ITU-EC HIPSSA Project

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

2nd Stakeholders Workshop on National Transposition of SADC Model Laws on Cybersecurity into Zimbabwe law, Harare, Zimbabwe 15-18 July 2013

Transposition of SADC Model Law on Computer Crime and Cybercrime into Zimbabwe Law – Guiding principles

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

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

- Guiding principles – key principles taken into account when transposing SADC Model Law on Computer Crime and Cybercrime into Zimbabwe law

A. Key Principles

- **1. Definition of cybercrime** – No single definition - offences including traditional computer crimes, as well as network crimes committed using computers and computer networks.
- **2. Nature of crime**

  2.1 Types of offences – four categories
- Offences against confidentiality, integrity and availability of computer data and systems
- Content related offences
- Computer related offences

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

2.1.1. *Offences Against the Confidentiality, Integrity and Availability of Computer Data and Systems*

- offences in this category directed against at least one of the three legal principles of confidentiality, integrity and availability.
- Unlike crimes that have been covered by criminal law for centuries (eg. theft, murder), the computerization of offences is relatively recent, as computer systems and computer data were only developed over last sixty years.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

- effective prosecution of these acts requires that existing criminal law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles.
- most commonly occurring offences included in this category -
- illegal access (hacking, cracking) eg breaking of password-protected sites, circumventing password protection on computer system – usually used to commit further crimes, eg data espionage, data manipulation or denial-of-service (DoS) attacks

  - factors supporting increasing attacks include inadequate/incomplete protection of computer system, devt of software tools that automate attacks

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

- Data Espionage – illegal data acquisition –
- Illegal interception
- Data interference
- System interference

2.1.2 Content-related offences – content considered illegal, including child pornography, xenophobic material or insults related to religious symbols.

- development of legal instruments in this category more influenced by national approaches, which can take into account fundamental cultural and legal principles – which tend to significantly differ vis avis illegal content.

eg dissemination of xenophobic material illegal in many European countries, but can be protected by the principle of freedom of speech in some other countries.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

2.1.2 Content-related offences cont'd

common offences

- Erotic or pornographic material (excluding) child pornography
- Child pornography
- Racism, hate speech, glorification of violation
- Religious offences
- Illegal gambling and on-line games
- Libel and false information
- Spam
- Copyright and related offences, trademark related offences.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

2.1.3 Computer-related offences - category covers a number of offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles. - includes computer-related fraud *******, computer-related forgery, phishing, identity theft and misuse of devices.

2.1.4 Combination offences - category covers various terms used to describe complex scams that combine a number of different offences. Egs. include terrorist use of the Internet *, cyberlaundering and phishing.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

3. Challenges

3.1 Nature of crime (Medium involved) – computer / computer networks - offences against computers (eg. illegal access) vis-avis offences using computer to commit offence(eg. content related offences)

Issues

- acts needing to be criminalized – elements of offences, definitions, penalties

- organizational structures

- scale & volume of crime (eg malicious software, SPAM) vis-avis traditional law enforcement; identifying perpetrators, location

- evidence involved - electronic

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

3. Challenges cont'd

Organisational structures eg. Types of cybercrime units –which one??

- Cybercrime Units (offences against + by means of computers) - e.g. France, Cyprus, Czech Republic, Mauritius, Romania, Spain
- High Tech Crime Units (against + technical support) - e.g. Austria, Belgium, Ireland, Luxembourg
- Computer Forensic Units (forensics + technical support) - e.g. Brazil
- Central Units (intelligence + support) e.g. UK
- Crime-specific Units - e.g. UK-CEOP
- Specialised Prosecution Units - e.g. Romania, Belgium and Serbia.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

3. Challenges Cont'd

3.2 Borderless - absence of physical barriers - actions and potential victims for cyber-criminals not geographically limited; traditional evidence gathering techniques not effective – distinguished from traditional terrestrial crimes

- Issues

  – jurisdiction – extent

  - procedures

  - international dimension – enforcement, co-operation & collaboration

3.3 Cultural context – content offences

- Issues

  -discretionary/optional criminalization of certain acts

3.4 Capacity & capacity building – law enforcement, judiciary, parliamentarians, regulator, users, etc

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

- 2007 – estimated that revenues from cybercrime exceeded USD 100 billion in 2007, outstripping illegal trade in drugs for the first time

