The status of Cybercrime in Tanzania

Strasbourg, France

Presented at the Octopus Conference on Cooperation Against Cybercrime

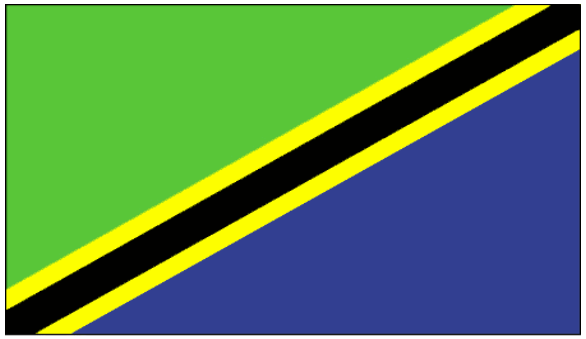
&

10th Anniversary of the Budapest Convention

By

Saidi M. Kalunde

[State Attorney - AG Chambers]



Policy, Legal & Regulatory Framework

There is **NO** specific Legislation on Cybercrime:

Cybercrimes in Tanzania: Computer Fraud, Hacking, IP Crimes, ATM Fraud, DoS

Victims: Government Agencies, Banks, Private Business, Universities, Public

The Tanzania ICT Policy 2003:

Cyber-criminals around the world are constantly seeking loopholes through which to perform illegal or illicit businesses. Any country that has ***inadequate*** cyber-law is essentially offering a ***safe-haven*** for ***cyber-criminals*** to act with impunity.

P**olicy Statements:**

- The Government will ***set-up legal regulatory*** frameworks that are appropriate to the ICT sector taking into account that ***electronic transactions*** are also susceptible to electronic ***criminality.***
- The Government will have compelling interest in ***shielding contents inappropriate for minors*** or those that promote behavior that might endanger minors and society.

Legal & Regulatory Framework

Legislations & Regulations, Guidelines:

- Electronic & Postal Communications Act, No. 3 of 2010 [CAP 306 R.E 2002]:
- Penal Code [CAP 16]
- Amendment to the Tanzania Evidence Act [e-Evidence]
- Draft bill on e-transactions,
- Draft bill on e-Payment systems
- There is an initiative to build up a CERT Regulations under s. 124(1) of the Electronic and Postal Communications Act No. 3, of 2010. The Draft Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2011

  [http://www.tcra.go.tz/regulation/draftRegulation/5_RegulationsCERTJune2011.pdf]
- Initiative to develop, guidelines on Search, seizure, collection, storage and presentation of e-evidence [DPP]

Regional Framework:

- Draft AU Convention on the Establishment Legal Framework for Cyber Security
- EAC Cyber law Framework Phase I & II: [Incorporates CoE Convention]
- Initiatives under SADC [SADC Model Law on e-Comerce]

Institutional Framework

Division of Public Prosecutions [AG]: Cybercrime Schedule [June 2011]:-

- Coordinate Investigation & Prosecute Cybercrime cases
- Review and propose policies, laws, regulations, guidelines and standards on the management of fraud, corruption and ***cybercrime***;
- Coordinate and provide guidance to all law enforcement agencies in fraud, corruption, ***cybercrime*** and other related offences

Tanzania Police Force: Cybercrime Unit:

- Specialized team of police investigators specialized in cybercrime investigation
- Few years of experience[24/7 centre]

Tanzania Communication Regulatory Authority [TCRA]

- ICT security Policy &Regulatory Body

Financial Intelligence Unit [FIU]

Challenges/Way Forward

- Absence of a robust legal regime on cybercrime
- Harmonization of Laws, Legal and Regulatory Frameworks
- Institutional Capacity vs. Capacity Building [AG, Police, Judiciary, Parliament]
- Policy issues vs. Legislative Priority
- Inadequate Funding
- Mobile Money Industry [Related VAS products]

Contact:
Saidi M. Kalunde
attorney General's Chambers
Public Prosecutions Division
P.O. Box 71069
Mobile: +255784788212, +255715788212
Email:saidimj@gmail.com