM slips, which display the customer's account number, were then allegedly passed over to the bank employee who retrieved further details to access the customers' accounts via the bank's Internet site. In one case, 24,000 rands ($\sim$ US$2797.42) was transferred out of an account, with no one arrested. The criminals

remain faceless because of the ease of the Internet. In another instance however, a businessman had 2 million rands (~ US$258,481.00) siphoned from his account by an internet hacker. Two people were arrested and were later released on bail (Schronen, 2001).

Also on the increase, and posing new challenges are phony business opportunities. There is no doubt that Internet fraud is worldwide. For example, from January 1, 2001 to December 31, 2001, the US Internet Fraud Complaint Center (IFCC) web site received 49,711 complaints. The mission of IFCC, a partnership between the national white Collar Crime Center (NWCCC) and the Federal Bureau of Investigation (FBI), which began operation on May 8, 2000, is to address Internet fraud. Its site serves as the mechanism by which people file online tips with the FBI regarding Internet attacks. While perpetrators come from a varied international background, significant representations have also been found in Nigeria. In the Internet fraud report by IFCC, 2.7% of total perpetrators have been found to be from Nigeria, 0.5% from South Africa, and 0.3% from Togo (National White Collar Crime Center, 2002).

The most popular of the abuses however is the so-called ***Nigerian fee scam*** *letters*. The Internet Fraud Complaint Center reports that the Nigerian fraud letters made up 15.5% of complaints received mostly from individuals. Nigeria also ranked 2nd for total complaints on businesses by country (National White Collar Crime Center). Sometimes these frauds are carried out in collaboration with other nationals (e.g. South Africans and Cameroonians) (Wearden, 2002).

While electronic mail (e-mail) provides faster means of communication than snail mail, and therefore opportunity for faster and easy means of doing business, its use is daily being abused. For example, the scam letter is usually an email correspondence mostly from Nigerian nationals outlining an opportunity to receive non-existent government funds from alleged dignitaries. The scam usually mentions an ex-dictator or relative of ex-dictator who is trying to get money out of the country before going to jail. Other scams may involve a religious-based contribution, inheritance, and people purporting to want to invest in your company. The scammers then try to get the victims 100% convinced that they will get the payoff. These letters then offer the victim a percentage of millions of dollars in exchange of letting the sender use the victim's bank account to transfer the funds.

In some cases, Nigerian nationals, purporting to be officials of their government or banking institutions, will e-mail letters to individuals and businesses in other countries informing the recipient that a reputable foreign company or individual is needed for the deposit of an overpayment on a procurement contract. The letter will claim that the Nigerian government overpaid certain amounts in millions on a contract and will be seeking assistance to get the money transferred. The scams have also taken the form of bogus sales contracts. An African firm or government official requesting a rather large export sale will contact the targeted individual or company. The sale will often ask for samples to be sent in advance of the sales negotiation. Such fraud as above is called 4-1-9, after the section of the Nigerian penal code that addresses fraud schemes.

Although initially linked to Nigeria, the scam is now prevalent in many other African countries, and the targets are usually gullible individuals who could be from any country. Such individuals usually see the proposed offer as a means of making fast money. Many of them are linked to countries such as Ghana, Benin, Togo, Sierra Leone, the Democratic Republic of the Congo (Michigan District Export Council, 2004) and South Africa. For example, using the Nigerian scam letters' approach, the tricksters in Zimbabwe are beginning to use the controversial land crisis in their e-mail scam letters to try and deceive innocent people in Zimbabwe, including Kenyans, into parting with their money sometimes running into thousands of shillings (Standard Correspondent, 2004). The Michigan District Export Council Website provides other examples of such letters emanating from African countries to warn users. African Scams Site (2003) also reports other variations of the African Internet-based scam letters.

Another variation of the Internet abuse is a growing number of fictitious banking web sites falsely aligning themselves with respectable offshore financial institutions. In these fraudulent web sites and unlicensed banking operations according to Oyesanya (nd), confidence tricksters pose as Nigerian politicians to solicit funds or advance fees for massive bank transfers, which subsequently never happen.

In addition, the Internet is beginning to be used as a means to incite members of the public to lawlessness. It is also being used positively as a means of campaign for revolutionary change, particularly where an oppressive regime needs to be relieved of governance. For example, Zimbabweans are being urged to "Get up! Stand up" to challenge the Robert Mugabe's government by an underground movement called "Zvakwana—which means, "enough is enough" in Shona language through their website (The Observer, 2004). The

revolutionary movement urges Zimbabweans to take courage and defy any person, state authority, organization or business that infringes their basic rights or that of their loved ones. Through the anonymity of the Internet, the group has also been able to challenge the government.

