OCTOPUS CONFERENCE

Cooperation Against Cyber Crime

6-8 June 2012

Council of Europe
Strasbourg, France

AN EFFECTIVE AND EFFICIENT INVESTIGATION
"Striking the balance"
-
SRI LANKAN EXPERIENCE

By

Jayantha Jayasuriya, President's Counsel[1]
&
Jayantha Fernando, Attorney-at-Law[2]

Sri Lanka is a Common Law country[3]. On 07 July 2007, the Speaker certified the Computer Crime Act[4]. This law provides, that the offences relating to Computer Crime to be investigated under the provisions of the Code of Criminal Procedure Act[5]. However, Section 17 of the Computer Crime Act provides for the appointment of a "Panel of Experts" to assist police officers to conduct investigations under the Act. Their competency in Electronic engineering and Software Technology is taken into account at

[1] Additional Solicitor-General, in the Attorney-General's Department, served the State as a Public Prosecutor since 1983 and presently supervising the investigations and prosecutions relating to Computer Crime, Credit Card Frauds and matters relating Child Abuse.

[2] Director & Legal Advisor ICTA, responsible for ICT policy and legislative affairs, with specialization in ICT law, one time ICANN GAC Vice Chair

[3] Sri Lanka was a British Colony for nearly thirteen decades. Therefore the influence the English legal system had in the Sri Lankan legal system is immense. Main three statutes that deal with Offences, Investigations and Evidentiary matters introduced during British Regime continue to be in force with certain amendments to meet with the new challenges with the passage of time.

The Code of Criminal Procedure Act No 15 of 1979 mainly deals with the investigation of crimes, procedural aspects of a trial and an appeal. "Peace Officers" are entrusted with the duties relating to investigations including arrest and seizure.

[4] For a brief overview See
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres-SriLanka_Jayantha.pdf

[5] Under this Act a "Peace Officer" who is either a "Police Officer" or a "Village Administrative Officer" (Gramaniladhari) will have all powers of investigation. However, considering the complexities and technicalities involved in a "Computer Crime" an obvious issue that will be raised is the "competency" of the "Peace Officers" to ensure an efficient and an effective investigation.

the time the appointment is made. These investigators although are appointed to assist police officers in an investigations, they themselves are vested with wide powers such as: enter any premises, access any information system, computer or computer system, any programme, data or information held in a computer, require any person to disclose any traffic data and includes the power to orally examine any person..

The legislative scheme having provided these powers and protection to the "Experts" requires them to exercise these powers under Magisterial Supervision in instances of calling for information from Service Providers and in the interception of communications.

Section 18 of the Act requires a warrant issued by a Magistrate for an expert to initiate such action. It is also important to note that the power vested on an expert and a police officer to Order any person in charge of a computer or a computer system to preserve date in such system is restricted to a period of seven days. An extension of this period can be secured only by a Magisterial Order on an application made in that behalf.

Another provision that strikes a balance between an efficient investigation and the legitimate use of a computer or a computer system under investigation is embodied in Section 20. It requires Experts and Police Officers to ensure that the legitimate use of a computer is not hampered due to their search, inspection or any other step. It further prescribes that a computer or a computer system should not be seized if it hampers the legitimate use, unless the inspection cannot be conducted at the premises it is located, seizure is necessary to prevent the commission or the continuation of the commission of an offence or to obtain custody of any information.

Coordination among different State Agencies is a prominent feature in the Sri Lanka's fight against cyber crime.

Within the framework of the Criminal Investigations Department, a special unit called "Cyber Crime Investigations Unit" is established and an Inspector of Police is

functioning as the Officer in Charge of this unit. The Inspector General of Police has certified the skills and the competency of the OIC as provided under Section 21(2) of the Act[6].

To further strengthen and enhance the ability of law enforcement to investigate offences under the Computer Crimes Act, the ICT Agency of Sri Lanka (ICTA)[7] has taken the initiative to establish a Digital Forensic Lab for the "Cyber Crime Investigations Unit" of the Criminal Investigations Department (CID)[8].

In the Attorney-General's Office, Cyber Crime & Credit Card Frauds are classified as a separate subject and the supervision is entrusted to a Senior Officer in the Criminal Division[9]. Mainly, advising the law enforcement agencies, filing of indictments and conducting prosecutions in the High Court comes within the purview of the Attorney-General.

There are nearly 200 on going investigations handled by this unit. Around 66 complaints were received since January this year. Majority of these complaints relate to incidents in Social Networking Cites. They include publishing defamatory material. However, most of these investigations draw a blank as the administrators of those cites decline to provide necessary details.

There are two bank frauds relating to which investigations are continuing. In one such incident the bank computer system was hacked into and several transfers of funds from individual accounts of bank customers were made. Those customers whose accounts

---

[6] Under Section 21(2) no police officer can access a computer for the purpose of an investigation under this Act unless the Inspector General of Police has certified such officer as a person with who possesses adequate knowledge and skill in the field of Information Communication Technology and he posses required expertise.

[7] www.icta.lk – ICTA is the Apex ICT Policy and Implementation Arm of the Government vested with powers under the Information and Communication Technology Act No. 27 of 2003

[8] See http://epaper.dailymirror.lk/epaper/viewer.aspx , http://www.colombopage.com/archive_11A/Aug24_1314192985JR.php and http://www.lankajournal.com/2011/07/cid-to-track-computer-crimes/

[9] I have been supervising this area from its inception

were debited complained to the bank and the Cyber Crime Unit of the CID commenced an investigation on a complaint made by the Bank.

To conduct this investigation it was necessary to examine the data in the bank computer system. Investigators who were mindful of the requirement to ensure uninterrupted legitimate usage of the system, initially obtained details necessary to identify the relevant service provider through whom the suspect secured unauthorized access to the bank system. This information was obtained through the IT section of the bank itself. Thereby investigators ensured uninterrupted continuous operations in the bank computer system. Hence they succeeded to obtain necessary information while preserving the protection guaranteed under Section 20 of the Act.

The next stage of the investigation had to focus on the relevant service provider to obtain the subscriber information. Section 18 of the Act requires a police officer to obtain a Magistrates Order to request such information from a Service Provider. However, to avert any delay or to maintain the confidentiality the same section empowers any Police Officer to obtain such information directly from the Service Provider. According to the internal procedures laid out by circulars no police officer can make a direct request to a Service Provider for such information. Any police officer who needs to obtain such information should make a request to the relevant Deputy Inspector-General of Police who – upon being satisfied with the need - would in turn contact the service provider for the relevant information. Service Providers who maintain a separate unit to assist criminal investigations would then provide such information to the law enforcement agencies.

This procedure protects the service providers from unnecessary and arbitrary requests from the law enforcement while ensuring that they would assist law enforcement officers to combat crime effectively.

To further enhance checks and balances in the Cyber Crime enforcement process and also to mitigate cyber threats and incidents, ICT Agency of Sri Lanka (ICTA) has

established a national CERT, known as "Sri Lanka CERT - CC"[10], as part of a wider Cyber Security strategy. This entity functions as a public private partnership and Sri Lanka CERT was admitted as a full member of FIRST, APCCERT and function as a National Cyber Security Coordination Centre, establishing several sector specific CSIRTS[11].

Sri Lanka in practice has achieved the required standard of investigation while preserving and protecting guarantees provided under the Computer Crime Act. Safeguards provided under the legislation have not adversely affected the efficiency or the effectiveness of Criminal investigations.

[10] See www.slcert.gov.lk
[11] See also http://www.icta.lk/index.php?option=com_content&view=article&id=1107 for CERT activities