CYBERCRIME LEGISLATION - SRI LANKAN UPDATE

Jayantha Fernando[1]

The networked or inter-connected environment has created opportunities for Governments, businesses and users and has resulted in the increased use of Information and Communication Technology (ICT) based devices. In Sri Lanka the government embarked on an ICT Development initiative known as *e-Sri Lanka Development Project*[2], to promote the use of ICT in all sectors of the economy. Over the past several years the Government has actively promoted Sri Lanka as an "outsourcing" destination, with the rapid expansion and opportunities for the BPO/ ITES sector. As a result for these development measures, the ICT literacy alone in the country has jumped from 9% to 19% in four years. But this increased use has resulted in challenges manifested in the form of abuses and misuses.

In 2008 alone Sri Lanka CERT (Computer Emergency Response Team) responded to 49 incidents compared to the 6 reported in 2007.

Computer Crimes Act - Background

Sri Lanka responded to this challenge by enacting the Computer Crimes Bill (LD-O 72/2000) on 8th of May 2007. This Bill, which was certified by the Speaker of Parliament on 9th July 2007, as **Computer Crimes Act No. 24 of 2007,** was brought into operation with effect from 15th July 2008. This legislation is the result of contributions from CINTEC Committee on Law & Computers[3] (1995-2000), Computer Crimes Sub-Committee of the Law Commission and the Ministry of Justice (2001-2004) and ICT Agency of Sri Lanka –ICTA (2004 – 2007).

During the early stages of the Drafting process the provisions contained in the Penal Code of Ceylon - 1885 (with emphasis on Offences against property) were examined in order to determine whether the Penal Code could be modified to adapt to deal with Computer Crime related offences. However, it was felt that definitions of offences such as THEFT, Cheating and Criminal Misappropriation (and the definition of property) in the Penal Code of Ceylon were limited in scope and basically reflect the conditions that prevailed in the previous century. It was found that those definitions were formulated on the assumption that an identifiable human offender and victim are in existence and envisaged the commission of an act in a specified manner by the offender against the victim. As such it was decided to pursue a *sui generis* approach to legislation.

---

[1] LLM – IT & Communications Law (Lond.), *Attorney at Law*
Program Director & Legal Advisor, ICT Agency of Sri Lanka (ICTA) – JFDO@ICTA.LK or JFDO@sltnet.lk

[2] See www.icta.lk for details

[3] Council for Information Technology (CINTEC) replaced by ICT Agency of Sri Lanka the apex ICT Agency of Government of Sri Lanka (Information and Communication Technology Act No. 27 of 2003)

During the formulation of the legislation in Sri Lanka it was agreed that the term "Computer Crime" is a generic term used to identify all crimes or frauds that are connected with or related to computers and information technology. As such the term "computer crime" is not defined in the Act and legislators felt that it was synonymous with "Cyber Crime", although the latter tends to be focussed towards criminal activity resulting from the use of the internet.

Computer Crimes Act – Key provisions

In terms of scope and applicability Section 2 stipulates that the Act would apply where:-

(a) A person commits an offence under the Act while being present in Sri Lanka or outside Sri lanka
(b) The Computer, computer system or information affected, by the act which constitutes an offence under this Act, was at the material time in Sri Lanka or outside Sri Lanka
(c) The facility or service, including computer storage or information processing service, used in the commission of an offence under this Act, was situated in Sri Lanka
(d) The loss or damage is caused within or outside Sri Lanka by the commission of an offence under the Act, to the state or to a person resident in Sri Lanka or outside Sri lanka.

In terms of substantive offences the Sri Lankan Computer Crime Act covers a broad range of offences, which could broadly fall into the following two categories of offences. They are:-

(1) Computer Related crimes (where computers are used as a tool for criminal activity such as theft, fraud etc)
(2) Hacking offences – which affects integrity, availability and confidentiality of a computer system or network (also includes the introduction of Viruses, worms etc)

The following are some of the key substantive offences under the Computer Crimes Act:-

- **Section 3** of the Act criminalises the securing of unauthorised access to a computer, or any information held in any computer, with knowledge that the offender had no lawful authority to secure such access.
- **Section 4** is an enhanced version of Section 3 and criminalises unauthorised access with the intention of committing another offence under the Computer Crimes Act or any other law.
- **Section 5** criminalises activity where any person causes a computer to perform a function which results in an unauthorised modification and damage to a computer, computer system or computer program[4].

[4] Illustrations to Section 5 of the Sri Lankan Computer Crimes Act identifies broad categories of offences which constitute modification and damage to a Computer, computer system or computer program.

- **Section 6** deals with economic and national security related offences committed by means of a computer.
- **Section 7** criminalises buying, receiving, uploading and down loading information unlawfully obtained from a computer or storage medium.
- **Section 8** deals with illegal interception of subscriber information or traffic data or any communication to, from or within a computer
- **Section 9** criminalises activity such as producing, selling, importing and exporting and distributing Computer or Computer Program or computer passwords or access codes, which could be used for the purpose of committing offences under the Computer Crimes Act.
- **Section 10** deals with unauthorised disclosure of information enabling access to a service.

A closer review of the broad range of offences under the Sri Lankan Computer Crimes Act, outlined above, would demonstrate the level of compatibility it has with the Council of Europe Convention on Cyber Crime.

