Cybercrime Legislation in Sri Lanka

16th November 2016

Jayantha Fernando

Attorney-at-Law, LLM – Telecom & IT Law (Lond.)

Director / Legal Advisor, ICTA

&

Chairman, .LK Domain Name Registry

Nature of Cyber threats and Recent challenges in Sri Lanka

“Cybercrime”

“Multi-National Nature, Tracing e-Evidence – Where was the offence committed”

News

Sri Lankan teller helps bust world’s biggest bank fraud

By Feizal Samath
View(s): 5803

- **US$ 1 billion scam involves China, Bangladesh, Lanka, the Philippines and US Fed**
- **CB launches massive money laundering probe on dubious NGO here**

Sri Lankan authorities have launched a massive probe into a dubious NGO here that tried to sneak in millions of US dollars stolen by Chinese hackers from the Bangladesh Central Bank, government officials here said, adding that this is part of a global crackdown on a money laundering scam.

They said the scam, which hit media headlines across the world, was thwarted two weeks ago by an alert teller at the Colombo branch of a foreign bank when an inward remittance of about $25 million appeared to be suspicious.

The officials, who declined to be named, said a major probe was underway by the CB to ascertain the background of the intended receiver of the funds. “We found that the recipient NGO Shalika Foundation had been registered here by some outside parties who have now gone back. We are also probing whether there were any other funds that came from the source (hack-in) and had slipped through the radar here.”

Several NGO heads and activists said they had never heard of the Shalika Foundation. “Never heard of it,” said Dr. Vinya Ariyaratne from Sarvodaya. News of the theft, however, broke only this week, several days after the Sri Lankan teller’s query tipped off the US Federal Reserve, Bangladeshi authorities and the local Central Bank (CB),

exposing a near US$1 billion theft through hacking, the biggest ever hack-in of bank funds in world history. CB Governor Arjuna Mahendran yesterday confirmed to the Sunday Times that “it was the Sri Lankan teller that alerted the US, Bangladesh and us (and the world) over a suspicious transaction”.

Cybercrime : Global Nature

- Multi jurisdictional in most cases
  - Actions of criminals can reach computers/ devices and victims in many other countries
  - Evidence in multiple countries (“Evidence in the Cloud”)
  - Where was the offence committed and which Country has jurisdiction
  - Need for global Legislative standard, tool for Police & Judicial Collaboration

Computer Crime Act No. 24 of 2007

Application of the Act (Jurisdiction)

- Committing an offence while being present in Sri Lanka
- Computer, Computer system affected by the offence is in Sri Lanka
- Facility or service (including storage or data or information processing service) used for the offence was in Sri Lanka
- Loss or damage is caused in or outside Sri Lanka

Computer Crimes Act- Key Features

- **Section 3** - 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. *(Article 2)*
- **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. *(Article 2)*
- **Section 5** criminalises activities which results in *unauthorised modification and damage* to a computer, computer system or computer prog *(Art.4 & 5)*
- **What constitutes "Modification or damage" clarified**
  - impairing the operation of any computer, or the reliability of any data or information held therein
  - destroying, deleting or corrupting or adding, moving or altering any information held in any computer
  - unauthorized use of Computer services etc
  - Introduction of a program resulting in malfunction (Viruses, worms etc)

Computer Crimes Act – Key Features

- Section 6 - Causing a computer to perform a function which will result in harm to National Economy, National Security and Public Order, an offence.

- Section 7 - Obtaining information from a computer or a storage medium without authority – *(Article 10)*
  - Including buying, selling, uploading and downloading, copies or acquires the substance or meaning of such information

- Sec 8 - Illegal interception of Data – *(Article 3)*

- Sec 9 - Use of Illegal devices – *(Article 6)*
- Section 10 - Unauthorised disclosure of Information

Other Relevant Legislation

- Penal Code (Amendment) No. 22 of 1995
  - Section 286A – Introduced offences to ensure Child Protection . Can be extended to online child abuse images (Meets minimums requirements under Article 9 of the Budapest Cybercrime Convention)
- 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 sexual abuse of children.
- 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)

Computer Crimes Procedures
Safeguards for Businesses

- Provision to designate "***experts***" to assist Investigators with defined powers (Section 17 – 22)
- Experts – "Public Officers" qualified in Electronic engineering or Information Technology – Sec 17 (1)
- Broad powers for Experts – Section 17(4)
- Normal use of Computers not to be hampered (Sec 20)
- Competency of Police Officers to be certified by IGP (Sec 21)
- Ensure Strict confidentiality by Police & Experts in connection with all information collected during an investigation (Sec 24)
- Powers of search and seizure with warrant – Section 18
  - Obtain information including subscriber information and traffic data
  - Interception of Communication at any stage of communication
- Expert or Police Officer can issue notice for preservation of Information for 7days - extension of time with Magistrate's warrant (Sec 19)
- Investigations ⇨ Multi jurisdictional ⇨ Electronic Evidence

