CYBER SECURITY, CHALLENGES AND LEGAL ISSUES

Facilitator/Presenter

1. Adam Mambi, (LLM, Advocate)
   - Deputy Executive Secretary, Law Reform Commission Tanzania
   - Part-time Lecturer Cyber Law/ICT Law, Intellectual Property, University of Dar Es Salaam. Tanzania
   0768291302
What is cyber /computer/information Security?

- Security under cyber space
- The branch of Security dealing with digital or information technology.
- is the prevention of unauthorized access and/or damage to computer systems via internet access.
- entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.
- involves protecting that information by preventing, detecting, and responding to attacks.
- How much of your personal information is stored either on your own computer or on someone else's system?

Building confidence on the use of ICT.
Cyber Security & Legal Issues

- Cyber Security is another key area that raises legal issues such as cyber crimes.
- Cybersecurity is one of the most profound challenges of our time. (Theft of identity, hacking, cyber-terrorism, e-financial crimes)
- The costs associated with cyberattacks are significant—in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages.
- Some use ICT benefits to the detriment and harm of others.
- Technology facilitates the commission of “old fashioned crimes” such as fraud, theft, money laundering, terrorism etc.
- Technology creates new illegal activities such as computer hacking, distribution of computer viruses, unsolicited emails and other related computer misuse.
- Easy to manipulate information online. Internet removes the geographical boundaries.
Key Legal Issues to be addressed in cyber security and privacy

- e-commerce, & Cyber crimes
- e-security/e-Privacy & Data protection
- Content regulation
- cyber-stalking
- e-abuse of women & children
- e-identification
- Consumer protection
- e-Jurisdiction problem
- Converged technologies
Definition of some ICT concepts

**What is cyber/computer crime?** refers to crimes that are:

- committed electronically
- committed using computer technology.
- committed using information technology
- Cyber-crimes are the crimes which had already existed before the emergence of computer.
- The computer provided a new tool by which the offence is done. Examples of this type are theft, fraud, industrial espionage, facilitation of prostitution, terrorism and forgery.
Challenges on Cyber Security

1) Lack of Legal Framework at national and Regional Level (EAC & Africa)
2) Nature of offences
3) Nature of cyber space
4) Lack of Knowledge on computer forensic & e-evidence
5) Admissibility of e-evidence

Jurisdiction problem on enforcement
Legal implications of ICTs (e-security/Cyber crimes) & The Law

- Most affected Laws: Criminal, Evidence, civil, commercial laws etc

- Why?
  - The Laws were made before the development of Computer technologies
  - Laws were made to facilitate paper based transactions
  - There was no ICT Law/Cyber Law/Computer Law—There was a gap between ICT/Cyber Space and Law

- The Law has now been developed to bridge the gap
Examples of Cyber or computer crimes

- Fraud, hacking, theft of data/information, e-financial crimes, phishing,
- Cyber-terrorism, cyber-corruption, cyber-stalking, e-child grooming, e-child pornography, spoofing attacks, defacement attacks
- Data theft, payment fraud and other related frauds, software and data theft
- Unsolicited emails, distribution of e-viruses, publications of obscene materials
- Do our Laws cater for these e-offences?
- The UK Computer Misuse Act 1990 deals with cyber crimes, jurisdictions and extradition
CYBERCRIME TYPES

**Target**
- Viruses
- DoS

**Weapon**
- IPR
- Spam

**Accessory**
- Fraud
- Id-Theft
How serious is the problem?

- How much computer misuse is committed?
- *Who commits the misuse?*
- *How much does it cost?*
- *Who do we believe?*
- The media?
- The computer security consultants
- The police?
- Academics?
- Users such as banks?
- System Administrators?
FACTS AND FIGURES for Cyber Crimes:

Cybercrime is worth an estimated 105 billion dollars and cybercriminals can earn around 23,000 dollars a week. (rival computer security firm McAfee)

Several computer security consulting firms estimate global financial losses from viruses, worm attacks and other hostile computer-based attacks to be between $13 and $226 billion (the Congressional Research Service).

Cybercrime in Africa is growing faster than anywhere else. Out of the top ten countries in the world with a high level of cybercrime prevalence, Africa is host to four of them (Nigeria, Cameroon, Ghana and South Africa).
Legal Issues on Cyber Crimes & Role of Cyber Law;
(1) Computer fraud & theft of Information/Data

- What is fraud under the existing laws (Ss 120, ?)
- What is computer fraud?
- Can e-information be stolen?
- What is “theft” under the current Laws (Penal Code)?
- 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?
- Issues: can the computer be deceived?

Relevant Case: US v. Girard and Lambert 138 DLR 73
Consider the offence of theft in the following scenario

- **Does a person who uses computer system to transfer funds temporarily from somebody's account to his account commits an offence of theft?** His aim is to gain interest and return the funds.

- The answer might be **NO**. He does not commit an offence of theft.

- **WHY?** No intention to *permanently depriving* the owner.

