



Sri Lanka
smart people smart island

ICTA
ideas actioned 

Regional Conference on Cybercrime 2017
Philippines Dept of Justice & Council of Europe
(Cebu, Philippines)

27-29 June 2017

Jayantha Fernando

Director/ Legal Advisor, ICTA
Chairman .LK Domain Registry
Bureau Member, T-CY (Council of Europe)

Sri Lankan Digital Landscape

Transition to Digital Economy



- Internet has benefitted Sri Lanka's growth potential
- First in South Asia to Liberalise Telecom Sector and introduce competition (Telecommunications Act No. 25 of 1991) - 4G Mobile Providers, 19 ISPs, 5 gateways --- On-going Consolidation
- No Common - Point of Inter-Connection
- Mobile Usage – Over 107% (*More mobiles and toothbrushes*) !!!
 - 1st in South Asia to introduce Mobile Payment Regime
- Internet Contributor to Economic growth – 30% per annum growth in BPM workforce & 5th Largest Revenue Earner
- Sri Lanka ranked No 1 in South Asia in Networked Readiness Index (NRI)

UN e-Gov Index (Sri Lanka Status)



- Placed **71** among 192 countries
- Leapfrogged **41 places** since 2012
- Ranked **6th** in ASEAN following S. Korea, Singapore, Japan, Malaysia & China
- Ranked **7th** globally in 'High On-line Service Performance, relative to income'
- Ranked **37th** in Online Service Sub index
- Ranked **38th** in e-Participation.

Cyber Threats & Challenges



The Telegraph

Search - enhanced by OpenText

Thursday 30 July 2015

[Home](#) [Video](#) [News](#) [World](#) [Sport](#) [Finance](#) [Comment](#) [Culture](#) [Travel](#) [Life](#) [Women](#) [Fashion](#) [Luxury](#) [Tech](#) [Cars](#) [Film](#)
[Politics](#) [Investigations](#) [Obits](#) [Education](#) [Science](#) [Earth](#) [Weather](#) [Health](#) [Royal](#) [Celebrity](#) [Defence](#) [Scotland](#)

[HOME](#) » [NEWS](#) » [UK NEWS](#) » [CRIME](#)

Cybercrime could become more lucrative than drugs, police chief warns

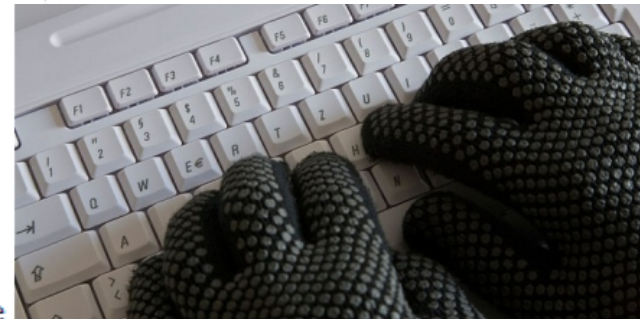
Adrian Leppard, the Commissioner of the City of London Police, says at least a quarter of organised criminals in Britain are now involved in online fraud

International gangsters are increasingly abandoning drug dealing and other high risk rackets in favour of cybercrime, putting everyone who uses the Internet at risk, one of the country's most senior police officers has warned.

Up to a quarter of all organised criminals in Britain are now thought to be involved in some form of financial crime, netting them tens of billions of pounds in profit every year.

But with the majority of online fraud being committed by overseas gangs and victims often unwilling to report offences, law enforcement agencies are finding it difficult to even assess the scale of the problem.

Adrian Leppard, the Commissioner of the City of London Police, which takes a lead in fighting fraud and cybercrime, said while traditional crimes were continuing to fall, financial offences were soaring.



A new sophisticated malware buy Regin has been detected by Symantec Photo: Alamy



Recent Cyber Incidents....