Budapest Convention: Solution to Problem

Scope and Mandate covering 3 elements

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Interception of computer data

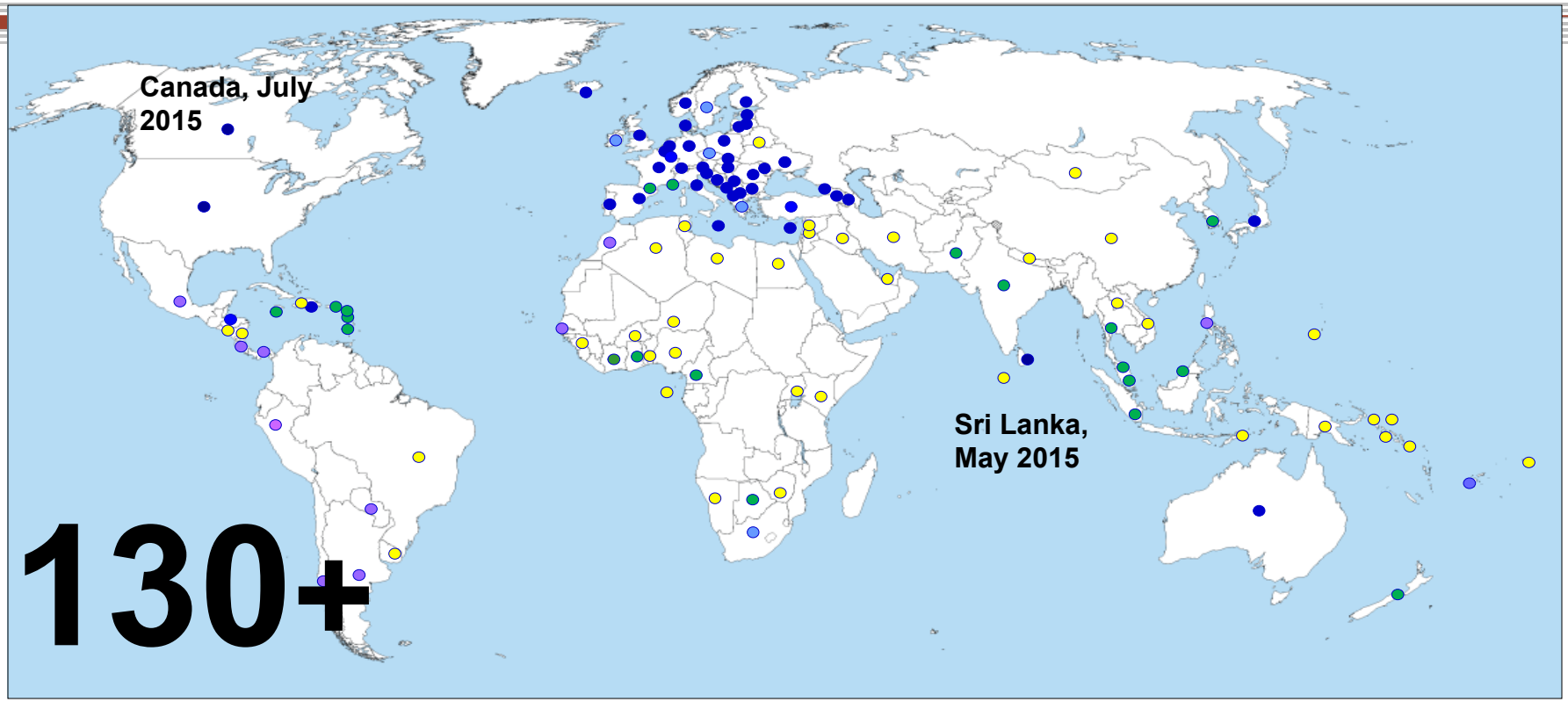
+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Budapest Convention – Influence globally…