- 2009 - the USA, China, Brazil, Germany and India among countries reporting most malicious activities

- 2011 - PriceWaterHouseCoopers Global Economic Crime Survey, cybercrime ranked as one of the top four economic crimes. Reputational damage was the biggest fear for forty percent of the respondents.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

B. Features of cybercrime legislation

I. Taking into account nature of cybercrime:

- Technological neutrality – law should be drafted in such a way as to ensure its applicability to changing technology and techniques used to perpetrate criminal offences as far as possible.

II. Substantive laws –

- - must be made applicable to electronic transactions and digital assets including money and products (ie the one step recourse); preferably through specific stand-alone legislation or new provisions, but otherwise through amendment of existing laws and definitions, harmonized to international standards.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

II. Substantive laws cont'd

Pre-emptive measures – As far as possible should have effect of deterring and preventing offences from occurring rather than merely punish for offences that have occurred.

- Appropriate remedies – legislation should create a credible and effective deterrent effect and sufficient punishment to suit the nature and severity of the offence.

- Prescriptive jurisdiction – criminalize offences through applicable laws that have mutually enforcing effect globally, whether through extra-territorially applicable laws or a comprehensive network of same or similar laws or both.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

II. Substantive laws cont'd

- Legislation should - contain provisions covering **most common and internationally accepted forms of cybercrime as well as those offences that are of specific interest for the region e.g**. SPAM.

  -be compatible with both international standards and best practices, in order to ensure cooperation with law enforcement agencies from countries within and outside region.
- provide for the criminalization of the **intentional and illegal** accessing of a computer system as well as the illegal remaining in system.

  - Where circumvention of **protection measures** occurred to facilitate access, an increase in the severity of the penalty should be considered.
- Intentional and illegal **interception of non-public data transmission**, (illegal interception), should be criminalized, without hindering lawful interception by competent authorities.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

II. Substantive laws cont'd

- Where circumvention of protection measures occurred to facilitate the interception of the transmission, an increase in the severity of the penalty should also be considered.
- Cybercrime legislation should provide for criminalization of

  -intentional and illegal **interference with computer data** - should ensure that application of procedural instruments necessary for investigations is not hindered in cases where offender commits several offences and each only leads to limited damage.

  -Intentional and illegal **interference with computer systems**, (such as denial of service attacks), should be criminalized, and consideration be given to an **increased penalty, in cases where critical infrastructure is affected.**

  -intentional and illegal production, sale and related acts, of tools that are primarily designed to commit computer crimes, while ensuring that legitimate use of such software tools are not criminalized.

4.TRANSPOSITION OF MODEL LAW -GUIDING PRINCIPLES

II. Substantive laws cont'd

- criminalization of

  -intentional and illegal **computer-related fraud** and should ensure its compatibility with existing legislation criminalizing fraud, in circumstances where offenders are communicating with victims via electronic communications.

  -Intentional and illegal **computer-related forgery** ensuring that legislation covers acts such as the sending out of phishing emails. Consider increasing penalty in cases where numerous emails are sent out.

  -intentional and illegal **production and sale of child pornography**; and related acts taking into account international standards.

4.TRANSPOSITION OF MODEL LAW -GUIDING PRINCIPLES

II. Substantive laws cont'd

- criminalize

  -**possession of child pornography** and gaining **access to child pornography websites** with exemption to enable law enforcement agencies to carry out investigations.

- acts related to sending out of **SPAM** if it affects ability of users to utilize internet access and should reflect challenges related to attribution.
- intentional and illegal acts of **identity-related crime,** taking into account different phases of identity theft, (obtaining, transferring and using identity-related information).