Technology-based attempts at securing the Internet from abuses

A number of technology-based security measures are currently being implemented in all countries worldwide including the countries in the African continent to reduce Internet abuses. Guenther (2003) framed web security within three different areas: web server security, security of the user's computer, and the security of information transmitted between the web server and the user. A number of Internet and/or web security measures are already in place, some of which also infringe on privacy. These include the use of utility programs such as monitoring and detection software (e.g. filters to guard against hacker attacks such as *SurfWatch, Cybersitter, Net Nanny, Cyber Patrol*, etc; firewalls to segment networks; digital signatures; secure authentication of users; the use of document encryption; and strict control of cryptographic keys or secure backup of the information being encrypted). However, the explosive growth of the Internet makes it very difficult for software programs to completely monitor and control access to Internet sites. With millions of sites on the web, it is impossible to catch them all. Typically, the software recognizes a database of banned sites and/or blocked sites and search words. But by the time a list of blocked sites is installed, thousands of new sites may have appeared. There have also been reported attacks on some of the programs (Attacks on Popular Firewall Program, 2004), which suggest that technology solutions alone are inadequate.

Attempts at securing the Internet from abuse in Africa

It is worth noting that all the security measures and protocol that have been identified or are yet to be identified require human involvement, which is usually based on trust. However, human trust cannot always be absolutely guaranteed. Human beings can be lured and/or tempted to compromise their integrity. A sacked employee may decide to take revenge on the employer. Similarly, pauperized individual may decide to take advantage of the Internet for property benefit or financial gain. These unpredictable human behaviors are the hallmark of the Internet and web abuses. Anything is possible where human beings are involved. The Internet therefore is not yet a secure medium over which to communicate information especially financial and personal information. Any technological solution without legal restrictions would be futile.

In other words, cyber criminals are becoming increasingly sophisticated. A legal framework to backup the technology solutions is therefore becoming a necessity for all countries, including those in Africa. It is obvious that law enforcement officials cannot take action against cyber criminals unless countries first enact laws, which criminalize the activities in which these offenders engage. The existence of such laws is a fundamental prerequisite for investigation as well as for prosecution. It is therefore obvious that all nations would desire to have cybercrime laws in the books. The difficulty would however lie in properly defining the laws needed to allow for cyber criminals' apprehension and prosecution.

Internet abuse is rising in Africa and there is either no law or the common laws are grossly inadequate to reduce it. For example, in Kenya, while Internet crime is said to be rising, the country has no laws to deal with the cyber-crooks. The country's laws of evidence were inadequate and did not say how perpetrators of cyber crimes could be prosecuted when arrested (Kithi, 2002). Similarly, South African laws are clearly ill equipped to deal with Internet crimes, while the current procedural aspects of the law (The Criminal Procedure Act 51 of 1977) were also not designed with the Internet in mind e.g. Computer Evidence Act 57 of 1983 as it relates to admissibility of evidence. The laws are not effective to prosecute the crimes. For example, the common law does not cater for offences involving the theft and abuse of data and programs stored and found on computers; and general provisions applicable to search and seizure of 'articles' are inadequate when it comes to evidence on a computer. (Nedbank ISS Crime Index, 1999; Makhanya, 2001; Masters, 2001).

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create an inhospitable environment. They also create barriers to economic growth of countries. However, there are efforts at putting in place laws that would reduce the abuses in many African countries, South Africa and Nigeria inclusive (Masters, 2001; Okonji, 2004). Similarly, according to McConnell International's (2000) report, of the 13 countries indicating progress toward

the adoption of updated legislation to combat cyber crime in the E-Readiness study conducted, seven are in Africa or the Middle East. Five of the seven countries were identified in the study to be in Africa. They include Gambia, Lesotho, Morocco, Sudan, and Zambia. Mauritius, according to the report, has already updated its laws with stronger penalties than many other countries for convictions of covered cyber crimes.

A Commission charged with the responsibility of investigating computer-related crime in South Africa in 1997 also released an exciting proposal, called, Discussion Paper 99, which if adopted will change the way South African law system deals with computer misuse (Masters, 2001). The penalties suggested in the proposal include imprisonment for a period not exceeding 5 years and imprisonment for a period not exceeding 10 years for different computer offences. South Africa is a member of the Council of Europe, which is trying to set a legal infrastructure standard, which all member countries could follow. This is an added advantage for South Africa in her efforts to build proper legislations.

