Combating cyberspace fraud in Africa

Marthie Grobler, Joey Jansen van Vuuren

Council for Scientific and Industrial Research

Defence, Peace, Safety & Security

our future through science

Combating cyber crime in Africa is a reality

- Computer crime and cyber survey conducted in 2006:
  - Nigeria is the most Internet fraudulent country in Africa
  - Africa is ranked the third highest continent regarding cyber fraud and computer crime (Cyber Crime Africa Summit 2008)

- Africa has recently seen explosive growth in ICT, making cyber crime a reality in this part of the world
- Limited or inadequate action and controls to protect computers and networks, making Africa a target of attack as well as a medium to attack other parts of the world

our future through science

Reduction of Cyber Crime was given as one of the major objectives during the State of the Nation address by President Zuma on 3 June 2009.

"Amongst other key initiatives, we will start the process of setting up a Border Management Agency; we shall intensify our efforts against cyber crime and identity theft, and improve systems in our jails to reduce repeat offending"

State of the Nation Address by His Excellency, JG Zuma, President of the Republic of South Africa; Joint Sitting of Parliament, Cape Town

Current cyberspace threats and trends in Africa

Internet users and population statistics for Africa (Internet World Stats 2009)

Region	Africa	Rest of the world	**World total**
Population	991,002,342	5,776,802,866	**6,767,805,208**
% world population	14.6%	85.4%	**100.0%**
Internet users	65,903,900	1,602,966,508	**1,668,870,408**
Penetration	6.7%	27.7%	**24.7%**
Use growth (2000 - 2009)	1,359.9%	349.7%	**362.3%**
% users in world	3.9%	96.1%	**100.0%**

Underground economy

- Credit card fraud is on the rise in the African continent, especially in Egypt, South Africa, Kenya, Ghana and Nigeria, with losses estimated at billions of US dollars (Cyber Crime Africa Summit 2008)
- **31% of all goods and services for sale is credit card information (highest ranking)**
- Credit card information can be obtained and used for fraud: phishing schemes, monitoring merchant card authorisations, magnetic stripe skimmers, breaking into databases (Fossi *et al*. 2008)
- Easy target: South Africa has more than
  17.14 million active credit consumers
  (Davids 2009)

Cyber crime in Africa

- The intense increase in cyber crime occurrence:
  - shortcomings of both local and international legislation
  - innovative ideas that criminals have with regard to new types of cyber crime and new ways to commit these crimes

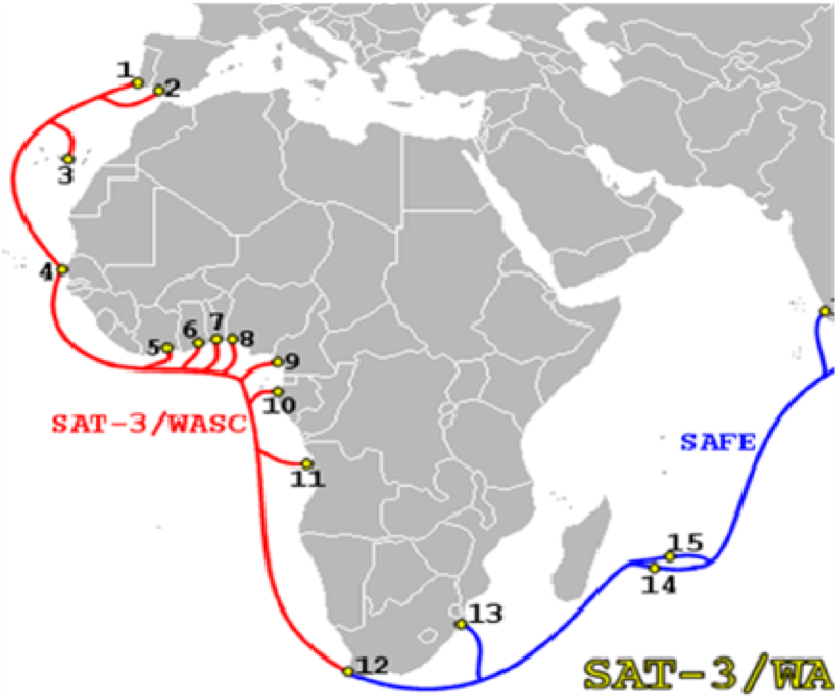
***"The government has identified at least 27 cases where a syndicate has swindled more than R199-million from government departments in four provinces over the past three years - using cyber-spyware..."* (Mail & Guardian 2008)**

Influence of broadband access on cyberspace

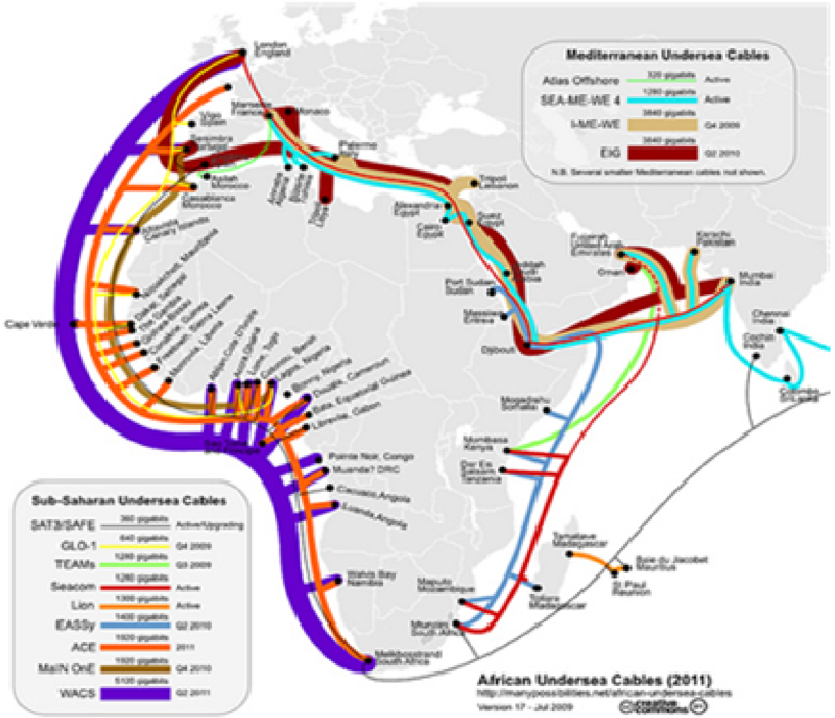
- France Telecom-Orange signed a memorandum of understanding in November 2008 concerning the installation of a submarine fibre optic cable that will provide Internet access to over 20 countries within the West African coastal region
  - The Africa Coast to Europe cable will stretch from Gabon to France, but will extend to other countries from 2011
  - This cable went live on 23 July 2009