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

III. Criminal law procedures

-Development of Effective but Balanced Procedural Instruments which Enable Competent Authorities to Investigate Cybercrime

- No procedural instrument should interfere with a **suspect's** internationally or regionally accepted **fundamental rights**.
- Legislation should enable competent authorities to order expedited preservation of computer data, as well as partial disclosure of preserved computer data.
- should facilitate **gathering of evidence and investigation** of computer related crimes, and investigators and detectives must be equipped and skilled with necessary expertise and technological know-how to investigate and deal with such

4.TRANSPOSITION OF MODEL LAW -GUIDING PRINCIPLES

III. Criminal law procedures Cont'd

-Development of Effective but Balanced Procedural Instruments which Enable Competent Authorities to Investigate Cybercrime

- should enable competent authorities to
  - order **production of computer data**.
  - use specific search and seizure instruments related to digital evidence and computer technology.

4.TRANSPOSITION OF MODEL LAW -GUIDING PRINCIPLES

III. Criminal law procedures Cont'd

- should **regulate search and seizure proceedings** in such a way to avoid collection of evidence being questioned, as not having been certified and produced as material evidence of data collected, and of existing digital environment.
- Competent authorities should be enabled to order lawful **collection of traffic data** and lawful interception of content data.
- should enable law enforcement to **use sophisticated investigation instruments** such as key-loggers and remote forensic software, to collect passwords used by suspect, or to identify connection used by suspect –
- should limit use of sophisticated instruments to serious crime

4.TRANSPOSITION OF MODEL LAW -GUIDING PRINCIPLES

IV. Development of Instruments for Transnational Cooperation in Cybercrime Investigations

Framework for international cooperation should **reflect international standards of cooperation as well as specific needs of cybercrime investigations -** should include creation of designated 24/7 point of contact for requests and enable use of expedited means of communication such as email and fax.

V. Jurisdiction

- Prescriptive jurisdiction – criminalize offences through applicable laws that have **mutually enforcing effect globally**, whether through extra-territorially applicable laws or a comprehensive network of same or similar laws or both.

4.TRANSPOSITION OF MODEL LAW - GUIDING PRINCIPLES

V. Jurisdiction Cont'd

- Enforcement jurisdiction – must have effective enforcement provisions (for full effect of system to work, particularly if offender or accomplices, instruments of crime or assets are in other jurisdictions).

- Adjudicatory jurisdiction – Criminal procedure laws must ensure that offenders cannot avoid being brought to courts in at least one country; eliminates /drastically reduces possibility of safe havens.

4.TRANSPOSITION OF MODEL LAW -GUIDING PRINCIPLES

VI. Development of a Framework Regulating the Responsibility of Internet Service

- **Providers**
- In cases where liability exists, framework should limit criminal responsibility of Access Providers with regard to offences committed by users of their service, if provider did not initiate transmission, did not select receiver and did not modify information contained in transmission.
- Criminal responsibility of Caching Provider should likewise be limited, if liability exists, for the automatic, intermediate and temporary storage of information.
- Also for the Hosting Provider, if liability exists, this should be limited by framework, in cases where the provider has no actual knowledge about the existence of illegal data or immediately removes them upon obtaining such knowledge.

4.TRANSPOSITION OF MODEL LAW GUIDING PRINCIPLES

C. Application of principles in transposing Model Law to Zimbabwe draft Computer Crime and Cybercrime Bill

In applying principles to transposing Model Law to Zimbabwe draft law, reviewed

- National ICT Policy for Zimbabwe
- national laws on cybercrime /cyber-related laws and regulations (Constitution, Communications Act No. 4 of 2012, Penal Code Act No. 30 of 2012, Race Relations Act, Labour Code Order, No.18 of 1992, Anti-Trafficking in Persons Act No. 1 of 2011, Criminal Procedure and Evidence (Amendment) Act No.3 of 2001).

4.TRANSPOSITION OF MODEL LAW GUIDING PRINCIPLES

D. Findings

- Zimbabwe ICT Policy – objectives (4.1) :
- No statute, in Zimbabwe, objective of which is criminalisation and investigation of computer and network-related offences.

E. Review findings vis-avis Model Law

- Zimbabwe ICT Policy findings consistent with Model Law provisions – Model law provisions harmonized with global standards vis-avis expected features of cybercrime law – eg Council of Europe Convention on Cybercrime, 2001 (COE) 2001 on elements expected to be covered in such law **** also endorsed by Commonwealth Model Law on Computer and computer Related Crime.

