www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs

20 April 2011

Global Project on Cybercrime

Meeting report

Cooperation against cybercrime in South Asia

International workshop

Colombo, Sri Lanka, 5-6 April 2011

Project funded by Estonia, Monaco, Romania, Microsoft, McAfee and the Council of Europe

Contents

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

1 Background

For countries of South Asia – as for societies in other regions of the world – information and communication technologies provide unprecedented opportunities for social and economic development. However, as societies rely on ICT, at the same time they become vulnerable to risks such as cybercrime. Cooperation at all levels – interagency, public-private, international – is a crucial element of the response.

In Asia, a number of countries, such as Bangladesh, India, Pakistan and Sri Lanka have taken or are in the process of taking important steps, including the strengthening of their legislation in line with the Budapest Convention on Cybercrime and of relevant institutions such as units responsible for high-tech crime investigations or incident response.

Building on earlier, country-specific workshops in India, Pakistan and Sri Lanka since 2008, the Information Communication Technology Agency (ICTA) of Sri Lanka and the Council of Europe (within the framework of the Global Project on Cybercrime) agreed to hold a regional event for countries of South Asia, that is, Bangladesh, India, Maldives, Pakistan and Sri Lanka. The meeting took place in Colombo, Sri Lanka, on 5 and 6 April 2011.

The aim was to enhance the capacity of countries of South Asia to cooperate internationally against cybercrime and more specifically:

- To assess the cybercrime legislation of participating countries in view of their compatibility with international standards (a prerequisite for international cooperation)
- To share experience and promote international police and judicial cooperation, including accession to agreements such as the Budapest Convention on Cybercrime
- To promote interagency and public-private cooperation at domestic levels.

More than 100 participants engaged in a open and constructive exchange of experience and developed proposals for a further strengthening of legislation, interagency, public-private and international cooperation.

In the final session of the workshop, participants adopted conclusions that summarise the proposals made.

2 Conclusions adopted by the workshop

International Workshop on Cooperation against Cybercrime in South Asia

Colombo, Sri Lanka, 5-6 April 2011

Conclusions

An international workshop on cooperation against cybercrime in South Asia was held in Colombo on 5 and 6 April 2011 with the participation of more than one hundred public and private sector representatives from Bangladesh, India, Maldives, Pakistan and Sri Lanka. The workshop was addressed by the Hon Mohan Pieris, President's Counsel, the Attorney General of Sri Lanka, by Supreme Court Justice Suresh Chandra, by Suhada Gamlath, Secretary Justice, and by Professor P.W. Epasinghe, Chairman ICTA and Advisor to the President of Sri Lanka. Speakers and participants from countries of South Asia as well as the Council of Europe and the Cybercrime Convention Committee shared their experience.

The workshop agreed that:

- Cybercrime – ranging from offences against computer data and systems to offences committed by means of computer systems and data as well as content-related offences – was a concern common to all countries. Specific threats include malware, botnets, fraud and criminal money on the internet, denial of service attacks and attacks against infrastructure by criminals as well as terrorists. The fact that almost any crime can have an element of electronic evidence entails major challenges to criminal justice systems;

- A distinction should be made between strategies against cybercrime – primarily aimed at criminal justice and the rule of law – and strategies to enhance cybersecurity – primarily aimed at enhancing the protection, reliability and resilience of computer systems and the information infrastructure in general. Intentional attacks against the confidentiality, integrity and availability of computer systems are to be addressed by both, and thus both are linked;

- Legislation providing for the criminalization of conduct and for effective investigations is an essential precondition for criminal justice measures. Legislation should be harmonized with international standards, that is, the minimum standards of the Budapest Convention on Cybercrime, in order to ensure consistency and interoperability. It was noted that the legislation of Sri Lanka is already largely in conformity with the Budapest Convention, and important legislation in line with this treaty has also been adopted in India

and Bangladesh. In Pakistan a previous ordinance on electronic crime is to be amended and brought in line with the Budapest Convention when transformed into a law in the very near future. In the Maldives, the preparation of such legislation – possibly through a special law – should be envisaged;