Influence of broadband access on cyberspace

SUB SAHARAN UNDERSEA CABLES



CURRENT


Mediterranean Undersea Cables
Atlas Offshore 320 gigabits Active
SEA-ME-WE 4 1280 gigabits Active
I-ME-WE 3840 gigabits Q4 2009
EIG 3840 gigabits Q2 2010
N.B. Several smaller Mediterranean cables not shown.
Sub-Saharan Undersea Cables
SAT3/SAFE 360 gigabits Active/Upgrading
GLO-1 640 gigabits Q4 2009
TEAMs 1280 gigabits Q3 2009
Seacom 1280 gigabits Active
Lion 1300 gigabits Active
EASSy 1400 gigabits Q2 2010
ACE 1920 gigabits 2011
MaIN OnE 1920 gigabits Q4 2010
WACS 5120 gigabits Q2 2011
London England
Marseille France
Monaco
Palermo Italy
Tripoli Lebanon
Alexandria Egypt
Cairo Egypt
Suez Egypt
Jeddah Saudi Arabia
Port Sudan Sudan
Massawa Eritrea
Djibouti
Fujairah United Arab Emirates
Oman
Karachi Pakistan
Mumbai India
Chennai India
Cochin India
Colombo Sri Lanka
Mogadishu Somalia
Mombasa Kenya
Dar Es Salaam Tanzania
Toamasina Madagascar
Baie du Jacobet Mauritius
St Paul Reunion
Toliara Madagascar
Maputo Mozambique
Mtunzini South Africa
Melkbosstrand South Africa
Walvis Bay Namibia
Sangano Angola
Cacuaco Angola
Muanda DRC
Pointe Noir, Congo
Libreville, Gabon
Bata, Equatorial Guinea
Douala, Cameroon
Bonny, Nigeria
Lagos, Nigeria
Cape Verde
Casablanca Morocco
African Undersea Cables (2011)
http://manypossibilities.net/african-undersea-cables
Version 17 - Jul 2009

ANTICIPATED

Influence of broadband access on cyberspace

- The intention of this cable is to provide access to Africa
  - The SEA Cable System, referred to as Seacom, will provide African retail carriers with equal and open access to inexpensive bandwidth
  - Will remove the international infrastructure bottleneck, support African economic growth, dramatically reduce the cost of bandwidth, reduce the Round Trip Times (RTT) and increase the connection capacity to reduce current congestion
- To illustrate, in 2003 South Korea was one of the countries most severely affected by the Slammer worm. Since most of the people in South Korea had very high-speed Internet links at home, the Slammer worm was easily distributed through networks. These high-speed Internet links only became common to other countries a few years later.

Increased broadband access in Africa

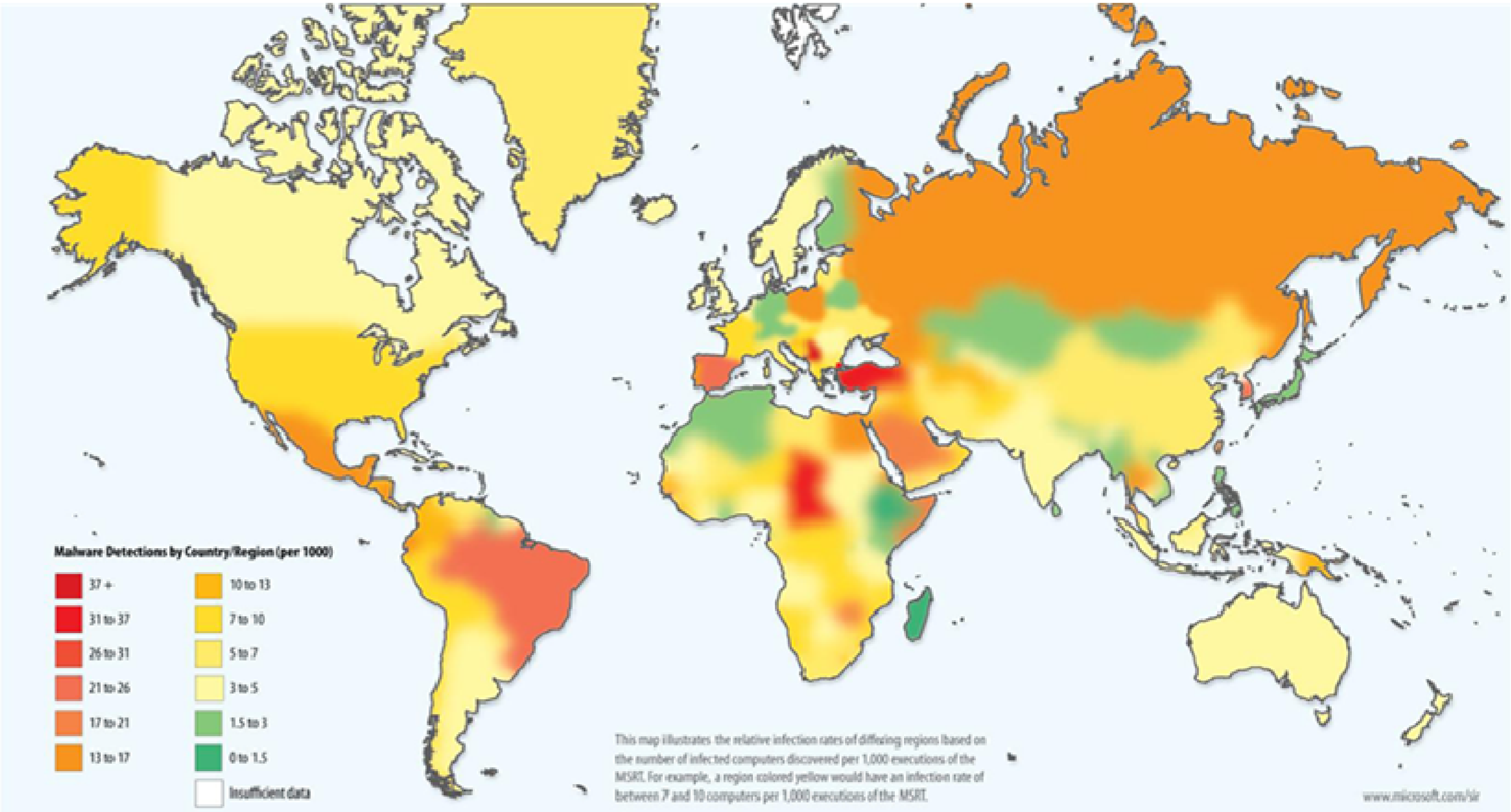
- World Wide Worx predicted that the arrival of the Seacom undersea cable will increase South Africa's maximum international bandwidth 50-fold
  - *"South Africa's Internet population is expected to grow as much in the next five years as it has in the 15 years since the Internet became commercially available in SA"*
- According to Symantec's annual Internet Security Threat Report, an increase in broadband speeds is directly proportional to a spike in cyber crime (Doyle 2009)

