OCTOPUS Interface Conference (2010)

Co-operation Against Cyber Crime

Workshop 2 – Law Enforcement Responsibilities

Comments by Jayantha Fernando, Director/ Legal Advisor ICT Agency of Sri Lanka

& ICANN GAC member (Sri Lanka)

It is indeed a pleasure to be back at the OCTOPUS Conference and I thank Council of Europe (especially Alexander Seger and his team) for its dynamic leadership in organizing this high level cooperation to address global challenges associated with cyber crime on an annual basis.

Although this session addressed law enforcement responsibilities in the prevention and control of cyber crime, the emphasis was about the crucial role other actors such as CERT's, CSIRTS and even organizations such as ICANN can play to support the efforts of law enforcement authorities. In this context my *brief comments* today are in two Parts, addressing two perspectives:-

(1) The Sri Lankan perspective, giving a snap shot of the institutional framework we created to support law enforcement efforts. This perspective would be relevant to other developing countries wanting to pursue similar options.

(2) The ICANN perspective and more specifically what governments represented in the Governmental Advisory Committee (GAC) could do to support the efforts of law enforcement so as to help ICANN achieve one of its core missions, namely, security and stability of the Internet.

PART 1

Sri Lanka is at the threshold of moving towards an information society. In the post conflict era the Government stands committed to transforming the nation into a "*knowledge economy*". To achieve the objectives of a digital economy Sri Lanka embarked on a series of policy & regulatory reforms. In doing so we realized quite early that we had to conform to international standards and best practices. Consequently, three of the key ICT legal enablers, i.e. Intellectual Property Act No. 36 of 2003, Electronic Transactions Act No. 19 of 2006 as well as the Computer Crimes Act No.24 of 2007 were based on International legal norms and best practices. More particularly, when we embarked on the preparation of cyber crime legislation there were few international precedents available in this area. But later we felt comfortable in drawing on the principles contained in the "*Budapest Convention 2001*", as it was (and still remains) the only available convention on the subject of Cyber Crime and contains the appropriate checks and balances in the enforcement and investigation of Cyber Crime.

We are reaching 2 years since the Computer Crimes Act of 2007 was brought into operation on 15th July 2008. Several challenges are being encountered by law enforcement officials in the prevention and control of Cyber Crime. Our brief experience has shown that several actors are imperatively required to work in co-ordination with law enforcement to support their efforts. The role of expert assistance in law enforcement efforts has become crucial in the investigation and prosecution of Cyber Crime. Realising this we established a national level CERT, known as the Sri Lanka CERT (see www.slcert.gov.lk).

SL CERT was established as a Government owned company, a fully owned subsidiary of my agency, the ICT Agency of Sri Lanka (ICTA). The company model gives flexibility in its day to day operations and we able to draw on the best talents available to make it functional, where we are able to pay market level salaries to professionals, whose services can be retained in the long term. This structure has enabled SLCERT to be equipped with a world class team of information security incident handlers who are working closely with law enforcement as well as govt & private sector to deal with cyber threats. In its short period of operations I am pleased to say that SL CERT has been admitted as a full member of APCERT as well as FIRST.

The following are some of the key areas of activity where there has been high level of cooperation between Sri Lankan law enforcement and SL CERT

- Advising the implementation of a state-of-the-art Digital Forensics Laboratory for a law enforcement agency.
- Assisting the formation and accreditation of sector-based Computer Security Incident Response Teams (CSIRT)
- Conducting Malicious Software Analysis and removal mechanisms
- Investigating and solving incidents relating to spam mails being sent from Sri Lankan ISP's to overseas constituents. (based on incidents reported to SLCERT by FIRST members).
- Investigated and solved a DoS attack on mail servers at several Government Departments.
- Carried out network assessments at a Ministry, identified multiple issues and recommended solutions

The relationship between SL CERT and Law Enforcement has gradually gained momentum. In order to strengthen SL CERT operations further we recently signed into the global Security Co-operation Program (SCP) of Microsoft. The Government of Sri Lanka is appreciative of these efforts by global private sector entities such as Microsoft to further support and sustain Sri Lanka CERT operations which will help in the cyber crime control measures of law enforcement agencies.