See **R v. Lloyd [1985] 2 All ER**

See also **Chan Man-sin v. AG [1988] All ER**
Legal implication of e-security under e-banking

- E-banking might raise legal issues on the question of privacy and data protection.
- The security risk might cause banks and other related financial institutions to loose gain and hope of e-banking if the legal issues are not properly addressed.
- 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.
- There is a great concern on the threat which the improper use of data processing techniques, access and storage of such information can pose to the rights and freedoms of those individuals whose personal data is subjected to some form of automated processing.
- Consumers lack confidence.
- There is no highly assured security against fraud and other related cyber offences.
7. Cyber-laundering

- In the beginning, laundering money was a physical effort required that the launderer have the means to physically transport the hard cash.
- ICT (e-commerce) simplifies and facilitates money laundering (cyber-money laundering) technology facilitates anonymous Digital Cash Laundering
- Cyber-laundering done by means of anonymous e-cash. Anonymous e-cash may facilitate money laundering on the Internet
- Wire transfer systems allow criminal organizations, as well as legitimate businesses and individual banking customers, to enjoy a swift and nearly risk free conduit for moving money between countries.
Why cyber Security?

Cyber Security, Privacy, and Trust aim at improving the e-security and privacy of individuals, enterprises, Governments and the entire cyber space.

Building confidence & empower the Internet users.

enable and encourage e-commerce (e-business), e-prosecution

Protect children online

e-confidence and e-security play crucial role in building a secure and global information society
Challenge on CROSS-BORDER JURISDICTION

• Why does the cyber space have no owners, is lawless and illimitable?
• One of the reasons is the fact that Internet is a free-flow information channel.
• This fact has however created a new problem which concerns jurisdictional issues.
• Whenever a crime is committed via cyberspace, the court will face a problem in deciding which country’s jurisdiction does the committed crime fall under.
e-Jurisdiction problem/Legal issues

- The cyberspace has no boundaries.
- Which country has the right to arrest e-crime offenders and prosecute?
- Which enforcement agency will have jurisdiction under the cyberspace?
- Which Legal System will apply? (Refer Yahoo Case 2000)
- Jurisdiction problem on prosecution
- How can we address Legal issues at Regional and global level?
- How can e-Providers/ISP/OSP be liable and how can they defend themselves?
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
- age cheating
- Use of different legal systems

- 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
Yahoo Case, 2000

- A French judge ordered Yahoo.com (California, US) to implement technical or access control measures blocking auctions featuring Nazi memorabilia hosted on the Yahoo.com site from French residents.

Yahoo’s arguments
- Its flagship site, Yahoo.com, was targeted primarily toward a U.S. audience and not intended for a French audience and users
- Only U.S. law would be binding,
- A French judge could not credibly assert jurisdiction over the site.

Courts Decision
- Judge Gomez of the Paris Court ruled that he was entitled to assert jurisdiction over the dispute since the content found on the Yahoo.com site was available to French residents and was unlawful under French law.

See Article 22 (jurisdiction) European Convention on Cyber Crime
Privacy, Surveillance
Data Protection

- The processing of Data gives rise to many privacy, e-security, misuse in cyber space activities.
- Personal data such as credit cards etc may be routed via countries with lack of data protection.
- Threats on the use of data processing techniques on freedoms & rights of individuals.
- The threats range from risks of data security and privacy, system intrusion etc.

How to regulate and protect data at national and Regional Level?

Some Countries have Data Protection Laws.
Content Regulation under cyber space

- What type of information content that need to be transmitted electron lay?.
- How about freedom of information/speech?
- E-distribution of illicit contents
- Children protection against obscene materials
- e-content regulation has been a great debate over the world
- How to harmonize different Policies and Legal system to have a common understanding?
- How can e-Providers/ISP/OSP be liable and how can they defend themselves?
e-Children protection

- Legal implications of ICT to Children
- What is ICT doing to Children?
- e-Child pornography under the digital era
- Dangers Children Face on-line?
- Exposure to inappropriate & harmful materials (obscene, drugs & alcohol)
- Young Persons/Children most vulnerable
- Internet Grooming- e-abuse of children
- How can we make cyber-world a safe place for young people to work, learn and play?

Some Regulations available in TCRA

9/10/2012
Identification problem. How to identify criminals/culprits/exploiters

- Presence of anonymity under Internet/cyberspace.
- Difficult to identify criminals/culprits
- The identification and investigation may be hard
- Anything can happen anywhere by any one
- Content can originate and be accessed to locations anywhere around the world,
- 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? (}
The Role of Intermediaries (ISPs/OSPs)

- ISPs play a big role on computer users to access materials online.
- Facilitate access to materials on the internet and gain financially.
- Facilitate transactions and communications for end-users and identification of parties.
- ISPs are under risk of liability if they host a website displaying obscene materials.
- They are concerned about unknowingly committing an offence of possession of children obscenities.
What will be the Legal Basis for Intermediaries Liability?