Influence of broadband access on cyberspace threats and trends

- The increasing broadband usage creates a favourable environment for increased cyberspace criminal activities
  - Not only are there potentially more victims, but the technology is faster, allowing more virus distributions and infections (Halbheer 2009)

"Experience seems to indicate there is indeed a link between the connectivity of a country and its subjectivity to cyber crime" (Doyle 2009)

Influence of broadband access on cyberspace threats and trends

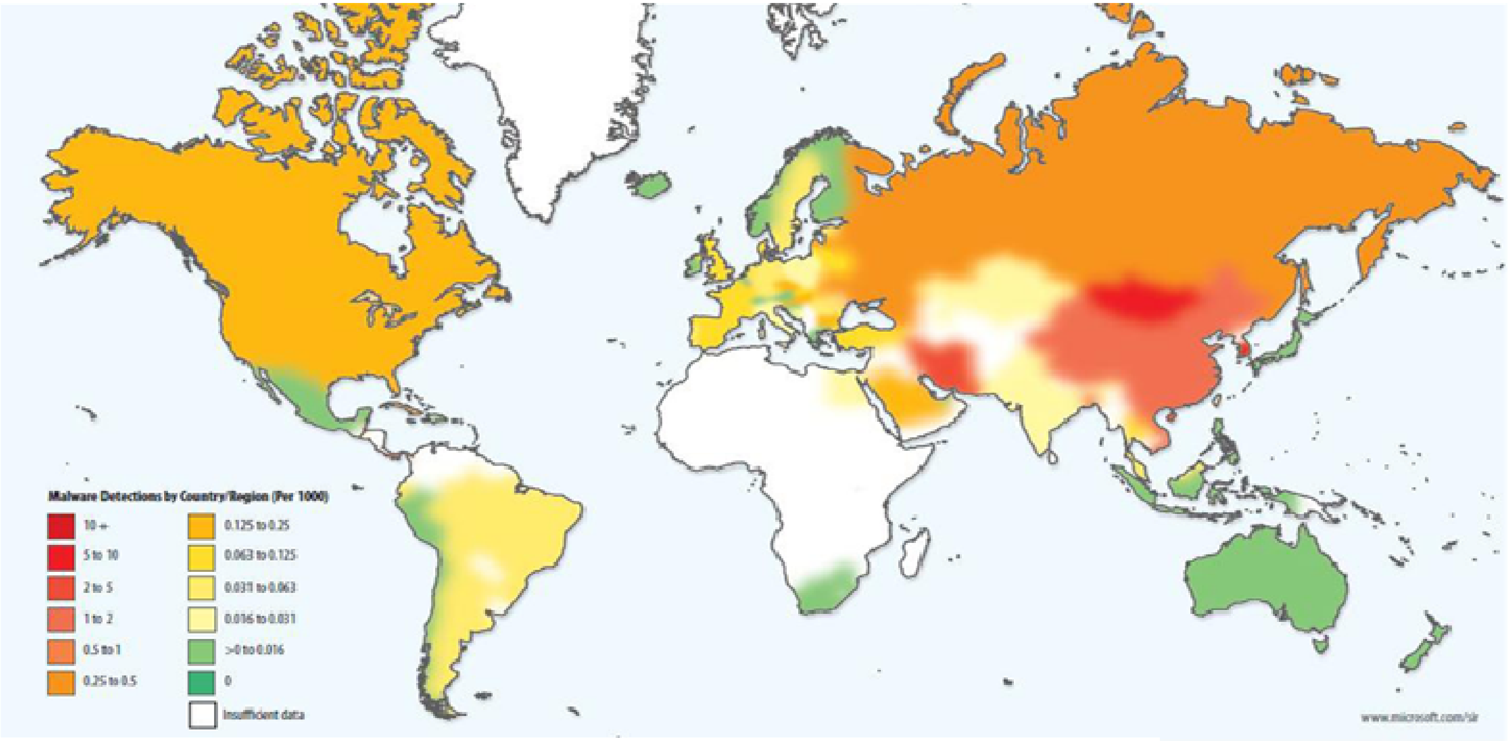


This map illustrates the relative infection rates of differing regions based on the number of infected computers discovered per 1,000 executions of the MSRT. For example, a region colored yellow would have an infection rate of between 7 and 10 computers per 1,000 executions of the MSRT.

www.microsoft.com/sir

Worldwide Infections of computers

Influence of broadband access on cyberspace threats and trends



Malware distribution sites per 1,000 Internet hosts for locations around the world in 2009

Primary cyberspace threats and trends

- The primary threats and trends to cyberspace identified are largely phenomena that are specific to Africa
- Many similar threats and trends may be visible in other countries across the world, these phenomena are applicable in the current African cyberspace environment
- Africa's specific socio-economic status has an impact on these threats and trends

our future through science

Primary cyberspace threats and trends

- Bandwidth availability
- Shortage of IT education
- Absence of African languages
- Operating system distribution
- Lack of standardised procedures

Primary cyberspace threats and trends: Bandwidth availability

- Slow download times in Africa is a reality in 2009
- A daily update of new virus definitions from Symantec is around 40MB and McAfee's is around 100MB. *"On a 56Kb dialup link, we are talking all day to download…"*
- Although frustrating, it is an inherent type of risk proofing
  - higher Internet speeds equate to more data being vulnerable to theft and other types of cyber crime
  - *"Over a slow Internet link, it might have taken days to transfer even one 1GB of stolen data, but with fibre optics, the same can happen in minutes. Generally, the faster the link, the higher the amount of threats that might come"* (Doyle 2009)

Primary cyberspace threats and trends: Bandwidth availability

- The restrictive bandwidth availability is currently being addressed by the South African government
- The Department of Communication released a draft broadband policy in September 2009, in which the objective of the policy is stated *"… to facilitate the provisioning of affordable access to Broadband infrastructure to citizens, business and government and also stimulate the usage of Broadband services at national, provincial and municipal levels"*
- The Department of Communication aims to build the South African information society, increase affordability, uptake and usage (MyBroadband 2009)