Similarly, Nigeria has also just recently inaugurated a cybercrime working group to immediately begin tackling the abuses of the Internet and other electronic crimes that have become a source of great embarrassment to the country. Under the new act recently forwarded to the National Assembly for enactment, all crimes carried out with the use of computers, electronic and/or ancillary devices are punishable. The crimes were categorized into three yet to be named groups. Although the list is quite exhaustive, it is unclear how the groupings were arrived at. The first group includes unauthorized access to computer systems, access exceeding authorization, computer and system interference, data interception, denial of service, computer trespass and "e-mail bombing". The second category of crimes includes computer contamination, illegal communications, computer vandalism, cyber squatting, cyber terrorism, cyber pornography and intellectual theft. The third group includes the use of computers to corrupt a minor, soliciting to compel prostitution, sending obscene materials to minors over the Internet, indecent exposure and tampering with computer evidence (Onuorah, 2004). The report of a committee headed by its National Security Adviser, set up to study the implications of the rising spate of cyber crime in 2003 gave birth to the inauguration of the working group (African Online Correspondents, 2003; Okonji, 2004). It is however not yet known when the law would be enacted, and what the punishments would be.

The way forward

In spite of the efforts being made by individual countries to combat cyber crimes, bringing reason into the use of the Internet and the WWW requires the creation and enforcement of international laws, complimented with individual country laws, which preserve basic civil rights in the electronic environment. However, international cybercrimes may be impossible to prosecute, if countries do not update their laws to deal with computer-related offenses. The world is becoming a global village, it is therefore appropriate that international laws exist that keep pace with the advances in information technology developments and applications, while addressing all areas of potential abuses.

Such laws must also incorporate measures that would prevent governmental abuses. Government agencies (either at the state or federal level) wishing to obtain information about any individual must be made to seek the consent of such individual or the permission of the court of law (where such individual is uncooperative). This would go a long way in reducing the rate at which the abuses are perpetrated in the society. This will however, require the setting up of a separate international court with exclusive jurisdiction over the Internet. The recently concluded 3-day 2004 international conference on Cybercourts, Cyberlaw and the Cyberworld put together by the American Bar Association and Nigeria's Federal Judiciary's International Relations Committee held in the US (Igbanoi, 2004; Gbadamosi, 2004) is therefore a step in the right direction. The purpose of the conference was to give boost to the development of law and practice in the area of technology, particularly the Internet. The sessions expected to feature e-filing, e-discovery, e-evidence, e-trial, etc. was to demonstrate how technology assists the Law and Practice (Igbanoi, 2004). It was attended by high-level officials, legal practitioners and law firms from the US and Nigeria (APC Africa ICT Policy Monitor, (2004).

Conclusion

The Internet will continue to be abused as long as humans remain innovative. Technology solutions will continue to be implemented while criminally minded users will continue to find ways of bypassing them. The only long lasting solution is the creation and enforcement of international laws, coupled with complimentary country laws, and an international court with exclusive jurisdiction over the Internet to

reduce the rate of Internet abuses. This implies that country laws would have to be updated to deal with computer-related offenses for effectiveness.

References

African Online Correspondents. (2003). Nigeria to tackle Internet fraud crimes: Nigeria government to crack down on Internet 419 scammers. Retrieved June 29, 2004 from http://www.africaonline.com/site/Articles/1%2C3%2C54624.jsp, November 28.

African Scams. (2003). African Scams. Retrieved June 29, 2004, from http://www.africanscams.com/

Allen, M. (2001). Internet banking fraud goes online in Durban. Retrieved June 21, 2004 from http://www.iol.co.za/index.php?set_id=1&click_id=31&art_id=ct20010330092530682I53653961, March 30.

Anti-Defamatory League. (2001). The consequences of right-wing extremism on the Internet: inspiring crimes and guiding criminals. Retrieved May 10, 2004 from http://www.adl.org/internet/extremism_rw/inspiring_intro.asp

APC Africa ICT Policy Monitor (2004). Nigerian government to fine tune cyber crime bill. Retrieved January 6, 2005 from http://africa.rights.apc.org/index.shtml?apc=21861n21833e_1&x=21309. June 22.

Attacks On Popular Firewall Program. (2004). PC World, 22 (6), p55, 1/6p. Retrieved 13 May, from Academic Search Premier Database, June.

Case, C. J., & Young, K. S. (2002). Employee Internet management: current business practices and outcomes. *CyberPsychology and Behaviour*, *5*(4), 355–361.

Gbadamosi, G. (2004). Government to fine—tune cybercrime bill, says Olujimi. The Guardian. Retrieved May 13, from http://www.ngrguardiannews.com/news/article05

Guenther, K. (2003). Protecting your web site, protecting your users. Online, 63—66, Retrieved May 12, 2004, from Academic Search Premier Database.