- Knowledge?
- Possession? Or Transmission?
- Intention to distribute?
- What acts that can be committed by ISPs to make them liable?
- Where are these acts committed?
- Should we grant ISPs some limited immunity from liability for 3party content?
electronic evidence

- electronic evidence is the proper medium to prove the perpetration of crimes committed with new technology.
- The use of electronic evidence has become a necessary element to deal with in order to solve crimes committed with or through electronic devices.
- Generally there are three requirements for the evidence to be admissible in the court. (a) Authentication, (b) the best evidence rule, and (c) exceptions to the hearsay rule.

- Under physical world, transactions depends partly on trust with documented agreements.
- Agreements/contracts are made, witnessed physically and authenticated with original documents manually signed.
Most Common Law Statutes recognize the **Best Evidence Rule (Original & signed Documents).**

Admissibility of evidence depends on original documents.

However in Electronic transactions the situation might be different as the parties to the agreement may never have physically met or spoken.

Do we have Court Rules on other statutory Rules e- evidence?

The best evidence rule requires that the original of any record or document in a written form and signed, be used if available.

- **Is the print-out of an email message the original?**
- **If there is a dispute about the authenticity of an email, which will hold more force?** (the electronic version or the printed)
Any crime can create digital evidence

Cybercrimes - Computer used to commit crime
- Illegal access to computer systems - “hacking”
- Interference with data or computer systems

MANY CRIMINALS DO NOT KNOW ABOUT THE DIGITAL EVIDENCE THEY CREATE!
The Role of The Judiciary on the legal implication of technology in Tanzania

- The lacuna on the admissibility of electronic evidence was tested by the High Court of Tanzania Commercial Division in the case of Trust Bank Tanzania Ltd. v. Le-marsh Enterprises Ltd., Joseph Mbuui Magari, Lawrence Macharia [2000].

- The Court through Nsekela, J. as he then was, boldly adopted the provisions of the English Civil Evidence Act, and the Seychelles Evidence (Bankers Books) Act Cap 75 on computer documents and other authorities.

- The issue before the court was whether Computer/electronic Evidence is admissible in our Courts under our Laws.
Status of Cyber Laws, Tanzania/How Tz dealt with cyber Security

- No Specific law on Cyber Crime & Data
- There as some development in making laws to cope with implications of ICT
- In 2007, The Evidence Act was amended to accommodate e-evidence
- Done after the LRCTs Report and the Courts Decision on the admissibility of e-evidence.
- Electronic and Postal Communications Act, (EPOCA), 2010
- Draft Regulation on m-banking
- Draft Bill on e-transactions & e-payment
- Draft Regulations on the establishment of CERTS
- Draft Regulations on e-procurement
Regional & International Initiatives e.g. Legal Instruments

1. **UN Level-No Legal Instrument**

2. **Regional Level:**

   (1)-Africa-Draft Convention on Cyber Security

   - Each Member State shall adopt legislative measures to combat criminal offenses and acts which affect the confidentiality, integrity, availability of data and related infrastructure networks.

   - Member States shall take into account the approved language choice in international cyber crime legislation models, such as the language choice adopted by the Council of Europe.
(c) Europe: EU Convention on Cybercrime, 2001.

- Provides for cyber crimes, privacy, data protection, child protection online, international cooperation
- Applicable at International level. Non-EU can also be members
- Several non-member States in the Council of Europe such as Canada, Japan and South Africa signed the convention, which was also ratified by the United States
INSTITUTIONAL ARRANGEMENTS FOR CYBER CRIME

• The government of Tanzania has task forces within various institutions that deal with problems relating to cyber crimes:
  - The Police Force,
  - Tanzania Communications Regulatory Authority (TCRA),
  - The Prevention and Combating of Corruption Bureau (PCCB), and
  - Tanzania Intelligence and Security Service

• The Criminal Investigation Department of the Tanzania Police Force reports that about 275 cyber crime cases were handled and investigated out of which 99 cases were completed in the year 2010 (http://www.policeforce.go.tz/)

• Cyber-crimes Unite has been established under the Police Force of Tanzania (Capacity???)
What Should be done to ensure e-security?

- adopt effective legal framework to combat cybercrime and other misuses of information technology.
- Enact enforceable cyber laws in a well-defined geographical boundaries that are either national or regional.
- need for international cooperation, information sharing, and investigative assistance— See Article 23 & 25 EU Cyber Convention
- involve all relevant stakeholders in initiatives in a framework of international cooperation.
The End.

Thank you Very Much
for your attention

❖ Adam Mambi

• Deputy Executive Secretary, Law Reform Commission Tanzania
• Advocate of the High Court
• Expert on Cyber Laws/ICT Law & Intellectual Property
• UN Consultant on e-commerce & CyberCrimes

• Email: adammambi@yahoo.co.uk
• Mobile Phone: 0713291302/0768291302

9/10/2012 Copyrighted Work--A. MAMBI 36