

OCTOPUS INTERFACE CONFERENCE COOPERATION AGAINST CYBERCRIME

Sri Lankan Perspective

Jayantha Fernando *Attorney - at - Law*

LLM – IT & Comm Law (Lond)

Director / Legal Advisor – ICTA

jfdo@sltnet.lk

Sri Lanka

- v A Country in the Indian Ocean
- v Population - approx. 20 Million
- v ICT & BPO is a major growth Sector
(approx USD 200 million from software exports)
- v Legal enablers (i.e Intellectual Property Act, Electronic Transactions Act in place)

Computer Crimes

- The Problem
 - Difficult to measure magnitude .. Losses estimated to be in Millions
 - Lack of Reporting - Business / Govt concerns regarding integrity and confidentiality of investigation process
 - Growing economic threats (connected with terrorism)

Computer Crimes Legislation - Process

- Process commenced in 1995
- Law Commission & Justice Ministry Review (2000 - 2005)
- Bill Presented to Parliament - 23rd Aug 05
- Parliamentary Review (2005-07)
- Legislation Enacted on 8th May 2007
- Salient Features
 - Introduces several new features ranging from Unauthorised use, Introduction of Viruses and hacking offences

Defining Computer Crimes

- Three Broad areas of Cyber Crimes
 - Computer Related crimes - Computers used as a tool for criminal activity such as theft, fraud etc
 - Content related Cyber Crime - Computers with internet used to distribute illegal data. Eg;- Internet based pornography, Criminal copyright infringement
 - Hacking - affects integrity, availability and confidentiality of a computer system or network (also includes Viruses, worms etc)

Salient Features of the Sri Lankan Act (First Class of offences)

- The first component of offences in the Computer Crimes Act criminalises attempts at unauthorised access to a
(a) computer; or
- (b) any information held in any Computer
- (Section 3 and 4)

Salient Features of Sri Lankan Act

- For (a) Mere turning on of a computer is sufficient
- For (b), the following is required
 - There should be an intention to secure any programme or data held in any Computer
 - The access intended to be secured, should be unauthorised
 - it is not necessary to have access directed at any particular programme, date or computer.

Salient Features of the Sri Lankan Act (Second Category)

- Section 5
- Any person who intentionally or without lawful authority carries out a function which has the effect of modification or damage or potential damage to any computer or computer system or computer programme shall be guilty of an offence.

Salient Features of Sri Lankan Act (Second Category)

- Modification or damage or potential damage
Clarified by illustrations
 - impairing the operation of any computer, or the reliability of any data or information held in any computer
 - destroying, deleting or corrupting or adding, moving or altering any information held in any computer

Salient Features Sri Lankan Act (Second Category)

- Modification or damage or potential damage
Clarified by illustrations
 - makes use of a computer service involving computer time and data processing for the storage or retrieval of data
 - introduces a computer program which will have the effect of malfunctioning of a computer or falsifies the data or any information held in any computer or computer system

Other Offences under Computer Crimes Act

- Offences against National Security - Section 6
- Obtaining information from a computer or a storage medium without authority
 - - Section 7
- Illegal interception of Data - Section 8

Other Relevant Legislation

- Payment Devices Frauds Act No. 30 of 2006
An Act to prevent the possession and use of unauthorised payment devices (deals with credit card frauds)
- Penal Code (Amendment) Act No. 16 of 2006
Introduces an offence - Requiring all persons providing Computer service to ensure that the service is not used for offences related to sexual abuse of children

Unique Enforcement measures

- Enforcement measure
 - Unique features for Investigation and prosecution -
Interception of Communications
 - Obligations on Telecom providers and ISP s providers
(monitor Attributes of Communications)
 - Provision to designate experts to assist
Investigators
 - Broad Jurisdictional powers on High Court

Challenges

- Enforcement Measures
 - Inadequate - Institutional & Skills Development required
 - Digital Forensic Lab the Police (CID) -Facilitation by Government
 - Evidence Provisions - uncertain
 - Cross - border nature of cyber crimes - Requires foreign bilateral co-operation between enforcement officials

The background of the image is a vibrant, abstract pattern of blue and purple, resembling a nebula or a galaxy. The colors are soft and blended, with some brighter spots and darker areas, creating a sense of depth and movement. The overall effect is ethereal and cosmic.

Thank You