4.TRANSPOSITION OF MODEL LAW GUIDING PRINCIPLES

F. Action taken – Amending existing legislation / drafting new legislation - Issues

- amendment or separate legislation
- Amendment – challenges /best practice
  - electronic transactions - non-terrestrial and non-territorial
  - clarity, transparency and ease of recourse,

favours legislation directly dealing with computer and cyber crime preferably labeled as such, to amendment of different laws that may be applicable such as theft, fraud, identity theft and other legislation.

Legislation - Malaysia, Botswana, Sierra Leone, Ghana, Mauritius, Grenada, and Saint Kitts and Nevis, etc (UK, Singapore - dual approach).

4.TRANSPOSITION OF MODEL LAW GUIDING PRINCIPLES

G Draft Computer Crime and Cybercrime Bill Zimbabwe

- Above principles borne in mind when transposing Model law to Zimbabwe Law. In particular:
- Draft Law divided into eight parts – All provisions of Model law transposed and expanded as appropriate to suit Zimbabwe situation.

4.TRANSPOSITION OF MODEL LAW GUIDING PRINCIPLES

- Case demonstrations

Hopewell Nyamakazi v DPP Kwazulu Natal Case No.: AR215/08 – (review SA HC)

Appeal against conviction and sentence of 7years for fraud in respect of offences against Electronic Communications and Transactions Act 2002 (S.86(4) A/R Ss.1, 85 and 89(2) Electronic Communications and Transactions (ECT) Act 25 of 2002 and counts 18 to 34

- Conviction based on plea of guilty tendered in Magistrates court.
- Contested on ground that applicant did not understand charges and element of intent not proved by prosecution.

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- *while acting with other persons he ' unlawfully and intentionally [utilized] a device or computer programme in order to unlawfully overcome security measures designed to protect data or access to data, to wit an electronic card reader commonly known as a "Skimming Device", in order to gain unauthorized access to account information encoded on the magnetic strips as set on column 3 of schedule "A" of the charge sheet.*
- *purpose for use of the computer device or skimming device was to duplicate cards both debit and credit for his use.*

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- *that during the period August to September 2006 in Durban he duplicated the cards with the skimming device as charged, and 'committed the crime of fraud in concert with others by having performed the transactions set out' as charged*
- *admitted actions were designed for the purpose of 'self enrichment of myself and those with whom I acted in concert'*
- *pleaded guilty to having contravened relevant laws governing the ECT Act.*

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- In dismissing the appeal court stated that Applicant had pleaded facts to demonstrate that he was in fact guilty of contravening the relevant provisions. Paragraph 2.3 of the statement reads as follows:

  "I admit that whilst acting in common purpose with other persons, I did unlawfully and intentionally utilise a devise or computer programme in order to unlawfully overcome security measures designed to protect data or access to data, to wit an electronic card reader, commonly known as a ***"Skimming device"*** *in order to gain unauthorised access to account information encoded on the magnetic strips as set out in column 3 of schedule "A" of the charge sheet".*

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- Applicant did not only plead guilty to relevant charges, but he actually referred to the contraventions relevant to that specific Act and that is what is referred to in the charge sheet. **

- On the proper analysis of the plea explanation and the charge sheet in respect of counts 1 to 17 and the basic elements of the offences there are sufficient basis to justify the conclusion which the Magistrate came to when he indicated that he was satisfied with the plea explanation. The Magistrate's conclusion is confirmed by paragraph 2.15 of the plea explanation of the statement in terms of section 112(2) where he said that he had *no lawful defence to any charge mentioned in the charge sheet".*

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- Applicant's submission that he did not set out facts demonstrating that he knew that his conduct was unlawful, but instead that he merely pleaded the law, was entirely unfounded and was rejected.
- With respect to 'intent' that this was established by his own admission – particularly his statement that he knew that his actions were wrongful and unlawful in that he knew that the cards which he had presented for payment were duplicated or cloned and that the lawful card holders had never at any stage presented the lawful cards for payment.

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- In further determining whether or not, in all the circumstances of the particular matter, there in fact constituted a procedural irregularity, so that a failure of justice had resulted the court was satisfied that the alleged irregularities, such as may have resulted from non-compliance with the provisions of s. 112(2) of the Act, did not result in a failure of justice. (See : S v Carter 2007 (2) SACR 415 (SCA)).