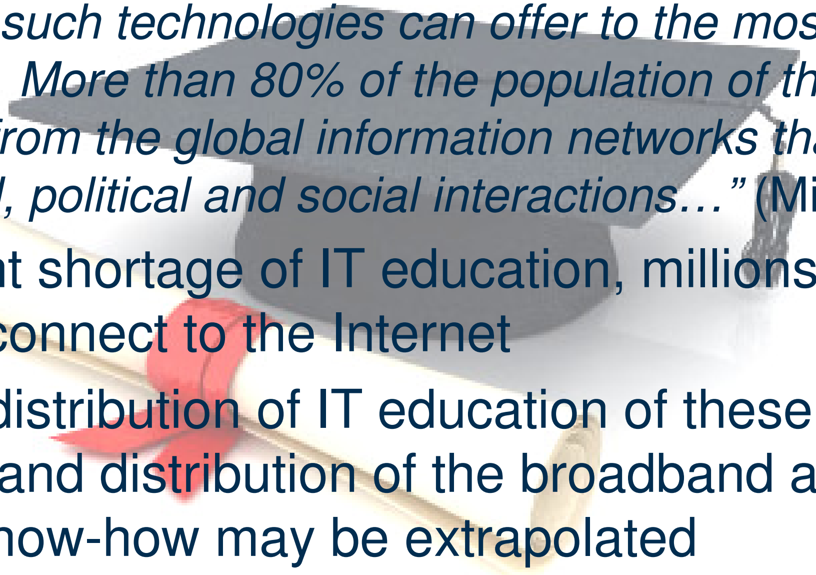
Primary cyberspace threats and trends: Shortage of IT education

- The current restrictive broadband situation indirectly impacted the availability of IT education in Africa
  - Internet connections are costly
  - logistics make it difficult to reach the rural areas of Africa
- As a result, IT education has not permeated throughout the African community, especially not to those areas with limited connectivity

Primary cyberspace threats and trends: Shortage of IT education

- Building on the digital divide, is the usability divide: technology is so complicated that many people couldn't use a computer to its full capability, even if they got one for free
  - *"… Many others can use computers, but don't achieve the modern world's full benefits because most of the available services are too difficult for them to understand. Almost 40% of the population has lower literacy skills, and yet few websites follow the guidelines for writing for low-literacy users …"* (Milicevic 2008:4)
- IT education often is theoretical in nature, with little practical experience included to further understanding

Primary cyberspace threats and trends: Shortage of IT education



- An increase in broadband access will give Internet access to more users in Africa
  - *"The existence of this digital divide impedes the possibilities of improvement that such technologies can offer to the most underprivileged… More than 80% of the population of the planet is literally excluded from the global information networks that provide economic, cultural, political and social interactions…"* (Milicevic 2008)
- Due to the persistent shortage of IT education, millions of new users will now be able to connect to the Internet
- If the increase and distribution of IT education of these users do not match the increase and distribution of the broadband access, the existent lack of IT know-how may be extrapolated
  - *"Newly-connected computers that are unprotected will be rapidly compromised and used to launch attacks on other computer systems across the globe"* (Doyle 2009)

Primary cyberspace threats and trends: Shortage of IT education

- This education should reach both computer users in the rural areas, as well as current computer users in urban areas that are currently risk proofed by slow download times
- *"Fast increasing broadband penetration such as we are seeing locally can be dangerous, as many South African companies are not security-savvy enough to be able to thwart attacks successfully"* (Doyle 2009)

our future through science

Primary cyberspace threats and trends: Absence of African languages

- The absence of African languages in cyberspace has a direct impact on the vulnerability of the African cyberspace due to a lack of cognizance
- In many instances, computer users willing to learn about cyberspace are restricted to do this, because African languages are used minimally in cyberspace

our future through science

Primary cyberspace threats and trends: Absence of African languages

- The absence of African languages in cyberspace has a direct impact on the vulnerability of the African cyberspace due to a lack of cognizance
  - *"… Though a few people have acquired computer skills, language is still a problem because the computer is dominated by English…"* (Musinguzi 2008)
- In many instances, computer users willing to learn about cyberspace are restricted to do this, because African languages are used minimally in cyberspace

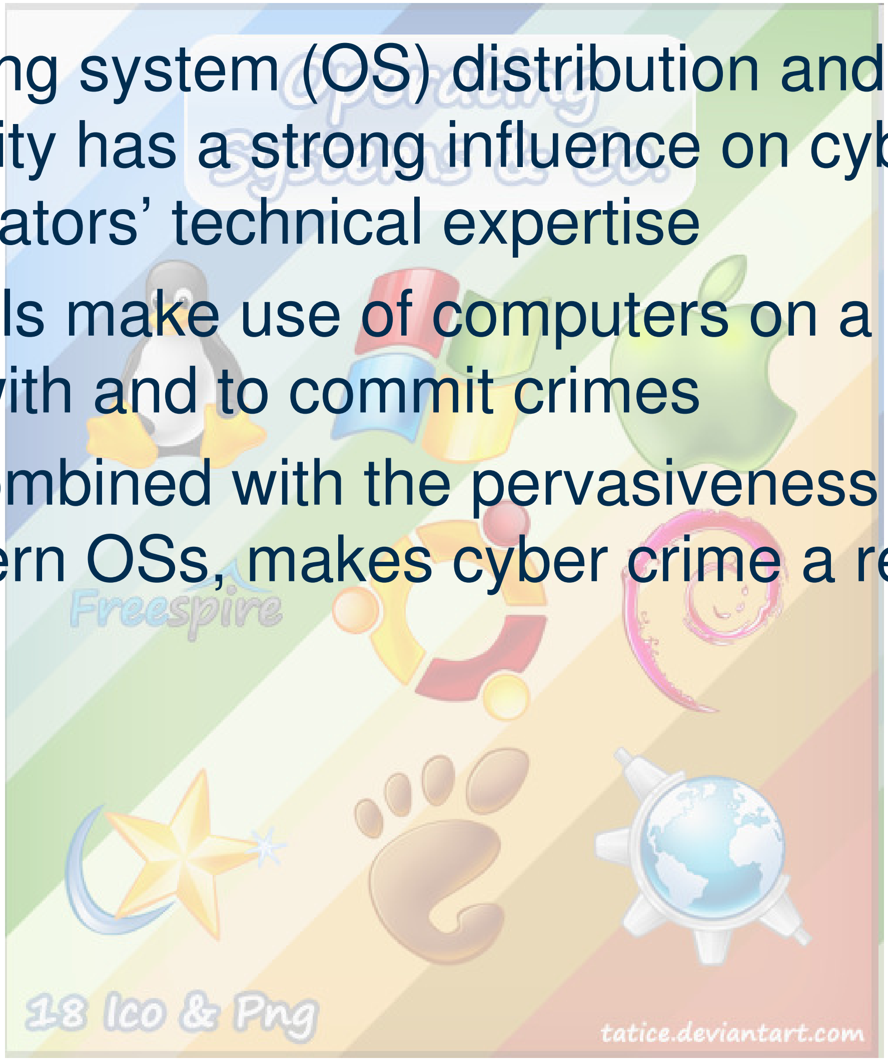
Primary cyberspace threats and trends: Absence of African languages

