ITU – EC HIPSSA Project

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

Sadc Harmoniseed Legal Cyber Security Framework For Southern Africa

2nd Stakeholders Workshop on National Transposition of SADC Cybersecurity Model Laws into Zimbabwe Law, Harare, Zimbabwe, 15 - 19 July, 2013

Presenter: ***Judith M.C.Tembo*** ITU HIPSSA International Expert on cybercrime

Overview of Draft Zimbabwe Computer Crime and Cybercrime Bill

Draft Computer Crime and Cybercrime Bill Zimbabwe

Draft Computer Crime and Cybercrime Bill Zimbabwe

A. Objectives

- Act provides a legal framework for the criminalisation of computer and network related offences.
- Principal aims are to criminalize certain illegal content in line with regional and international best practices, provide the necessary specific procedural instruments for the investigation of such offences and define the liability of service providers.

B. Provisions

- Draft Bill divided into nine parts – All provisions of Model law on cybercrime transposed and expanded as appropriate to suit Zimbabwe situation;
- Terms used and provisions other than those peculiar to Zimbabwe law defined;
- Proposed Bill, drafted using technology neutral language.

Draft Computer Crime and Cybercrime Bill Zimbabwe

- Bill avoids over-legislating and facilitates both technological advancements and new and innovative developments in cybercrime.

Part 1 - provides definitions and sets objective of Act, scope/application and date when Act will come into force;

- defines terms such as “computer system”, “access provider” and “hinder” etc., using sufficiently broad wording and where possible illustrative examples.

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part I Cont'd

-As far as possible, technical terms been defined to provide certainty as to which terminology's been left to judicial construction

Part II - provides Substantive criminal law provisions (offences)

-purpose of Sections 4-25 of the Act is to improve means to prevent and address computer and network-related crime by defining a common minimum standard of relevant offences based on best practice prevailing within the region as well as international standards. (eg CoECC, C/wealth Model Law)

- Ss.4-25 therefore provides minimum standards and therefore allows for more extensive criminalisation should country so desire.

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part II Cont'd

- all offences established in Act require that offender is carrying out offences intentionally. Reckless acts are therefore not covered.
- "person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification..."

  - eg Section 5 requires that the offender is carrying out the offences intentionally. Reckless acts are not covered.

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part II Cont'd

- provides a set of substantive criminal law provisions that criminalise certain conduct - eg illegally accessing and remaining logged into a computer system without lawful excuse or justification, obstructing, interrupting or interfering with the lawful use of computer data and disclosing details of a cybercrime investigation
- Other than unauthorised access to computer or computer system, unauthorised manipulation of computer programme, and to some extent, illegal devices (restricted to computer virus), and identity theft as defined (Criminal Code S.163 -168)*, illegal interception (telecommunication under Interception of Communications Act), offensive/false phone messages (Postal & Telecom Act S.88) none of these acts are currently legislated against by existing legislation in Zimbabwe.

Draft Computer Crime and Cybercrime Bill Zimbabwe

- **Part III** provides procedures to determine jurisdiction over criminal offences enumerated in Sections 5-25
- Jurisdiction – territorial/extra-territorial/nationality (ship/aircraft registered in enacting country, citizen etc)
- S.25 (1)- Territorial jurisdiction applicable if

  - both person attacking computer system and victim system are located within same territory or country.

  - computer system attacked is within its territory, even if attacker is not.

Draft Computer Crime and Cybercrime Bill Zimbabwe

- S26(1)(d) – applies if a national commits an offence abroad, and conduct is also an offence under law of state in which it was committed

Part IV. Electronic evidence – deals with admissibility of electronic evidence and incorporates by reference law dealing with electronic transactions & communication to apply

Part V. Procedural law – Provides a set of procedural instruments necessary to investigate Cybercrime;

- identification of offenders, protection of integrity of computer data during an investigation contains several inherently unique challenges for law enforcement authorities.

