Common Market for Eastern and Southern Africa

International Telecommunication Union

ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia, 25-28 August 2008[1]

Document RFL/2008/WG02-E

28 August 2008

Original: English

Working Group 2: Legal Foundation and Enforcement

Recommendations from the Ad Hoc Forum Working Group on Legal Foundation and Enforcement

1.0 Legal Foundation and Enforcement Introduction

As modern society's dependence on information and communication technologies (ICTs) grows, so too have cyber crimes. The need to develop and enforce legislation on cyber crimes is, therefore, underscored.

The ad hoc forum working group makes general proposals for inclusion in the COMESA model law on cyber security. These proposals address the following four areas:

- Substantive law criminalizing certain conduct
- Procedural law
- International cooperation
- The treatment of evidence

2.0 Substantive Law

The ad hoc forum working group proposes criminalization of the under listed acts. It is proposed that the working group give a clear description of these crimes:

1. Illegal access to a computer
2. Illegal interception of electronic communication
3. Interference with computer data
4. Interference with a computer system [it is proposed that the working group considers providing for greater penalties for interference with government systems]
5. Misuse of devices [note to have a clear definition of misuse so that legal use is not criminalized]
6. Computer related forgery
7. Computer related fraud
8. Creation, possession or distribution of child pornography [it is proposed that the working group considers penalizing pornography in general, especially for member states already penalizing physical creation, possession and distribution of such material]
9. Identity theft
10. Phishing [the description of the offence should be wide enough to cater for commission of a similar offence through the use of other technology e.g. smishing]
11. Data espionage
12. Spamming
13. Harassment

[1] ITU Regional Cybersecurity Forum website: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/

14. Sending of hate speech and commission of other religious offences [Members States should be allowed to exercise discretion in adopting this]

15. Attempt and aiding or abetting of the above offenses [penalties for these should be lighter than those for the actual offences]

16. Corporate liability for the above offences [the working group should determine whether to impose civil or criminal liability]

17. Data protection [to cater for countries that do not have a data protection legislation in place]

3.0 Provisions on procedure

There should be enabling provisions on:

1. Expedited preservation of stored computer data
2. Expedited preservation and partial disclosure of traffic data
3. Investigative authority to compel computer network providers to disclose content and non content information stored on the network
4. Search and seizure of stored computer data by law enforcement authorities
5. Real time collection of traffic data relating to electronic communications
6. Interception of the content of electronic communications
7. Retention of data

4.0 International co-operation

Insert provisions for international co-operation in accordance with relevant international instruments on international co-operation in criminal matters.

New standards should be adopted for mutual assistance, along the 24/7 network point of contact arrangements.

5.0 Evidence

The model law makes provisions addressing admissibility of electronic evidence in court.

****