- An increase in broadband access will give Internet access to more users speaking an African language
- If these users are not educated in the global English language, or more Internet content published in African language, these users might be vulnerable to cyber attacks due to miscomprehension

"The unfortunate reality is that innocent Web surfers can visit a compromised website and unknowingly place their personal and financial information at risk" **(Symantec 2009)**

our future through science

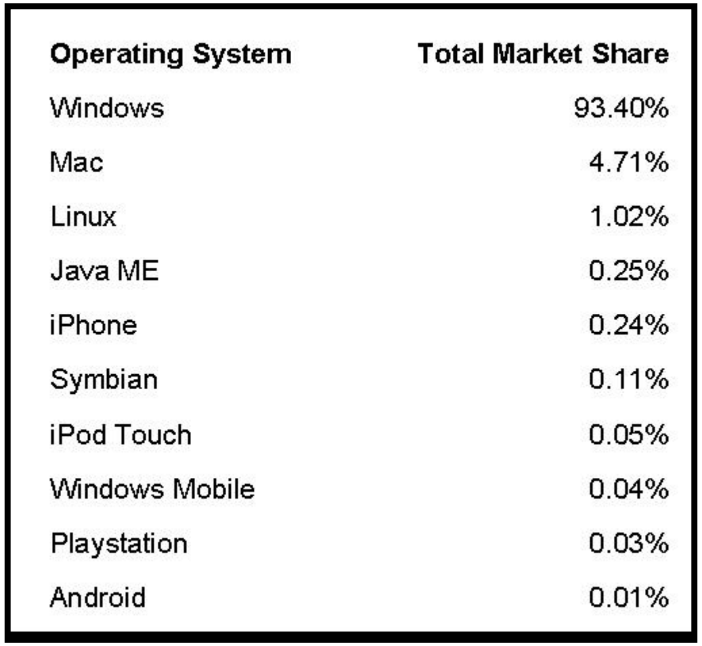
Primary cyberspace threats and trends: Operating system distribution



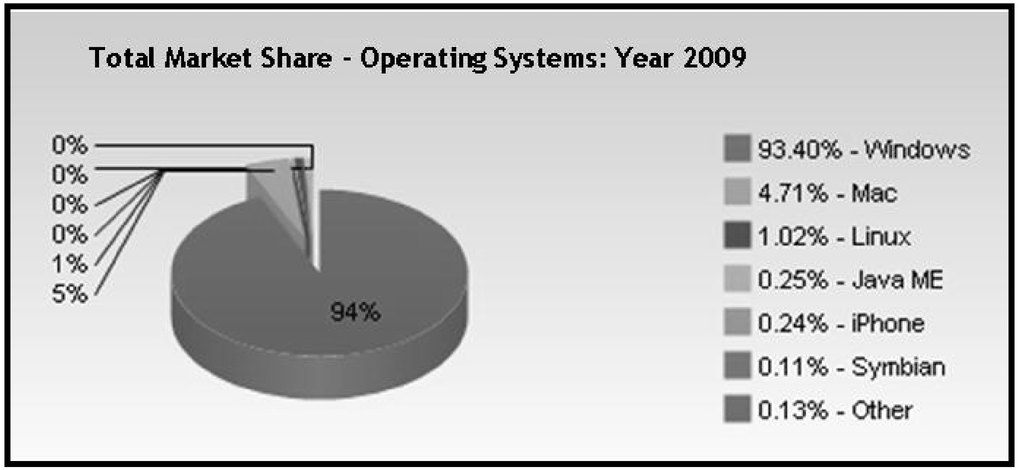
- Operating system (OS) distribution and industry popularity has a strong influence on cyber crime investigators' technical expertise
- Criminals make use of computers on a daily basis to assist with and to commit crimes
- This, combined with the pervasiveness and complexity of modern OSs, makes cyber crime a real and active threat

Primary cyberspace threats and trends: Operating system distribution

- Operating System distribution and industry popularity has a strong influence on investigators’ technical expertise
- Windows OS is the holder of the majority market share and accordingly computers with this OS are more pervasive in the community and more frequently the targets of computer crime, or used by cyber criminals to perform the crime



Operating System	Total Market Share
Windows	93.40%
Mac	4.71%
Linux	1.02%
Java ME	0.25%
iPhone	0.24%
Symbian	0.11%
iPod Touch	0.05%
Windows Mobile	0.04%
Playstation	0.03%
Android	0.01%



our future through science

Primary cyberspace threats and trends: Operating system distribution

- As the market share leader, Microsoft suggests the support of pirated versions of Windows 7 with patches (IntelliBriefs 2009)
  - *"There seems to be a link between the Internet speed and software piracy rate. In countries that are both poor and where Internet is cheap, people can download pirate software from the Internet, together with movies and music. These are between the most successful attack vectors for malware"* (Doyle 2009).
  - This will only be a viable solution if Microsoft commits for all Windows computers, and anti virus organisations offer free subscriptions on a project by project basis
  - Poverty has an influence on piracy or using outdated software with no available patches

Primary cyberspace threats and trends: Lack of standardised procedures

- The current lack of standardised procedures can lead to uncertainties about the effectiveness of investigation techniques
- The current practice is that courts of law look at standards, legislation and requirements to classify data as evidence that is admissible in court
- Without standardised procedures, this classification is left to the discretion of the judges and is not applied consistently throughout the world
  - very complex
  - potentially biased decision

Primary cyberspace threats and trends: Lack of standardised procedures

- A study done by WITSA and McConnell International showed that internationally, few countries made an attempt to minimise or control cyber crime (WITSA 2000)
- Very few legal systems presently take the digital world into account
  - criminal and penal laws need to be modified, edited or amended to fit the requirements of the cyber world

Primary cyberspace threats and trends: Lack of standardised procedures

- An increase in broadband access may potentially emphasise the current lack of standardised procedures
  - With more users connected to the Internet, and potentially more occurrences of cyber crime, it will be even more urgent to get consensus on how to handle cyber crime in a court of law
  - Without standardised procedures, this classification is left to the discretion of the judges and is not applied consistently throughout Africa, let alone the world
- It is necessary for law enforcement agencies and judiciary in the African continent to devise ways of curbing Internet fraud and enhancing their skills in computer security and risk management (Akinsanmi 2006)
  - This is the only way to counter the current lack of standardised procedures