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- Unauthorised access – exceptions – lawful authority
- **Sheryl Cwele, & anor v State** (671/11) [2012] ZASCA 155 (01 October 2012)

- Record of emails exchanged by two suspects, obtained in course of criminal investigations formally admitted by them, was admitted in evidence, in terms of section 15 of the Electronic Communications and Transactions Act (No.25 of 2002) as a true record of e-mails exchanged between. Investigation officer in this case obtained password from one of the suspects so as to gain access to her e-mails. He subsequently compiled a record of the emails exchanged between them.

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

Richard O'Dwyer (RD)* is demonstrative of a number of principles brought out in course of this week's presentations on the Lesotho draft Computer Crime and Cybercrime bill.

- RD – British citizen born 1988 (24years), university student – 2007 created TVShacks.net search engine provided on domain name in UK that also had links to sites having movies, music and other copyrighted material.

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- May 2011 - US Justice Department extradition request to UK based on US 2003 UK Extradition Act*, on US District Court order for charges against him for conspiracy to commit copyright infringement and criminal copyright infringement – on account of links provided on website to media on other sites, attracting maximum of five years imprisonment
- - Earlier, May 2010 TVShack.net domain name was seized by US Customs and Immigration under court order (TVshack.net domain name computer equipment together with five other sites committing copy right infringement")

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- TVShack.net changed name to TVShack.cc within four hours of seizure
- TV Shack.cc seized in Nov. 2010 with eighty two other domains
- (seizure described by Motion Picture Association of America as" largest takedown of illegal movie and television websites in a single action by the Federal govt.)
- RD lawyers claimed US lacked jurisdiction because TVShack.net not hosted on American servers.
- 13 January 2012 - UK magistrate's court ruled RD could be extradited to US, and extradition approved by UK Home Secretary.

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

- RD appealed against decision.
- November 2012 UK/US reached mutual agreement to avoid extradition under which entailed RD voluntarily going to US, pay a small compensation for the infringement and giving undertaking not to infringe copyright laws again.

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

RD demonstrated principles:

- International co-operation and mutual legal assistance agreements (US /UK 2003 extradition treaty, UK Minister's extradition approval following Magistrate's court decision),
- jurisdiction (impact of illegal act/offence in requesting country ie based on the first principle of extra-territorial jurisdiction),
- copy-right infringement, liability of hyperlink provider (links to infringing material),
- criminal law principles relating to conspiracy to commit an offence (aiding and abetting),
- procedural tools(seizure, court orders obtained, observance of safeguards of fundamental rights)
- Penalties (compensation/fines paid

4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

Restitution - issues - means available to pay, ability of courts to quantify financial loss – civil court domain

Geoffrey Osowski and Wilson Tang, for example, who were former accountants of Cisco Systems Inc., and who had illegally issued more than US$8million worth of stock to themselves through use of company's computers - sentences of 34 months' imprisonment were made in addition to restitution orders amounting to US$7.9 million (see: http://www.usdoj.gov/criminal/cybercrime/cccases.html).

State V Peterson (child pornorgraphy) –sentenced to four and half years with lifetime supervision on release in connection with child pornography found on his computer

Also **US V Cover**
http://www.cybercrimelawyerblog.com/cyber_crime/



4.TRANSPOSITION OF MODEL - LAW GUIDING PRINCIPLES

Cox v Riley - interference with computer data - changes to programs or data could be considered to be criminal damage to physical medium on which that data was stored.

Se also **R v Whitely -** in order for criminal damage to be made out, changes would have to result in "an impairment of value or usefulness of disc to owner". Changes of a lesser nature would not suffice: "[if] the hacker's actions do not go beyond, for example, mere tinkering with an otherwise 'empty' disc, no damage would be established".

R v Gold – comp. related forgery – used false user names to access secured British Telecom Prestel computer network by using customer identification numbers and passwords of authorised users. They used this access to obtain information to which they were not entitled and to make changes to stored data, to expose security flaws in the Prestel system.

Irish Criminal Law Journal - Volume 15, No.1, 2005; www.acadaemia.edu

Thank you for your attention!

jmctembo@hotmail.com

INTERNATIONAL TELECOMMUNICATION UINON