Ratified/acceded: 49

Signed: 6

Invited to accede: 12

= 67

Other States with laws/draft laws largely in line with Budapest Convention = 20

States drawing on Budapest Convention for legislation = 45+

Source – Alexander Seger (Council of Europe) ww.coe.int/cybercrime

Sri Lanka ----
Road to Budapest Convention

- Sri Lanka Invited to accede Budapest Cybercrime Convention - 23rd February 2015
- Acceded to the Cybercrime Convention (29th May 2015)
- 1st Country in South Asia & 2nd in Asia after Japan
- Fastest ever Accession in Council of Europe history
- Convention Effective from 1st September 2015
- Preparations towards Accession carried out over several years under "***e-Sri Lanka Development Initiative***", eg:-
  - Regulatory reform through adoption of relevant legislation
  - Capacity building measures – Law Enforcement and Judicial Training

Gathering Electronic "Evidence in the Cloud"
Domestic Production Orders – International effect

- Article 18 (1) – Budapest Cybercrime Convention

  Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

  (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

  (b) a **service provider** offering its services in the territory of the Party to submit "subscriber information" relating to such services in that service provider's possession or control.

- **Court Orders for Subscriber Data etc under Section 18 of CCA**
  - Broad Definition of **"Service Provider"** under Computer Crimes Act
  - Supervision by Courts

- **Data Preservation Order Under Section 18 – Can be served on Facebook, Microsoft, Google, Apple etc**

Budapest Convention Impact (Art 15)
Safeguards in Sri Lanka

- Article 15 – Conditions & Safeguards
  - Under the Computer Crimes Act of 2007, intrusive investigative measures, such as search and seizure of computers or the "***interception of a communication***", are subject to a warrant by a magistrate (see Section 18).
  - Similar safeguards in Section 19 (Preservation Requests)
  - Sri Lanka is Party to a number of international human rights treaties such as the International Covenant on Economic, Social and Cultural Rights, the International Covenant on Civil and Political Rights, the Convention on the Rights of the Child, the Convention against Torture and Cruel, Inhuman or Degrading Treatment of Punishment and others.
- **CCA is used for Investigation of Offences – After the fact**
  - **CCA is not a National Security related legislation – it cannot be used for Warrantless Wiretapping**

Recent Cybercrime Trends
Sri Lanka

Type of Incident	Year 2013
Phishing	8
Abuse/Privacy	8
Scams	18
Malware	2
Defacements	16
Hate/Threat Mail	8
Unauthorized Access/Attempted	11
Intellectual property violation	3
DoS/DDoS	1
Fake Accounts	1200
Total	**1275**

Type of Incident	Year 2015
Phishing	14
Abuse/Hate/Privacy violation (via mail)	21
Scams	18
Financial Frauds	12
Malicious Software issues	10
Web site Compromise	20
Compromised Email	16
Intellectual property violation	3
DoS/DDoS	3
Social Media related incidents	2850
Total	**2967**

Addressing Challenges in Sri Lanka

Institutional, Policy and Legal Measures

- Established Sri Lanka CERT – www.slcert.gov.lk
  - Supporting Public private partnerships to protect critical information infrastructure
  - SLCERT working with industry to create Sector specific CSIRTS (eg: - Bank CSIRT with Central Bank & Banking Sector established July 2014)
- Establishing "Digital Forensic Lab" for Computer Crimes Unit of Police (CID)
- Awareness and Skills Development
  - For Law enforcement, Stake holders (banking etc) and even public
- **Admissibility of Electronic Evidence (Dual Regime)**

Electronic Evidence
In Criminal Matters

- Evidence (Special Provisions) Act No. 14 of 1995
  - Response to *Benwall vs Rep of Sri Lanka [1978-89] Sri LR*
  - Provides for
    - (a)the admissibility of any contemporaneous recording made by electronic means and
    - (b)facts and information contained in a statement produced by a computer
  - Admissibility under the 1995 Act is subject to several conditions – that the computer producing the statement was operating properly, Information supplied to the Computer was accurate etc
  - Casus omisus (Section 3)
  - Presumptions (Section 9)
  - Indian Fisherman's Cases and Hon. Ambepitiya Cases
- **Act No. 14 of 1995 vs Act 19 of 2006**

Conclusions

- Sri Lanka - first in South Asia to join this Convention –
  - 1st September 2015
- Framework supports cross border investigation and help Law Enforcement & Judicial cooperation at International level
  - access to Computer systems and networks in other countries. The convention would greatly enhance the gathering of electronic evidence, the investigation of cyber laundering and other serious crime.
- Access to Judicial Precedents from USA, Europe etc
  - Guidance Notes / Interpretations from Council of Europe
- Creates Greater Confidence to Report Cybercrime Cases

- Sri Lanka to become a hub for Cybercrime enforcement
  - Centre of Excellence

- More capacity building needed

Thank You !

JFDO@icta.lk & Jayantha.fdo@gmail.com

www.icta.lk