Secondary cyberspace threats and trends

- The secondary threats and trends to cyberspace identified are largely phenomena that can be found across the world, irrespective of country
- Similar threats and trends may be visible in a number of other countries across the world
- The country's specific socio-economic status rarely has an impact on these threats and trends

Secondary cyberspace threats and trends

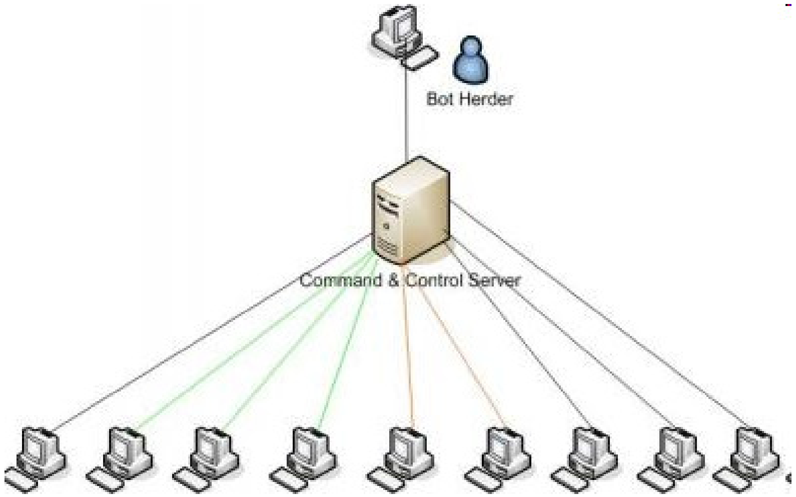
- Malicious attacks
  - Botnets
  - Crimeware
  - Pharming
  - Phishing
  - Ransomware
  - Spam
  - Spoofing
  - Spyware
  - SQL injections
  - Trojans
  - Viruses
  - Worms
  - to name a few….

Secondary cyberspace threats and trends: Malicious attacks

- Trojans generally are used during cyber attacks to control a machine, monitor local and network activity, and to download information form the infected machine
- According to Sophos (2009), 15 new bogus anti virus vendor websites are discovered every day, triple from an average of five detected per day during 2008
- In addition, approximately 6 500 new spam-related websites are discovered every day, almost double what it was in the same period in 2008

Secondary cyberspace threats and trends: Malicious attacks

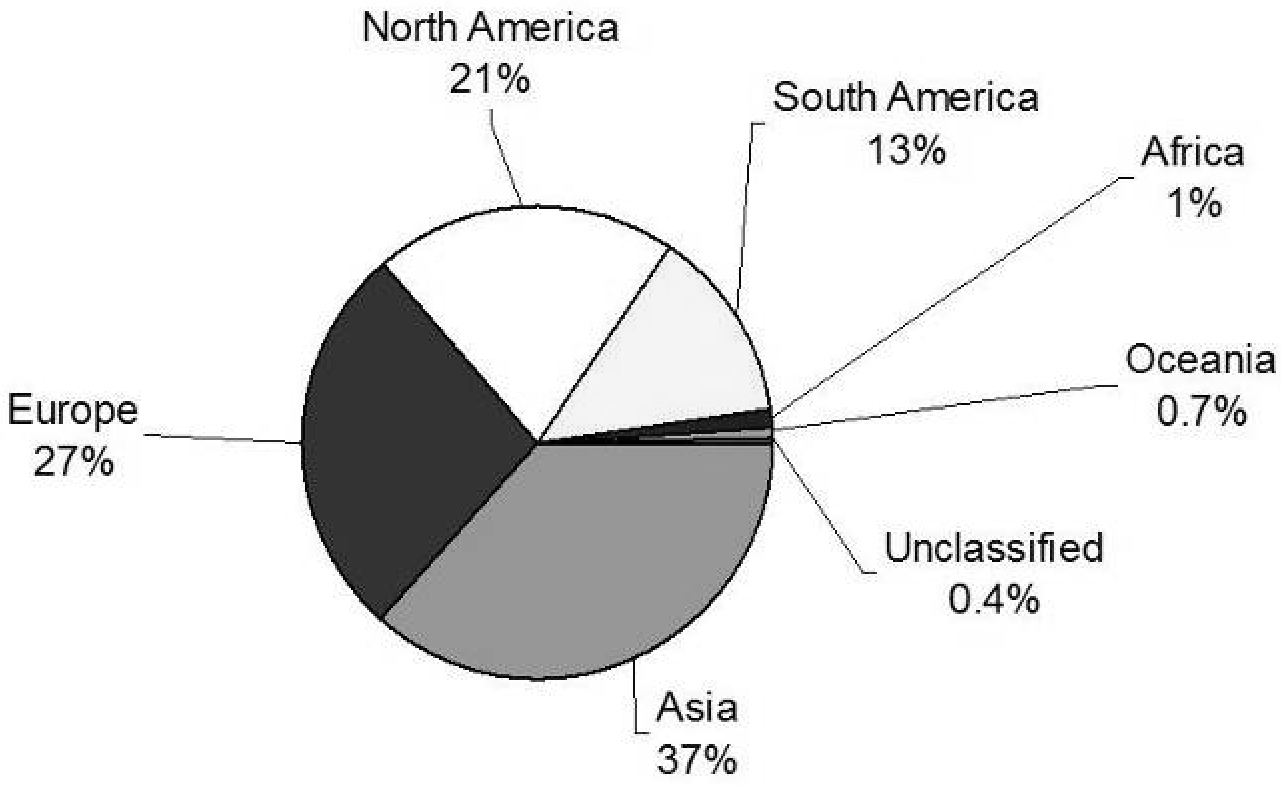
- Botnets often employ often employ other types of malware, such as Trojans, viruses and spoofing, to operate. Botnets make money in a number of ways:
  - phishing;
  - Nigerian 419 scams;
  - DDoS Attacks;
  - manipulating online polls/games;
  - sniffing traffic;
  - key logging;
  - spreading new malware;
  - Google AdSense abuse;
  - attacking IRC Chat networks;
  - mass identity theft; and
  - spamming



our future through science

Secondary cyberspace threats and trends: Malicious attacks

Spam relayed by continent in 2008 (Sophos 2008)



