CYBER SECURITY LEGISLATION AND POLICY INITIATIVES - UGANDA CASE

2009 ITU Regional Cybersecurity Forum for Africa and Arab States

Tunis, 4-5 June 2009

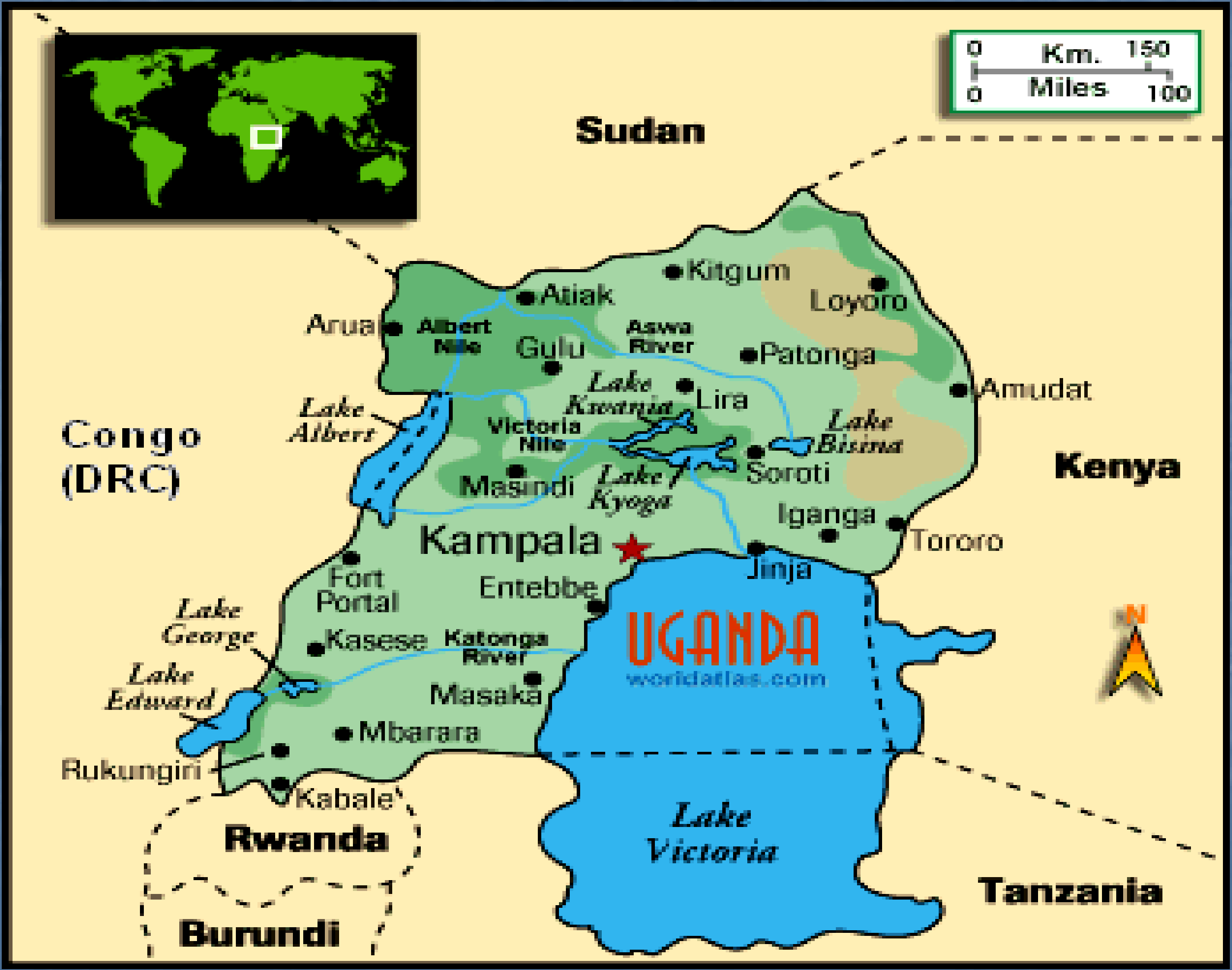
Patrick Mwesigwa, Director/Technology & Licensing, Uganda Communications Commission

UGANDA
COMMUNICATIONS
COMMISSION

Outline of presentation

- Introduction on Uganda
- Cyber laws formulation process
- Overview of proposed cyber laws
- Progress in harmonisation of Cyber Laws in East Africa
- National and Regional CERT initiatives
- Challenges in countering cyber crime
- Concluding remarks

Background on Uganda - location



Economic indicators

- Population – 30 million
- Surface Area – 241,000 sq. km
- GDP per capita - US$ 230
- Economic Growth (1995-2008) – 6% p. a

UGANDA
COMMUNICATIONS
COMMISSION

Cyber laws formulation process

- Formulation of cyber laws initiated in 2003
- Cyber laws drafted by National Task Force comprising several stakeholders led by Uganda Law Reform Commission that included
  - Ministries of Justice, Trade and Industry, Water, Lands & Environment, Ministry of Finance
  - Ministry of Works Housing & Communications, now Ministry of ICT
  - Uganda Communications Commission
  - Uganda Law Society, National Bureau of Standards
  - Bank of Uganda, Uganda Investment Authority, Makerere University, Uganda Insurance Commission etc
- Draft went through public consultation
- Benchmarking with other countries undertaken

