Public Policy Meeting, Legal Issues on Cyber Security in Africa

Dakar, Senegal

21-27 November 2009

Presenter

Adam Mambi, (Advocate of High Court)

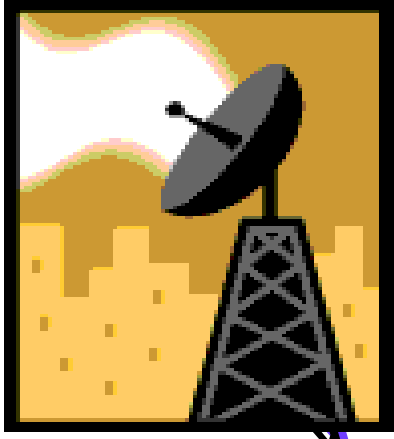
-Deputy Executive Secretary, Law Reform Commission Tanzania

-Expert & Lecturer on ICT/Cyber Law & Intellectual Property Law

AfriNIC

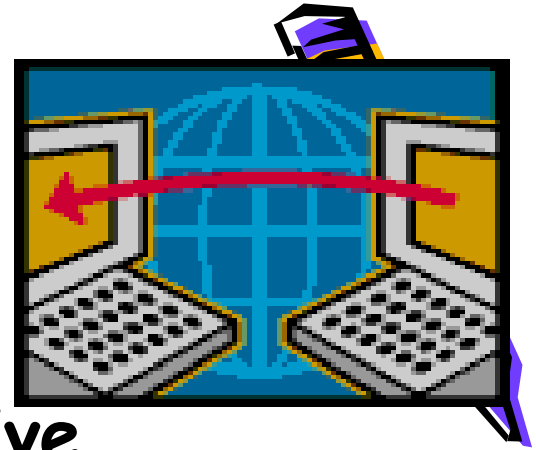
he Internet Numbers Registry for Africa

What is cyber Security?

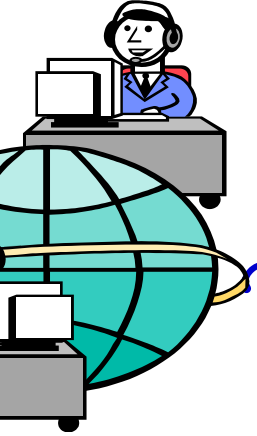


- How to create a secure environment cyberspace
- the prevention of <u>unauthorized access & misuse of computer systems</u>
- Building confidence on the use of ICT
- Cyber security is becoming a critical and major concern for governments due to the danger that such threats poses
- protection require more effort and active global cooperation from all stakeholders

ICT vis-à-vis CyberSecurity

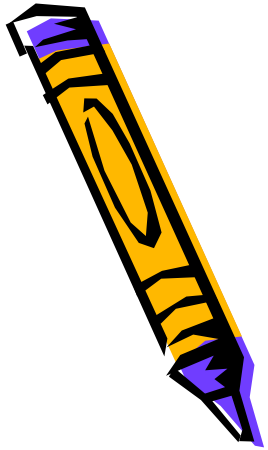


- ICT has changed the way we live, behave, interact and communicate.
- Some use ICT benefits to the detriment and harm of others.
  - ***Technology facilitates*** the commission of existing crimes such as fraud and theft
  - ***creates*** new illegal activities such as ***computer hacking, creating viruses, spams*** and other computer misuse
  - Banks/financial institutions most targeted



Hacking

What Threat the hackers can pose?

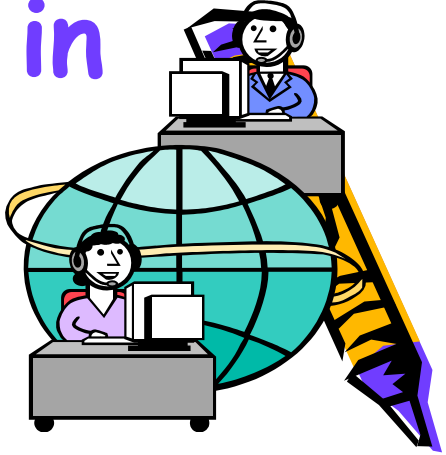


- Hacking – an e-offence-an unauthorized access
- Hackers can steal money
- Read, modify or copy or deleta information/files
- download programs or data, or add something,
- direct the computer to have goods sent to them .
- Employees-innocent hackers
- **Theft of Identify** is another great cyber threat

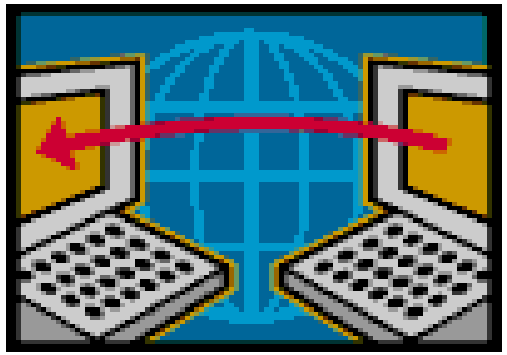
Why cyber Security?