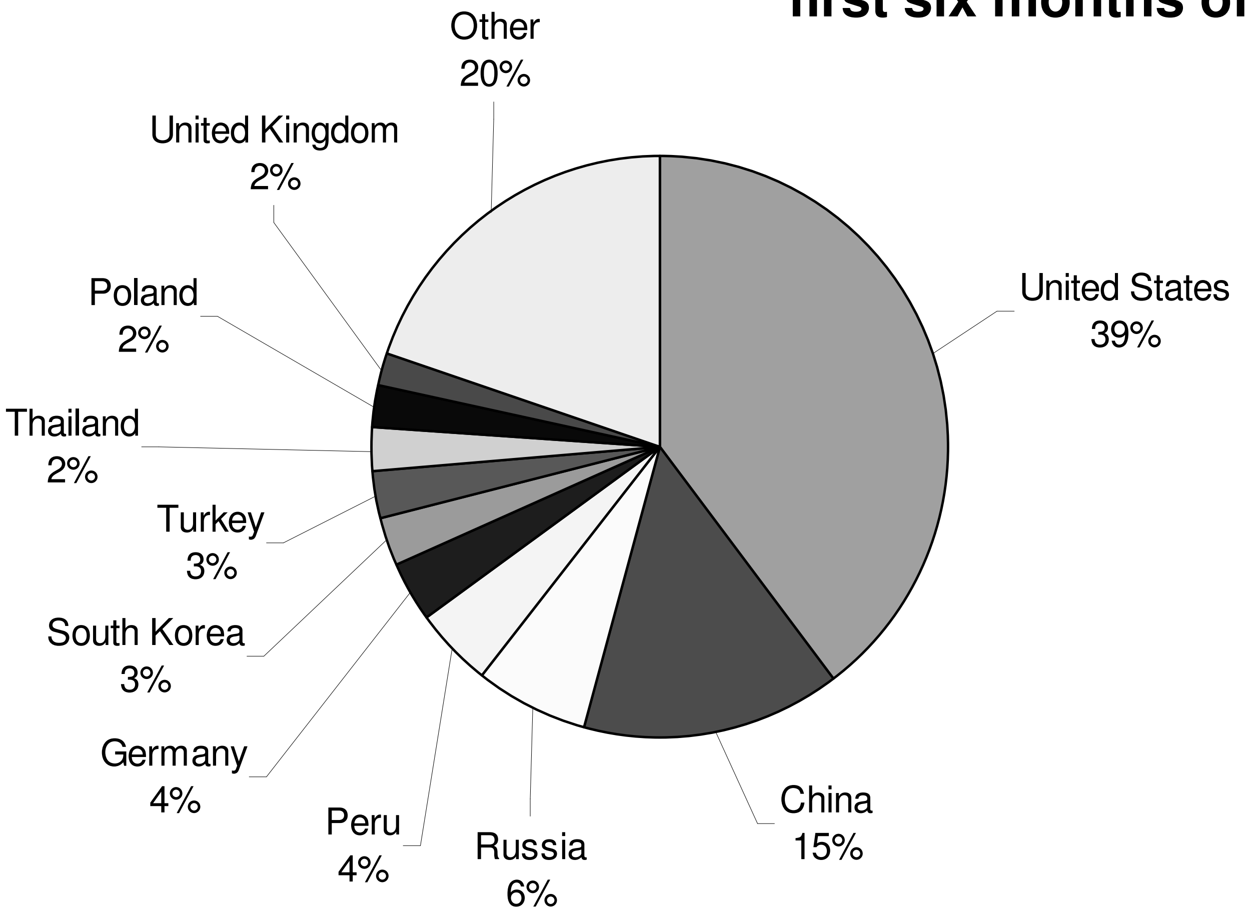
Africa contributes to 1% of the total amount of spam. This percentage may drastically change when broadband access becomes publicly available in 2010.

Secondary cyberspace threats and trends: Malicious attacks

- An increase in broadband access may potentially increase malicious attacks in Africa
  - Not only will more users in Africa be vulnerable to attacks, but with faster Internet access, these users' computers may be used in remote attacks and spam distribution
  - *"South Africa currently has a relatively small Internet population due to the historically high broadband prices, but this is all set to change. Millions of new people and new devices are going to be connecting to the Internet as prices tumble and capacity booms, few of which will be properly prepared for the barrage of Trojans, viruses, worms and hacks."* (Doyle 2009)

Secondary cyberspace threats and trends: Malicious attacks

Top ten malware hosting countries in the first six months of 2009



Although Africa is not listed under the top ten countries, this situation might change with the planned increase in broadband access in Africa.

CSIR our future through science

Secondary cyberspace threats and trends: Malicious attacks

- Africa is home to about 100 million PCs, 80% of which are estimated to be infected with some kind of malware
- This malware infestation is partly due to the intense poverty throughout the continent directly contributing to the pervasive distribution of pirated software and the inability to pay for anti virus protection
- Although the high percentage of malware infected computers is a dire problem, the current situation is that most Internet access occurs via dialup
  - With the increased broadband access planned for 2011, these unprotected computers will become an easy target for bot herders (IntelliBriefs 2009)

"While western countries have partially learned to neutralise the threat of computer viruses, Africa has become a hive of trojans, worms and exploiters of all stripes. As PC use on the continent has spread in the past decade (in Ethiopia it has gone from 0.01% of the Ethiopian population to 0.45% through 1999-2008), viruses have hitched a ride, wreaking havoc on development efforts, government programmes and fledgling businesses"

Michael, C. 2009. Computer viruses slow African expansion.
URL: http://www.guardian.co.uk/technology/2009/aug/12/ethiopia-computer-virus Date of access: 5 October 2009.

Secondary cyberspace threats and trends: Malicious attacks

- SQL injection attacks work by finding flaws in websites that links directly to databases
  - A poorly validated input field in a web input form may allow a cyber criminal to insert (or inject) SQL instructions that may be passed directly into the back end database
  - allows them to add malicious content to the database that can be served to unsuspecting users of the compromised site at a later stage (Symantec 2009)
- SQL injections are only one technique that cyber criminals can employ to commit cyber fraud

Combating cyberspace fraud in Africa

- Throughout Africa, a lack of understanding, education, training, unclear policies of government, insufficient Information Security and low confidence exhibited in Africa’s e-business poses potential problems for cyberspace safety and security (Akinsanmi 2006)

- With this rising number of cyber crimes, it is imperative to take specific counter measures to address crimes in cyberspace

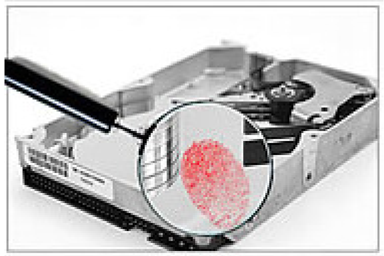
Combating cyberspace fraud in Africa

- Cyberspace initiatives
- Digital forensics
- Computer Security Incident Response Team (CSIRT)