PART 2

In addition to Sri Lanka's own national efforts, we believe we have a responsibility to support global efforts towards ensuring co-operation and coordination between law enforcement and other entities such as ICANN. If we are to prevent Cyber Crime as well as support its enforcement we need to act as responsible fraternity of the global internet community and as members of ICANN's Governmental Advisory Committee (GAC) we have a responsibility to advise our own governments to act in the best interest of all the good faith internet users and support efforts which will lead to enhanced global co-operation against cyber crime.

It is in this context that we support the twin recommendations of several Law Enforcement agencies to ICANN; i.e

(1) The amendments to the Registrar Accreditation Agreement (RAA), and

(2) due diligence recommendations for ICANN to adopt in accrediting registrars and registries

The RAA is the key contract which links ICANN and the over 800 ICANN accredited Registrars, who issue the key internet resources to end-user registrants of domain names, and regulates the rights and obligations between Registrars and registrants. The Registrars are the central players in the chain of domain name registrations.

The current format of the RAA seems to condone and encourage Proxy Registrations or Privacy Services, allowing key internet resource, namely the Domain Name System, to be used for wrongful conduct. This goes directly against the Joint Project Agreement (JPA) ICANN signed with the United States Department of Commerce on September 25, 2006 which specifically states "*ICANN shall continue to enforce existing (Whois) policy*", the September 30, 2009, Affirmation of Commitments, paragraph 9.3.1 which states "*ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information.*", and contravene the 2007 ICANN GAC "Principles on WHOIS".

These twin recommendations of law enforcement to ICANN, which have gained the support of the high tech crime experts in the G8 and Interpol, would aid the prevention and disruption of efforts to exploit domain registration procedures by Criminal Groups for criminal purposes. The proposed amendments take account of existing legislation in countries requiring individual's rights to privacy. These amendments would maintain these protections whilst facilitating effective investigation of Internet related crime.

Such recommendations, if adopted, would be an ideal way to mitigate global cyber threats and truly create the environment for digital empowerment of nations in developing countries as well.

In this context I see the ICANN's Governmental Advisory Committee (GAC) as a platform for enhancing greater level of co-ordination between law enforcement and those responsible for the development of policies associated with the management of key internet resources, as such as the DNS. There is a disconnect in respect of cooperation between the law enforcement of the developed and developing world in the area of development of policies concerning the management of key internet resources. The ICANN GAC is helping to overcome this gap and making it possible for policy makers from both the developed and developing world to keep abreast of the latest trends and efforts, which would help them advise their governments on the level of coordination needed between law enforcement agencies and their respective governments as well as other entities such as ICANN.

In the most recent communiqué issued after the Nairobi meeting, the GAC agreed to forward the above mentioned twin recommendations of law enforcement agencies to ICANN Board, indicating GAC support for these proposals. I hope we could give full endorsement to these recommendations at the GAC meeting in Brussels.

ICANN GAC is established pursuant to the ICANN By Laws and functions independently. GAC is governed by its own operating principles and working methods. (See www.gac.icann.org). GAC decisions are based on consensus reached between members represented in the GAC and is currently chaired by diplomat of international repute, Ambassador Janis Karklins of Latvia. It is representative of approximately 110 countries with many international organizations such as WIPO, UNESCO, Arab League and ITU participating as Observers

CONCLUSION

I am sure you all would agree that more needs to be done to support law enforcement agencies interface with governments across the world. This should happen across the political divide and I encourage events such these which could provide a platform for such an interface. We would encourage closer collaboration between Goverments, Law Enforcement Agencies as well as ICANN so that global challenges associated with Cyber Crime are addressed in a meaningful and realistic manner, both in the short and long term.

THANK YOU