Haskins, W. (2000). Super economy. PC magazines, Retrieved January 6, 2005, from http://www.pcmag.com/article2/0,4149,1119,00.asp. January 8.

Human Studies Center. (2004). Abuses—IT: assessment behaviour conflict development report. Retrieved May 3, from http://www.londonconsult.com/InfoKnow/itabuse.htm

Igbanoi, J. (2004). Cybercourts: an idea whose time has come. THISDAYonline. Retrieved January 6, 2005 from http://www.thisdayonline.com/archive/2004/04/13/20040413law06.html, November 16.

IOL: South Africa (2001). SA's first cybercrime kingpin arrested. Retrieved June 21, 2004 from http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=ct20010402205507505C1616408, April 2.

Kithi, N. (2002). Why cybercrooks have a field day. Retrieved June 23, 2004 from http://www.nationaudio.com/News/DailyNation/28082002/Business/Business67.html, August 28.

Magistrate dismisses Internet baby sale. (2004). Retrieved 7th June 2004 from http://www.smh.com.au/articles/2003/04/25/1050777385998.html?oneclick=true, April 23.

Makhanya, P. (2001). Hackers stealing millions from KZN firms. Computer/IT, Retrieved June 21, 2004, from http://www.iol.co.za/index.php?click_id=115&art_id=ct20010514212507126C1626355, May 14.

Marshall, C. (2002). Cyber laundering. ON Magazine, 7 (1), p44, 4p. Retrieved May 6, 2004, from Academic Search Premier Database.

Masters, M. (2001). South Africa—Computer Misuse Act, proposed. Retrieved 25, 2004, from http://www.sans.org/rr/whitepapers/legal/668.php, June 14.

McConnell International. (2000). Cyber crime…and punishment? Archaic laws threaten global information. A report prepared by McConnell International, Retrieved June 26, 2004, from http://www.mcconnellinternational.com/services/cybercrime.htm

Michigan District Export Council. (2004). Internet fraud. Retrieved June 29, 2004 from http://www.exportmichigan.com/internet_fraud.htm

Ministerstvo vnitra. (2002). Analysis of the current state and development trends in the area of information technology and the Internet. Retrieved May 4, 2004 from http://www.mvcr.cz/odbor/bezp_pol/english/dokument/anal_eng.html

National White Collar Crime Center. (2002). IFCC 2001 Internet fraud report: January 1–December 31, 2001.Retrieved June 28, 2004, from http://www.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf

Nedbank ISS Crime Index. (1999). Computer crime: challenges of new technology, 3 (4), Retrieved June 25, 2004, from http://www.iss.co.za/Pubs/CrimeIndex/99Vol3No4/Computer.html

Okonji, E. (2004). Mixed reactions trail cyber crime control. Daily Independent Online, Retrieved June 8, 2004, from http://odili.net/news/source/2004/mar/30/324.html, March 30.

Onuorah, M. (2004). Obasanjo raises group to tackle cyber crimes. Retrieved June 9, 2004, from http://odili.net/news/source/2004/mar/11/33.html, March 11.

Oyesanya, F. (nd.), Nigerian Internet 419 on the loose. Retrieved June 9, 2004, from http://dawodu.com/oyesanya1.htm

Schronen, J. (2001). Cyberthieves whip R2m from bank account. IOL. Retrieved January 05, 2005 from http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=ct20010312094011314B525890, March 12.

Standard Correspondent. (2004). Internet fraudsters reap from Zimbabwe land crisis. Retrieved June 10, from http://www.eastandard,net/headlines/news10060407.htm, June 10.

Steele, H. L. (1997). The prevention of non-consensual access to "confidential" health-care information in cyberspace. Computer Law Review and Technology Journal, Spring, [Electronic version], Retrieved June 29, 2004, from http://www.smu.edu/csr/Steele.pdf

Surrogate mum jailed. (2004). Sky News. Retrieved June 7, 2004 from http://www.sky.com/skynews/article/0,30100-13101361,00.html, May 21.

The African Internet—a status report. (2002). Retrieved May 13, 2004, from http://www3.sn.apc.org/africa/afstat.htm

The Observer (2004). Mugabe is spooked by the letter Z. Mmegi, June 25, 2004.

Wearden, G. (2002). Six arrested over 'Nigerian email' frauds. Retrieved June 9, 2004, from http://news.zdnet.co.uk/internet/0,39020369,2110589,00.htm, May 21.