HIPSSA Project

Support for Harmonization of the ICT Policies in Sub-Sahara Africa,

Workshop on Lesotho National Transposition of SADC Model Laws
Maseru, Lesotho,1 March 2013

Presenter: ***Judith M.C.Tembo*** HIPSSA International Legal Expert - cybercrime

International Telecommunication Union
Committed to connecting the world

1. Summary

- Context
- Background
- SADC Model Law on Cybercrime
- Conclusion

2.Background

- Context – Development of Lesotho law on cybercrime
- model law on cybercrime
- Globalization has given rise to activities and transactions increasingly conducted via ICT and internet
- ICT applications - e-Government, e-Commerce, e-Education, e-Health and e-Environment, seen as enablers for development, as they provide efficient channel to deliver a wide range of basic services
- Challenges - attacks against information infrastructure and internet, and cyber threats (legal, technical, institutional)
- Risks

  - financial, economic, health, security, technical etc
- Need to protect information infrastructure and internet against cybercrime

2.Background

1.0 Legal measures – cybercrime legislation (as part of cybersecurity strategy)

- Internet borderless, challenges global, global solution needed
- Harmonization of legislation needed

2.0 SADC countries situation analysis as at February 2011:

-countries with cybercrime laws,

-countries with cybercrime laws under development

- countries with cybercrime related laws

2.1 Countries with cybercrime laws:

Botswana , Mauritius, South Africa, Zambia

2.2 Countries with cybercrime legislation under development/cybercrime related legislation:

Angola, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mozambique, Namibia, Swaziland, Seychelles, Tanzania, Zimbabwe

2.Background

Cybercrime is to a large degree abuse of technology for criminal purposes

- Cybercrime legislation - is part of cybersecurity strategy)
- Efficient penal legislation criminalising certain forms of computer crime and cybercrime (crimes against computers, computer system, content related offences)
- Existence of related procedural instruments that enable law enforcement to carry out investigations are essential requirements for the involvement of law enforcement agencies in the fight against computer crime and cybercrime
- Lack of adequate cybercrime legislation

- deprives law enforcement agencies of effective tools to support citizens that have become victims of cybercrime

-might protect /encourage offenders from abroad to move their illegal activities to countries with such legislation

2. Background

- Harmonisation important because mutual legal assistance usually based on dual criminality ie investigations globally usually limited to crimes criminalised in all affected countries

SADC Model Law On Computer Crime and Cybercrime

- Model Law on Computer crime and cyber crime

- Law adopted by SADC ICT Ministers of at annual meeting held in Mauritius from 6-8 November, 2012
- adapted to regional requirements but harmonised in line with international standards (definitions, criminalisation of certain offences, terminology, etc) – common understanding
  - UN resolutions
  - CoE Convention on Cybsercrime
  - Organisation of American States
  - ITU Tool kit
  - Commonwealth Model Law
  - AU
  - EAC Framework on Cyberlaws
  - ECOWAS Supplementary Acts

SADC Model Law On Computer Crime and Cybercrime

Model law Cont'd

Divided into six parts

1. Preliminary
2. Substantive criminal law provisions (offences)
3. Jurisdiction territorial and extra-territorial (ship/aircraft registered in enacting country, citizen etc)
4. Electronic evidence – admissibility
5. Procedural law – investigative procedures and tools
6. Limitation of liability – carriers

Penalties – severity effectiveness/deterrence.

SADC Model Law On Computer Crime and Cybercrime

- PART I. Preliminary
- Short Title
- Objective
- Definitions

SADC Model Law On Computer Crime and Cybercrime

PART II. Offences

1. Illegal Access
2. Illegal Remaining
3. Illegal Interception
4. Illegal Data Interference
5. Data Espionage
6. Illegal System Interference
7. Illegal Devices
8. Computer-related Forgery
9. Computer-related Fraud

SADC Model Law On Computer Crime and Cybercrime

10. Child Pornography
11. Pornography
12. Identity-related crimes
13. Racist and Xenophobic Material
14. Racist and Xenophobic Motivated Insult
15. Denial of Genocide and Crimes Again Humanity
16. SPAM
17. Disclosure of details of an investigation
18. Failure to permit assistance
19. Harassment utilizing means of electronic communication

SADC Model Law On Computer Crime and Cybercrime

PART III. JURISDICTION

20.Jurisdiction

PART IV.ELECTRONIC EVIDENCE

21.Admissibility of Electronic Evidence

SADC Model Law On Computer Crime and Cybercrime

PART V. procedural law

22. Search and Seizure
23. Assistance
24. Production Order
25. Expedited preservation
26. Partial Disclosure of traffic data
27. Collection of traffic data
28. Interception of content data
29. Forensic Tool

SADC Model Law On Computer Crime and Cybercrime

PART VI. Liability

30.No Monitoring Obligation
31.Access Provider
32.Hosting Provider
33.Caching Provider
34.Hyperlinks Provider
35.Search Engine Provider

4. Conclusion

- cybercrime legislation important in context of misuse of ICT for criminal ourposes
- Legislation that facilitates international co-operation in investigations and effective penalties important
- Lack of effective penalties, differences in terminology, acts covered in offences, non-criminalisation of certain offences and or lack of provision for certain procedural instruments, and penalties encouragement for safe havens;
- SADC Model law on computercrime and cybercrime important building block for developing of Lesotho cybercrime legislation
- Differences including significant differences in penalties for offences of concern vis-avis effectiveness of deterrence provided for cybercrime and the need for removal of safe havens to would-be offenders;
- Harmonisation of laws in line with global standards to effectively fight cybercrime, remove safe havens improve international cooperation in the framework of cybercrime investigations and prosecution is essential.

Thank you for your attention!

jmctembo@hotmail.com

International Telecommunication Union

Committed to connecting the world