Draft Computer Crime and Cybercrime Bill Zimbabwe

- purpose of Part V - to improve national procedural instruments by defining common minimum standards based on best practices within the region as well as international standards. - definition of standards will help national lawmakers to discover possible gaps in the domestic procedural law. Sections 29-36 only define minimum standards and therefore do not preclude creation of more extensive criminalization at national level.
- introduces new investigation instruments (eg. Section 36) and also aims to adapt traditional procedural measures (such as Section 29). All instruments referred to aim at permitting obtaining and/or collecting of data for purpose of conducting **specific** criminal investigations or proceedings.
- instruments described in Part V to be used in both traditional computer crime investigation and in any investigation that involves computer data and computer systems.

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part VI Liability (Service Providers)

- defines limitations of liability of Internet service providers.
- responsibility of certain Internet service providers are limited in Act, if their ability to prevent users from committing crimes is limited - was therefore necessary to differentiate between the different types of providers
- Without clear regulation, uncertainty created as to whether there is an obligation to monitor activities and, whether providers could be prosecuted based on a violation of the obligation to monitor users' activities.

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part VI Cont'd Limitation (Service Providers)

- apart from possible conflicts with data protection regulations and secrecy of telecommunication, such obligation would especially cause difficulties for hosting providers that store significant number of websites. To avoid these conflicts S. 37 excludes general obligation to monitor transmitted or stored information.

- limits liability of providers to criminal liability.

Draft Computer Crime and Cybercrime Bill Zimbabwe

- **Part VII General Provisions –** administration of Act - includes issuance of Regulations

  – eg interception of computer data (security, functional and technical requirements for interception, etc),

  - critical information infrastructure (identification, securing integrity and authenticity of, registration and other procedures relating to critical information infrastructure, etc)
- **Part VIII(Consequential Amendments)** of legislation needing to be amended for purposes of bringing it in line with draft Bill ie
- Criminal Code, Chapter 9:23

Draft Computer Crime and Cybercrime Bill Zimbabwe

Amendment of Section 163-168 Criminal Code – removal of provisions on unauthorised access, unauthorised manipulation of computer programme, illegal devices (restricted to computer virus), and identity theft as defined offensive/false phone messages (Postal & Telecom Act S.88)

Postal & Telecom Act Chapter 12:05, S.88 – removal of phone harrasment

Draft Computer Crime and Cybercrime Bill Zimbabwe

Detailed Provisions

- PART I. Preliminary
- Short Title & Commencement
- Application
- Interpretation

Draft Computer Crime and Cybercrime Bill Zimbabwe

PART II. Offences

4. Aggravating circumstances
5. Illegal Access
6. Illegal Remaining
7. Illegal Interception
8. Illegal Data Interference
9. Data Espionage
10. Illegal System Interference
11. Illegal Devices
12. Computer-related Forgery
13. Computer-related Fraud

Draft Computer Crime and Cybercrime Bill Zimbabwe

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

Draft Computer Crime and Cybercrime Bill Zimbabwe

24. Violation of Intellectual property rights
25. Attempt, abetment and Conspiracy

PART III. JURISDICTION
26.Jurisdiction
27. Extradition

PART IV. ELECTRONIC EVIDENCE
28.Admissibility of Electronic Evidence

Draft Computer Crime and Cybercrime Bill Zimbabwe

PART V. Procedural law

29. Search and Seizure
30. Assistance
31. Production Order
32. Expedited preservation
33. Partial Disclosure of traffic data
34. Collection of traffic data
35. Interception of content data
36. Forensic Tool

Draft Computer Crime and Cybercrime Bill Zimbabwe

PART VI. Liability

37. No Monitoring Obligation
38. Access Provider
39. Hosting Provider
40. Caching Provider
41. Hyperlinks Provider
42. Search Engine Provider

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part VII

General Provisions

43. Limitation of Liability
44. Forefeiture of Assets
45. General Provision on Cybercrimes
46. Regulations
47. Offence by body corporate or un-incorporate
48. Prosecutions
49. Compounding of Offences

Draft Computer Crime and Cybercrime Bill Zimbabwe

Part VIII

Consequential AMENDMENTS AND SAVINGS

Postal & Telecommunications Act, Chapter 12:05

50. Construction

51.Amendment of Section 88 (phone harassment)

Criminal Law Codification Act Chapter 9:23

51.Construction

52. Amendment of Section 162 – 168.

Schedule

Details of amended provisions and corresponding provisions in new law

Thank you for your attention!

jmctembo@hotmail.com