- Conditions and safeguards regarding investigative powers should be put in place to ensure due process and protect fundamental rights. Countries should also consider data protection regulations to protect the rights of individuals, to facilitate international law enforcement cooperation and to enable e-commerce and out-sourcing of services;

- Parliamentarians need to assume responsibility to ensure that domestic legislation is adopted to criminalize conduct, allow for effective investigation and establish safeguards and conditions as well as provisions for international cooperation. Exchanges of views and experience among parliamentarians of South Asia are encouraged, possibly through a regional parliamentary advisory group;

- A "buy in" from policy makers is necessary to allow for the adoption of policies, strategies and responses to threats in a timely manner;

- The effectiveness and adequacy of legislation should be monitored and assessed on a continued basis in view of fast evolving challenges;

- Preventive measures, including awareness and education, should be promoted. High-tech crime units, Computer Emergency Response Teams (CERTs) and the private sector have a role to play in this respect. The national CERTs of Sri Lanka and India and the NR3C of Pakistan already have good practices to share in this respect;

- Channels for reporting complaints and incidents by the public should be established to provide a better understanding of cybercrime threats and trends and provide leads for investigations;

- Institutional capacities need to be reinforced to permit the enforcement of legislation and responses to incidents. This includes:

  - CERTs such as those created in India and Sri Lanka,
  - high-tech crime units such as those at the Federal Investigation Agency of Pakistan and the Central Bureau of Investigations in India or the cybercrime squad in the Criminal Investigation Department of Bangladesh. The CoE should develop a toolkit to provide guidance on the establishment of high-tech crime units by making use of the experience available in South Asia,
  - comprehensive law enforcement training ranging from first responders to forensic investigators,
  - digital forensic laboratories to cope with the increasing need for handling of electronic evidence,
  - an important role by prosecutors in the criminal procedure,
  - the training and specialization prosecutors and judges. The judicial training concept adopted by the Council of Europe may provide guidance

to help ensure that cybercrime and electronic evidence matters are mainstreamed into judicial training. In Bangladesh (where special cyber-tribunals have been created) and in Sri Lanka cybercrime training modules are already being delivered. Countries are encouraged to share experience by making available existing modules and training materials. This would contribute to common approaches on training and facilitate networking between judicial training institutions and between trained judges and prosecutors;
- Online resources for the training of law enforcement, prosecutors and judges in order to complement face-to-face training. The Council of Europe should consider linking cybercrime training initiatives in Asia with similar activities in Europe,
- training and education for private sector entities with large IT infrastructure. This includes in particular the financial sector but also the respective regulators;

- Guidelines for handling, analyzing and presenting electronic evidence in court should be developed to ensure that evidence is accepted in criminal proceedings. The Council of Europe should make use of the expertise available in South Asia in this respect;

- Considering that most cybercrime is aimed at obtaining undue economic benefits, measures should be taken to protect individuals and the financial system from attacks, to prevent money laundering and the financing of terrorism and to search, seize and confiscate crime proceeds on the Internet. This will help safeguard the financial infrastructure. Interagency and public-private cooperation, including trusted fora for intelligence sharing and analysis, should be created. The forthcoming typology study on criminal money flows of the Council of Europe will document good practices in this respect;

- Public-private cooperation is a condition for effective prevention and investigation of cybercrime and for enhancing cybersecurity in general. The Budapest Convention already includes obligations for service providers to cooperate with law enforcement during investigations but this should be complemented by a culture of cooperation and structured cooperation along the lines of the law enforcement/service provider cooperation guidelines adopted by the Council of Europe's Octopus Conference in 2008. India and other countries of South Asia already have valuable experience in this respect;

- Cybercrime is often transnational crime or involves evidence located in foreign jurisdictions or held by foreign service providers. Efficient international cooperation to secure volatile electronic evidence and obtain it for investigation and criminal proceedings is the main challenge. The setting up a regional council or similar mechanism for cooperation against cybercrime in South Asia is encouraged. Existing channels of police-to-police cooperation, CERT-to-CERT cooperation and judicial cooperation should be exploited. The Commonwealth framework may be useful in this respect, but also existing South Asia regional cooperation frameworks could offer opportunities to enhance cooperation against cybercrime in South Asia. Countries are encouraged to seek accession to the Budapest Convention.