Cyberspace initiatives

- *International Telecommunication Union High Level Expert Group* aims to develop strategies and guidance to countries in dealing with cyber crime (http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html)
- *Computers for Africa (CFA)* promotes sustainable information and communications technology development in rural African communities (http://www.computers4africa.org/)
- *One Laptop per Child* tries to create educational opportunities for the world's poorest children by providing each child with a connected laptop (http://laptop.org/en/)
- *African Information Security Association (AISA)* promotes knowledge and create awareness about computer security and cyber crime on the continent (http://www.jidaw.com/security/aisa/aisa.html)

Digital forensics



- Digital forensics is a practical way to address cyber fraud
  - not effective as pro-active technique in preventing online fraud
- As a result, digital forensics needs to evolve to address specific cyber crime developments:
  - *Dead forensics* involves pulling the plug on a suspect machine or shutting down through normal administrative procedures - focus on static data but cannot address encryption
  - *Live forensics* is done on an actively running machine - focus on the retention of volatile data and the expanded use of encryption, but may modify data
  - *Network forensics* involves analysis of actively processing and transmitting digital sources - may have a negative impact on bandwidth availability

Digital forensics

- Live forensics can acquire a wealth of information that may not be acquired with traditional dead forensic techniques
- Current African bandwidth restrictions currently limit/slow down a live forensic acquisition process
  - large remote acquisitions may have to be done after hours to accommodate the current small South African bandwidth
- The planned increase in broadband access may aid the fight against cyber crime
  - enable digital forensic investigators to actively investigate cyber crimes, with no bandwidth limitations

CSIRT

- A team of dedicated Information Security specialists that prepares for and responds to Information Security incidents
- Well established practice among network security specialists and dates back to the 1980's
- South Africa is unfortunately lagging behind the rest of the world in this regard with no national CSIRT
- **In the whole of Africa only Tunisia, Egypt, Kenya and Madagascar have a national CSIRT**

CSIRT

- Developing countries that don't have proper skills and organisations relating to incident response, are vulnerable and a big risk for other countries as well
  - These kinds of countries are an easy target for criminal activities in the form of botnets for example
  - Therefore establishing a national CSIRT capability throughout Africa will have promising crime combating effects

CSIRT

Reactive services	Proactive services
Alerts and warnings	Announcements
Incident handling	Technology watch
Incident analysis	Security audits or assessments
Incident response on site	Configuration and maintenance of security tools, applications and infrastructures
Incident response support	
Incident response coordination	Development of security tools
Vulnerability handling	Intrusion detection services
Vulnerability analysis	Security-related information dissemination
Vulnerability response	
Vulnerability response coordination	**CSIRT service categories to prevent cyber crime**
Artefact handling	
Artefact analysis	
Artefact response	
Artefact response coordination	

"Technology is changing and replacing itself faster and faster, population growth is taxing economic systems and the environment and constant social restructuring drives the complexity of our world"

CSIR

our future through science

References

AKINSANMI, G. 2006. *Fight against cybercrime, legislation as rescue* [online]. URL: http://www.cipaco.org/spip.php?article716 (Accessed 18 November 2009).

CHIZOBA, O.M. 2005. *Cyber crime* [online]. URL: www.takingitglobal.org/action/projects/download.html/4926/CYBER%20CRIME%20ABUJA.doc (Accessed 4 April 2008).

CYBER CRIME AFRICA SUMMIT. 2008. *Successful strategies to combat, prevent and Investigate Cyber crime in Africa* [online]. URL: http://www.oppiweb.com/suid-afrika/index.php?topic=354.0;prev_next=next (Accessed 18 November 2009).

DOYLE, K. 2009. Could SA lead cyber crime rankings? *ITWeb* [online]. URL: http://www.itweb.co.za/index.php?option=com_content&view=article&id=27948:could-sa-lead-cyber-crime-rankings (Accessed 17 November 2009).

FOSSI, M., JOHNSON, E., TURNER, D., MACK, T., BLACKBIRD, J., MCKINNEY, D., LOW, M.K., ADAMS, T., LAUCHT, M.P. & GOUGH, J. 2008. *Symantec report on the underground economy*. Symantec, 2008.

HALBHEER, R. 2009. *The Africa cable – a chance for Africa! – A threat for the internet?* InformationSecurity.com [online]. URL: http://www.infosecurity-us.com/blog/2009/10/7/the-africa-cable--a-chance-for-africa--a-threat-for-the-internet/28.aspx%20- (Accessed 3 October 2009).

INTELLIBRIEFS. 2009. *Africa – home of the world's largest cyber pandemic* [online]. URL: http://intellibriefs.blogspot.com/2009/10/africa-home-of-worlds-largest-cyber.html (Accessed 8 October 2009).

INTERNET WORLD STATS. 2009. *Internet Usage Statistics for Africa (Africa Internet Usage and Population Stats)* [online]. URL: http://www.internetworldstats.com/stats1.htm (Accessed 19 October 2009).

MAIL & GUARDIAN. 2008. *Cybercrime syndicate swindles govt out of R199m* [online]. URL: http://www.mg.co.za/article/2008-06-10-cybercrime-syndicate-swindles-govt-out-of-r199m (Accessed 18 November 2009).

MARKET SHARE. 2009. *Operating system market share* [online]. URL: http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8&qptimeframe= Y&qpsp=2009&qpmr=100&qpdt=1&qpct=3 (Accessed 14 August 2009).

MICHAEL, C. 2009. *Computer viruses slow African expansion*. guardian.co.uk [online]. URL: http://www.guardian.co.uk/technology/2009/aug/12/ethiopia-computer-virus (5 October 2009).

MILICEVIC, M. 2008. *Cyberspace and globalization* [online]. URL: http://www.ais.up.ac.za/ digi/docs/milicevic_paper.pdf (Accessed 19 October 2009).

MUSINGUZI, B. 2008. *African languages absent in cyberspace.* AllAfrica.com – The Monitor [online]. URL: http://allafrica.com/stories/200804081119.html (Accessed 12 October 2009).

MYBROADBAND. 2009. *Affordable broadband for all* [online]. URL: http://mybroadband.co.za/news/Broadband/9809.html (Accessed 18 November 2009).

SOFAER, A.D. & SEYMOUR, E.G. 2001. *The transnational dimension of cyber crime and terrorism.* Stanford, California: Hoover Institution Press.

SYMANTEC. 2009. *White paper: Web based attacks* [online]. URL: http://eval.symantec.com/ mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf (Accessed 18 November 2009).

WITSA. 2000. *Cyber crime … and punishment? Archaic Laws Threaten Global Information* [online]. URL: http://www.mcconnellinternational.com/index.php?option=com_content&view= article& id=10&Itemid=6 (Accessed 24 August 2009) p4.