- **Yahoo!** admitted largest data breaches of all time. The company was hacked by a state-sponsored actor in 2014, with more than half a billion usernames and passwords of its customers stolen.
- **US Agencies** blaming the Russian government for leaking emails stolen from DNC.
- **Cybercrime – No. 1 Economic Crime in Australia** - Between July 2015 and June 2016, CERT Australia – responded to 14,804 cyber security incidents.
- Data breach of major Indian Banks – an estimated 3.2 million debit cards compromised

The image shows a screenshot of a BBC News article. The URL is /news/uk-38964996. The page features the BBC logo, navigation links for News, Sport, Weather, Shop, Earth, Travel, and More. The main navigation bar includes Home, Video, World, Asia, UK, Business, Tech, Science, Magazine, and Entertainment. The sub-navigation bar lists UK, England, N. Ireland, Scotland, Wales, and Politics. The article title is "Cybersecurity: Queen opens centre to protect against attacks" by Gordon Corera, Security correspondent, BBC News. The article is dated 14 February 2017. A "Share" button is visible. The main image shows Queen Elizabeth II in a blue coat and hat, standing in a modern, brightly lit room with large digital displays and a laptop on a table. A man in a suit is pointing at one of the displays. The image is credited to PA.



- Multi jurisdictional in Nature

- 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

“Cybercrime Challenge for Sri Lanka”

“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”.

ICT Related Legislation Development in Sri Lanka



- Intellectual Property Act No. 36 of 2003
 - Protection for Software and other intellectual ICT outputs
- Amendment to Monetary Law Act No. 32 of 2002
 - Scriptless Securities Trading – Public Debt Settlement System
- Payment and Settlement Systems Act No. 28 of 2005
- Electronic Transactions Act No. 19 of 2006
 - UN Electronic Communications Convention (UN ECC)
 - Ratified July 2015 and ETA Amendment (2017)
- Payment Devices Frauds Act No. 30 of 2006
- Computer Crimes Act No. 24 of 2007
 - State Party to Budapest Cybercrime Convention (2015)



Road to Budapest Convention

- Sri Lanka Invited to accede to Budapest Cybercrime Convention - 23rd February 2015
- Acceded to the Cybercrime Convention (29th May 2015)
- Applicable on Sri Lanka - w.e.f - 1st September 2015
- **1st Country in South Asia** & 2nd in Asia after Japan
- Fastest ever Accession in Council of Europe history
 - First ever Non UN Treaty for Sri Lanka
- Preparations towards Accession carried out over several years under "**e-Sri Lanka Development Initiative**", eg:-
 - Regulatory reform through "International Legislative Standards"
 - Capacity building measures - Law Enforcement & Judicial Training

Sri Lanka – Legal & Regulatory Reform (Compliance with Budapest Convention)



- Primary Legislation – Computer Crimes Act No. 24 of 2007
 - Substantive Cybercrime offences - Sections 3 to 10 of the Act Consistent with the Budapest Convention (BC)
 - Procedural Law, including Article 15 Safeguards comply with BC
 - Provides for Mutual Legal Assistance Measures based on BC
- Other Relevant Legislation
 - PAYMENT DEVICES FRAUDS ACT, No. 30 OF 200
 - Intellectual Property Act, No. 36 Of 2003
 - Adopting recommendations of Financial Action Task Force (FATF)
 - Penal Code Amendment No. 22 of 1995 and No. 16 of 2006 – Criminalises Online Child Pornography
- New Obscene Publication Bill (New offences on child abuse Images & Grooming etc) planned for 2017

Benefit of Budapest Convention

Access to Evidence in the Cloud



- **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.

- Scope of Article 18(1)(b) implemented through Section 18 of Sri Lankan Law
- Broad Definition of "Service Provider" under Computer Crimes Act (2007)
 - Supervision by Courts
- Preservation Order Under Section 18 – Can be served on Facebook, Microsoft, Google, Apple etc
- **More effective than going through traditional MLA**
 - Guidance Note and Draft Protocol

Impact of Budapest Convention

As a tool for Criminal Justice cooperation



- **Assessment on the Use of the Convention by State Parties – Required to act with responsibility**
- **Transborder access to data: clarification of Article 32b and its limits → Guidance Note (adopted December 2014)**
- **Assessment of effectiveness of mutual legal assistance provisions (24 recommendations adopted in December 2014)**
- **Effectiveness of 24/ 7 contact points between Member Countries**
- **Application of Article 18 – Production Order**
 - **Participation in preparation of Guidance Notes**
 - **Sri Lanka involved in Negotiation of Protocol to the Convention**