- **Cyber Security,- <u>improve the e-security, confidence and privacy of individuals, enterprises, Governments and the entire cyber space</u>**
- enable and encourage e-commerce (e-business)
- Protect children online
- **building a secure and global information society**
- *How many of us feel very safe or secure when we are online every day?*

Issues to be addressed in cyber security& privacy



- Cyber crimes
- e-Privacy & Data protection
- Content regulation
- Children protection
- cyber-stalking
- e-identification
- Consumer protection
- Converged technologies
- Enforcement mechanisms
- e-Jurisdiction problem



AfriNIC
The Internet Numbers Registry for Africa

Privacy, Surveillance Data Protection

- The processing of Data which gives **rise to critical issues on privacy, e-security, misuse of information & individual data**
- Personal data such as **credit cards, debit cards** etc may be routed via countries with lack of data protection.
- Threats and concerns on the use of data processing techniques on freedoms & rights
- The threats range from risks of data security and privacy, system intrusion etc
- Governments must balance the need to protect public security with the need to protect individual rights to privacy

Legal Issues raised by cyber security on Cyber Crimes

Theft-Information/Data & theft of Identity

- Can e-information be stolen?
- What is "**theft**" under the current Laws?
- *Legal Elements of theft of "**asportation**" and **permanently depriving** someone property*
- *Can this apply to digital technology environment?*
- *What are the implication of technology on these legal provisions?*
- *How can we address these issues under the laws?*
- *Relevant Case; **US v. Girard and Lambert 138 DLR (3d) 73***
- ***How can laws and policies deal with identity theft?***

Content Regulation under cyber space & e-Children protection

- *Legal implications of ICT to Children*
- *Dangers Children Face on-line*
- *e-Child pornography*
- Exposure to inappropriate & harmful materials (**obscene, drugs & alcohol**)
- *Internet Grooming- e-abuse of children*
- File sharing abuse (P2P) and exposure to e-crimes
- *How can we make cyber-world*
- *a safe place for young people*
- *to work, learn and play ?*

Dangers Children Face on-line?

- Exposure to inappropriate & harmful materials (**obscene, drugs & alcohol**)
- Exposure to political & Civil War
- Access to Images of e-child sexual abuse (child pornography)
- Exposure to inappropriate and potentially dangerous contacts
- Cyber-seduction and cyber-sex compulsion
- Invasion of privacy and online fraud

Cyber stalking-(use of e-communications to harass victims)

- traditional behaviour of stalking/online harassment has always been common in the world
- Internet has facilitated the commission of these offences which attract cyber crimes
- email Stalking, Internet Stalking, mobile Stalking, sending unwanted, abusive, threatening or obscene e-mails.
- The most affected group has been women and children.
- In one case in US more than 5 women were stalked and harassed. Others women with their children received 600 harassing and threatening emails.

Cyber Security on Intellectual Property Rights

- Digital/online infringement of intellectual property rights (copyright & trademarks)
- Domain names cybersquating (*Marks & Spencer plc and others v One In A Million Ltd*[1998]FSR)265].
- Need for e-intellectual Prperty Rights

e-Identification problem. How to identify criminals/culprits/exploiters

- Presence of anonymity under Internet/cyberspace.
- Difficult to identify and investigation criminals/culprits
- How do we "know" who we are dealing with, when we cannot see or hear them?
- How do we protect ourselves, when we cannot see or feel our attackers, or when what they attack cannot be touched or seen? (("*In the Internet/cyberspace no body knows you are a Dog*"))

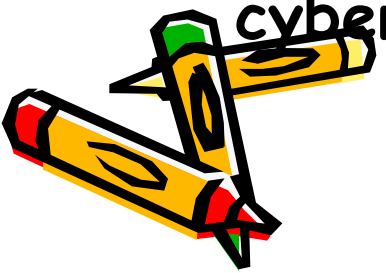
How can e-criminals escape their liability?

- The Internet can be used as communications mechanisms to make criminals escape liability and remain outside jurisdiction where they would be at risk of arrest
- Impersonation
- e-false pretence and age cheating
- Use of different legal systems
- How can enforcement agencies operate?