Overview of proposed cyber laws

UGANDA
COMMUNICATIONS
COMMISSION

Cyber Security legal framework

Legal framework consists of 3 main laws:

- Electronic Transactions Bill, 2003
- Computer Misuse Bill, 2003
- Electronic Signatures bill, 2003

The Electronic Transactions Bill

- The Bill creates a light handed regulatory regime for electronic transactions.
- It facilitates the development of e-commerce in Uganda by broadly removing existing legal impediments that may prevent a person from transacting electronically because of a lacuna in the traditional laws.
- it makes provision for functional equivalence, thus paper transactions and electronic transactions are treated equally before the law.

UGANDA
COMMUNICATIONS
COMMISSION

Electronic Transactions Bill *contd*

- Establishes rules that validate and recognises contracts formed through electronic means
- Sets default rules for contract formation and governance of electronic contract performance
- Defines the characteristics of a valid electronic writing and an original document
- Supports the admission of computer evidence in courts and arbitration proceedings

The Electronic Signatures Bill

- The Bill makes provision for the use of electronic signatures in order to ensure that transactions are carried out in a secure environment.
- It establishes a public key infrastructure for authenticity and security of documents
- Recognises the different signature creating technologies
- Provides effective administrative structures e.g. establishment of Certification Authorities

The Computer Misuse Bill

- The Bill takes cognisance of the fact that all computer operations are susceptible to computer crimes and our current legal system does not recognise computer crimes thus the importance of a legislation to provide for computer crimes.
- It creates several computer misuse offences e.g. unauthorised modification of computer material
- lays down mechanisms for investigation and prosecution of the offences.

Status of the proposed cyber laws

- The bills already approved by cabinet
- Currently under consideration by Parliament
- Expected to be approved by Parliament by end of 2009

UCC
UGANDA
COMMUNICATIONS
COMMISSION

Harmonisation of cyber laws in East African Region

- Ongoing process to harmonise cyber laws in the 5 E A countries under EAC
- Being undertaken by Task Force consisting of 4 members from each country
- Laws to be harmonised in 2 phases;
  - Phase 1: Electronic Transactions, Electronic Signatures and Authentications, Data Protection and Privacy, Consumer Protection and Computer Crime
  - Phase 2: Intellectual Property Rights, Domain Names, Taxation and Freedom of Information
- several regional meetings held, legal framework expected to be adopted by relevant organs of EAC and Partner States expected to enact the cyber laws by 2010

Status of cyber laws in E Africa

	Electronic Signature	Consumer Protection	Privacy	Cyber Crime	Online Content Regulation	Digital Copyright (WIPO Treaty, 1996)	Electronic Contracting	Online Dispute Resolution
Burundi	None	None	None	None	None	No	None	None
Kenya	Draft	Draft	Draft	Draft	None	Signatory	Draft	None
Rwanda	Draft	Draft	Draft	Draft	None	No	Draft	None
Tanzania	None	None	None	None	None	No		None
Uganda	Draft	Draft	None	Draft	None	No	Draft	None

Source: Report of 2nd EAC Task Force Meeting

Challenges in countering cyber crime

- Lack of awareness by users, law enforcement officials and policy makers on the adverse impact of cyber crime and measures to safeguard against cyber crime
- Lengthy process for putting in place necessary legislation
- Rapid changes in technology hence requiring more sophisticated tools to combat cyber crime
- Limited use of internet and low bandwidth availability which discourage use due to spam etc.

National Information Security Working Group

Uganda is in process of establishment of Information Security Working Group under Ministry of ICT with the following key ToRs among others:

- Developing guidelines for Computer Security Emergency Response Teams
- Coordinating Computer security incident response
- Collaboration with national, regional and international partners in information security
- Conducting regular seminars, conferences, and workshops for local and central government

Composition of Working Group

Ministry of ICT

Ministry of Finance, Planning & Econ. Development

Ministry of Internal Affairs

Ministry of Foreign Affairs

External Security Organisation

Internal Security Organisation

Uganda Police

Directorate of Public Prosecution

Judiciary

Uganda Communications Commission

Makerere University

Proposed East African CERTs

At the recent EARPTO Congress the 5 E A countries agreed to set up National CERTs whose mandate includes:

- Monitoring cybersecurity incidents and respond appropriately
- Giving recommendations, advice and guidelines for improvement of cybersecurity
- Dissemination information on management of cybersecurity incidents
- Collaboration with service providers, security and international organisations on cybersecurity matters

Concluding remarks

- Need to sensitize policy makers, network operators and individuals on the matters related to cyber security and in particular encourage all countries to put in place robust legal frameworks to combat cyber security threats.

- Because of the borderless nature of cyberspace, international cooperation is crucial in ensuring a safe online environment.

Thank you for your attention!

E-mail: pmwesigwa@ucc.co.ug

UCC
UGANDA
COMMUNICATIONS
COMMISSION