With respect to Content related Cyber Crime (where Computers together with internet resources are used for copyright infringement), there is a provision in the Act which enhances the scope of Intellectual Property provisions contained in the Intellectual Property Act 36 of 2003. Further, an Amendment made to the Penal Code in 2006[5] introduced an offence requiring all persons providing a Computer service like a cyber café etc, to ensure that such a service would not be used for offences relating to sexual abuse of a child. This offence was introduced prior to the Computer crimes Act.

In addition, Sri Lanka introduced the Payment Devices Frauds Act No. 30 of 2006 to specifically deal with possession and use of unauthorized payment devices. This legislation is couched in the widest possible terms to criminalise behavior where computers or the internet is used to commit offences related to payment devices.

Investigation and Enforcement

Any criminal investigation interferes with the rights of others, whether the person is the subject of an investigation or a related third party. In a democratic society any such interference must be justifiable and proportionate to the needs of society sought to be protected. However, the growth of network-based crime has raised difficult issues in respect of the appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of users of such networks.

In addition, there are the rights and interests of the network providers, the intermediaries that build and, or, operate the networks and services, through which data is communicated.

These challenges require parties to an enforcement process, namely investigators, prosecutors and judges to work in a coordinated manner. This "necessary co-ordination"

[5] New Sections 286B and 286C introduced through Penal Code (Amendment) Act No. 16 of 2006

is also challenging for Governments because of the lack of expertise to often deal with Cyber Crime. As such Governments have been compelled to rely on expertise outside governments, such as Academia and Business.

This is the experience in Sri Lanka as well. The Sri Lankan Computer Crimes Act responded to these enforcement challenges by providing for an "independent" group of experts to assist Law enforcement agencies in the investigation of Cyber Crime[6].

These designated experts are fully empowered and given protection under the legislation[7]. The introduction of the concept of an "experts" in the Act is to ensure that accessing of a computer is done only by skilled resources, capable of performing an efficient detection while at the same time ensuring that the computer hardware and software is not damaged.

Safeguards have also been built in to protect the businesses and Computer systems that are being investigated[8]. This to provide the "comfort" measures for businesses and individuals to Report Cyber Crime.

Challenges

However, the challenge is to get the required regulations designating the said experts. A common concern expressed by experts is whether they would be called upon to give evidence, thus exposing them to cross examination in a court of law. As such many capable experts have shown reluctance to be designated under the Act. The procedural laws have not been amended to facilitate the submission of affidavit evidence on matters concerning sensitive investigations.

The second challenge is to ensure the admissibility of electronic or computer based evidence. Although the existing evidence laws permit the admissibility of Computer generated records[9], admissibility is subject to several stringent criteria[10].

It is left to judicial interpretation to determine to what extent the more flexible rules governing Evidence contained in the Electronic Transactions Act 19 of 2006 would be applicable to proceedings under the Computer Crimes Act. The Computer Crimes Act is silent on the matter. If any Computer Crime committed arises out of an electronic based transaction, the admissibility provisions in the Electronic Transactions Act could be invoked in connection with the transaction. But this is an area requiring review and consideration.

---

[6] Section 17 of the Computer Crimes Act No. 24 of 2007
[7] Section 18 and 28
[8] See for instance Section 20 (ordinary course of legitimate business not to be hampered in the course of investigations); and Section 24 (ensuring confidentiality of information obtained in the course of an investigation)
[9] Evidence (Special Provisions) Act 14 of 1995
[10] Eg – Certificate that the computer was working properly etc

Institutional Measures – Sri Lanka CERT

Many Governments are increasingly relying on broad range of resources outside the traditional Governmental law enforcement expertise to address Cyber threats and forensic issues. As such new institutional models may have to be created. The Sri Lankan experience is an interesting example.

In mid 2006 Sri Lanka CERT[11](Computer Emergency Response Team) was created to address cyber security incidents. This is a government owned company (a subsidiary of ICT Agency of Sri Lanka- ICTA)[12], established with support from World Bank, and runs on a private sector driven model with highly skilled incident handlers. The Board consists of a range of key stake holders such as enforcement authorities, bankers, Private sector and academia.

SLCERT was admitted as a member of APCERT and became the first south asian CERT to be admitted as a member of FIRST[13] in 2008. In just a few years SLCERT has responded effectively to the Cyber Crime forensic issues. Due to the requests from law enforcement agencies SLCERT started offering digital forensics as a service for law enforcement agencies since the third quarter of 2008. SLCERT also carries out forensic investigations for other government establishments in Sri Lanka.

Conclusions

Cyber crime by nature is multi-jurisdictional and not confined to one country and such Governments cannot enforce it in isolation. The transnational nature of Cyber Crime activities, as well as concerns to avoid the proliferation of jurisdictional havens, has driven harmonisation initiatives within a number of international fora, including the Council of Europe, the British Commonwealth and the European Union.

Sri Lanka is fully supportive of the approach adopted by the Council of Europe and is positively looking at options to accede to the convention. Preliminary steps have already been initiated by the Government in this connection and it is expected that official dialog would commenced with the Council of Europe for this purpose, during 2009.

[11] www.slcert.gov.lk
[12] www.icta.lk
[13] www.FIRST.org