❖ *In one Case from the UK, cannabis dealers were able to avoid the application of the UK anti-drugs laws by selling from Dutch websites*

Conflicting International Legal Instruments?. Which supersede the other?

- How can we regulate e-content?. (Should we regulate both illegal and creative content?)
- What appropriate approaches that can we use to regulate content?
- How about Freedom of information under the Constitutions and International Legal Instruments as part of human rights?
- How to balance the Rights (freedom of expression and the right to privacy) vis-à-vis cyber security?.



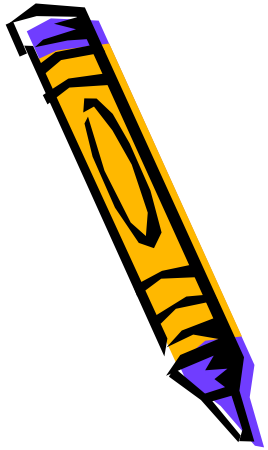
Legal implication of e-security & consumers under e-banking/cyber-payment

- E-banking raises legal issues on the question of **privacy and e-security**.
- The security risk might cause banks and other related financial institutions to loose gain and hope of e-banking
- The information based products (cards) which are personal confidential and valuable data can become a crime target or may be used as tools to commit cyber crimes.
- **Consumer *are vulnerable to* unsolicited emails (spams), phishing, spoofing)**
- Cyber-money laundering is growing

Cases on e-financial crimes

- There have been reported cases on e-financial crimes globally.
- The offence of **money laundering** has become **cyber/e-money laundering (using computers, mobiles etc)**
- In one case the accused **Thompson** was employed as a computer programmer by a bank in Country A. He managed to instruct a computer to transfer money to his account in Country B.
- On Appeal, the Court in **Country A had no jurisdiction over matters from Country B.**

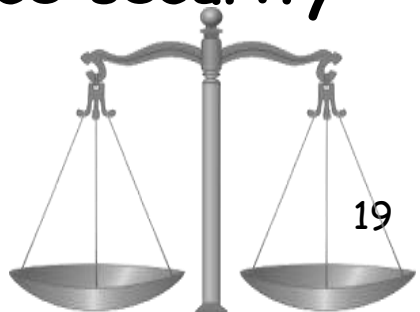
Legal Challenges; Jurisdiction Problem



- *The cyberspace has no boundaries.*
- *Criminals are always one step ahead of security agents*
- *Materials can be placed on a server anywhere and aced anywhere else*
- *Materials might be lawful somewhere but unlawful somewhere else where it is accessed*
- *Which legal system will apply*
- *Refer; Yahoo Case 2000*
- *Challenges on Converged Technologies*

What Should be done to ensure e-security?
-Legal Measures

- Develop **effective and harmonious cyber Laws at national and Regional Level**
- Create effective **International Legal Instruments on Cyber Security**
- **Adopt Models laws** that recognize both physical and cyber world (Functional equivalence)
- **Self Regulations** (trustmark schemes, Code of Conduct that reflect OECD Guidelines)
- **Use both hard and soft law to enhance security**



What Should be done

- adopt effective legal framework to combat cybercrime and other misuses of information technology.
- enforceable laws in well-defined geographical boundaries
- deterrence cybercrime requires international cooperation,
- Individual countries cant legislate over Internet content
- set up Computer Incident Response Centers or Computer Emergency Response Team (CERT)
- *Need for converged International Laws with common principles for cyber security*
- Harmonize cyber laws and policies
- Awareness/capacity building on policy and legal issues related to ICT

Other Suggested Solution;

- use of functional equivalence between paper based requirements and digital technology (UNCITRAL Model Laws & Commonwealth Model Laws).
- Consider some exiting regional and International Legal instruments;
- Enact uniform e-laws/Cyber Laws
- Bilateral Agreements/Extradition Treaties
- Prepare e-Conventions/e-Treaties at International Level under the UN

Status of Legal Measures at Regional (EAC & AU) level

- No specific Regional Legal Instruments (AU) to address cyber Security
- Most African countries are lagging behind in terms of legal measures for cyber Security
- Generally Most African Countries lack Cyber Laws
- Lack of harmonized policies and laws within African context

International Initiatives Role

- 2007-ITU launched the **Global Cybersecurity Agenda (GCA)** framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society.
- **ITU TOOLKIT FOR CYBERCRIME LEGISLATION**
  - **Focuses on harmonization of cyber crime legislation**
  - **Sample legislative language**
- Useful for developing countries better understand implications of growing cyber-threat
- **International Multilateral Partnershi**
  Cyber Threat (IMPACT)

ITU International Telecommunication Union

ITU (1) Guidelines on Children Protection online,- 2. Guidelines Policy Makers and Parents