- Sri Lanka CERT – www.slcert.gov.lk
 - National CERT established under e-Sri Lanka Development Initiative
 - Launched Sector specific CSIRTS (eg:- Bank CSIRT with Central Bank & Banking Sector) - **FinCERT**
 - A Public private partnerships model to protect critical information infrastructure
- “Digital Forensic Lab” for Cyber Crimes Unit of Police (CID)
- Capacity Building Measures
 - For Police, Judicial and Prosecution authorities under e-Sri Lanka Initiative
 - Public Awareness Programs & Cyber Security Week (CSW)
 - GLACY Project of EU/ Council of Europe

The Budapest Convention Framework



1 Common standards: Budapest Convention on Cybercrime and relates standards





2015

Assessing the Threat of Cybercrime Conference for Decision Makers, 26-27 March (Colombo, Sri Lanka)

- Workshops on cybercrime policies and strategies and criminal justice statistics and reporting systems

110 international participants

First Responders Course: Training of Trainers, 4-8 November

- Electronic Evidence sources, search and seizure; Practical exercises and training skills

15 officers from the Sri Lanka Police Service

2016

Scoping mission and workshop on cybercrime reporting systems and interagency cooperation, 12-14 January

- recommendations for the reform of existing reporting systems

8 participants (SL-CERT, ICTA, NCPA, Sri Lanka Police, CID)

Live data forensics training for law enforcement & CERT, 8-10 February

- conducting live data forensics and real-time monitoring of traffic data
- inter-departmental cooperation and intelligence sharing in combating cybercrime

46 participants (including 2 delegates from Tonga)

Study visit of two Tongan delegates to SL-CERT, 11-12 February

- best practice of Sri Lanka CERT shared with Tonga (challenges, incident handling, capacity building, coordination with others)



2016

| | |
|---|---|
| <p>Introductory Judicial Training of Trainers, 31 March – 3 April</p> <ul style="list-style-type: none">• create a pool of magistrate-trainers able to instruct their peers in the introductory skills and knowledge required in cases of cybercrime and electronic evidence | <p>16 Judges (High Court, Court of Appeal)</p> |
| <p>Introductory Training for prosecutors, 5-6 April</p> | <p>22 participants (State Counsels, Deputy Solicitor Generals)</p> |
| <p>International workshop and training for 24/7 points of contact in GLACY countries, 25-27 April</p> <ul style="list-style-type: none">•necessity and operations of a 24/7 PoC, best practices, international cooperation in criminal matters (INTERPOL, MLA etc.), cooperation with multinational service providers | <p>50 international participants & 20 officers from CID, TID and other Police Units</p> |
| <p>Study visit in the Philippines of forensics experts on benchmarking digital forensics services and standard operating procedures, 27-29 June</p> <ul style="list-style-type: none">•identify synergies between the approach and methodologies adopted by both countries in developing their digital forensic capabilities | <p>5 participants (Sri Lanka Police Units & SL-CERT)</p> |



2016

| | |
|---|--|
| <p>Advanced Judicial Training, 31 August – 2 September</p> <ul style="list-style-type: none">•follow-up on the Introductory ToT to reinforce the knowledge previously gained by the trained trainers | <p>12 Sri Lankan Judges and 2 magistrates from Tonga</p> |
| <p>National delivery of the Introductory Judicial Course, 24-25 September</p> <ul style="list-style-type: none">•monitor, benchmark and otherwise quality assure one course delivered by trainers trained under the GLACY Project | <p>22 participants (Sri Lankan Snr Judges and Magistrates)</p> |

2017

| | |
|--|--------------------------------------|
| <p>Development of cybercrime investigations, digital forensics capabilities, 14-17 March</p> <ul style="list-style-type: none">•INTERPOL led training on open source investigation using search engine and social media, guidelines on handling cybercrime statistics | <p>30 law enforcement officers</p> |
| <p>Residential training on cybercrime and electronic evidence for Prosecutors, 31 March – 2 April</p> <ul style="list-style-type: none">•condensed introductory course on cybercrime – substantive/procedural law; electronic evidence and investigative measures; international cooperation | <p>35 Officers (AG's Department)</p> |

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)
 - Hon. Ambepitiya Cases & Indian Fisherman's Cases
- **Act No. 14 of 1995 – Primary Legal Tool**



Thank You !

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

www.icta.lk