Children and young people online should be aware of the opportunities as well as the pitfalls"

International Telecommunication Union

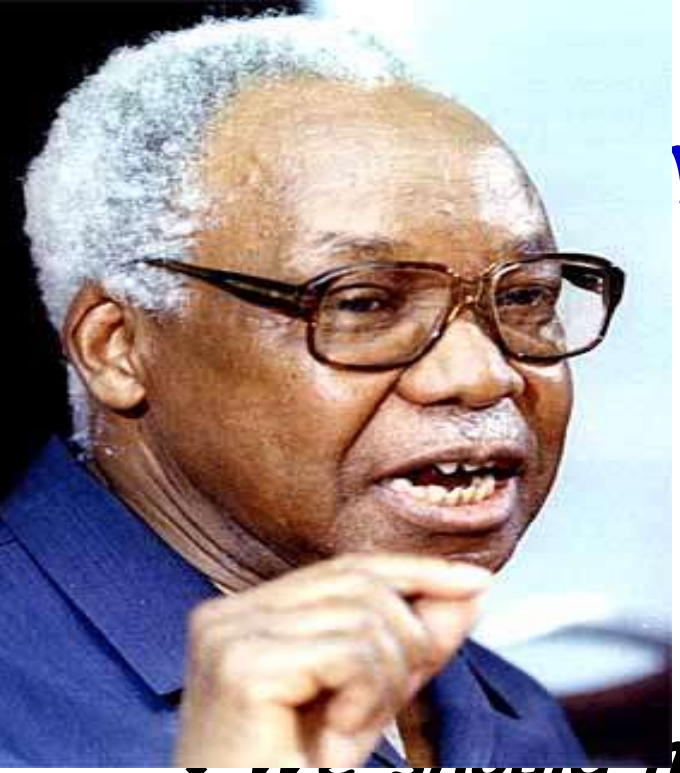
"All Children and Young People around the World have the right to a safe experience online"

EUROPEAN LEVEL

- (a) Council of Europe Convention on Cyber Crime, 2001 (open to any country in the World)
- (b) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse 2007 and other Relevant Legal Instruments (optional)
- EU Protocols on cyber security and e-comerce issues

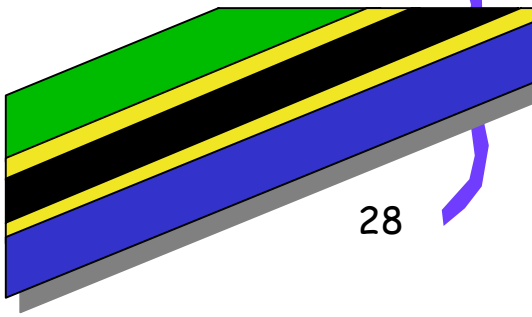
Winding up Messages

- *Be careful who you speak to.*
- *Be careful where you go.*
- *What is true offline is, unfortunately, also true on-line.*
- *we believe that children everywhere have the right to a safe environment, even w… environment is a cyber one".*



Last Message/ wise words!

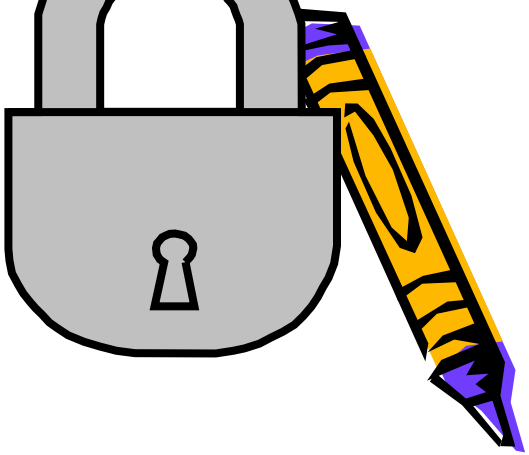
- We should not wait for others to make decisions on our behalf and then come to complain about those decisions!! (Late Mwl.J.K. Nyerere, The Former President ofTanznia.Former OAU Chairman)



AfriNIC
e Internet Numbers Registry for Africa

The End.

Thank you Very Much for your attention



Adam Mambi

- Deputy Executive Secretary (Director & Head, Research Dpt), Law Reform Commission of Tanzania
- Part-time Lecturer, ICT/Cyber Law & Intellectual Property Law, University of Dar Es Salaam.
- Advocate of the High Court, Tanzania
- Expert on ICT/Cyber Law & Intellectual Property Law
- Email: adammambi@yahoo.co.uk
- Mobile Phone: +255 (0)713291302