The workshop permitted a dynamic exchange of information and good practices among participants with immediate impact on cooperation between institutions within participating countries as well as between countries. Participants identified specific steps to be taken by their respective institutions. Follow up will therefore be required at the domestic level as well as regional and international levels. The Council of Europe and other organizations and donors should assist in such follow up.

The Council of Europe expressed its readiness to continue its cooperation with countries of South Asia against cybercrime. Representatives of South Asia may consider participation in the Octopus Conference on Cooperation on Cybercrime and the 10th anniversary of the Budapest Convention (Strasbourg, France, 21-23 November 2011).

Participants thanked the authorities of Sri Lanka, and in particular Jayantha Fernando and his team from ICTA, and the Council of Europe for providing an excellent forum for enhanced cooperation against cybercrime in South Asia.

Colombo, 6 April 2011

_____

3 Agenda

Tuesday, 5 April 2011	
8h30 – 9h15	Registration
Opening session	
9h30 – 10h00	Inauguration & opening statements (Head Table) ▪ Welcome Address – Prof P W Epasinghe, Advisor to HE the President ▪ Justices P A Ratnayake & Suresh Chandra, Judges of the Supreme Court (Special Guests of Honour) ▪ Mr Suhada Gamlath, Secretary Justice – Key note speaker ▪ Mr Alexander Seger – Council of Europe ▪ Secretary Ministry of Telecom & IT
10h30-10h30	*Tea break*
Session 1:	**The threat of cybercrime and national and international responses**
10h30 – 12h00	Moderator: Erik Planken, Ministry of Justice of the Netherlands, Vice-chair of the Cybercrime Convention Committee of the Council of Europe ▪ Introduction and overview (Alexander Seger, Head of Economic Crime Division, Council of Europe) Representatives from participating countries are invited to make short presentations and discuss the following questions: ➢ *What are the main cybercrime threats experienced by societies of South Asia?* ➢ *What measures on cybercrime and cybersecurity have been taken (overview)?* Interventions followed by exchange of views: ▪ Kamal Uddin Ahmed, Ministry of Home Affairs, Bangladesh ▪ Shahid Nadeem Baloch Director for Cyber-crime, Federal Investigation Agency Islamabad ▪ Jayanda Jayasuriya, DSG, Attorney General's Dept, Sri Lanka
Session 2:	**The threat of cybercrime: private sector perspective and responses**
12h00 – 13h00	Moderator: Pavan Duggal, Advocate at the Supreme Court, India Presentations followed by discussion: ▪ Jehan Ara, President Software Houses Association – P@ASHA, Pakistan ▪ Pratap Reddy, Senior Director Cybersecurity, NASSCOM, India ▪ Ms Sharmini Wickramasekera, Chief Risk Officer, Lanka Orix Leasing PLC, Sri Lanka

13h00 – 14h30	*Lunch break*
Session 3:	**Cybercrime legislation: International standards and examples of domestic legislation**
14h30 – 16h00	Moderator: Zahid Jamil, Pakistan The Budapest Convention on Cybercrime ▪ Cristina Schulman, Head of Cybercrime Unit, Council of Europe Current and planned legislation in countries of South Asia: ▪ Kamal Uddin Ahmed, Joint Secretary, Ministry of Interior, Bangladesh ▪ Pavan Duggal, Advocate, India ▪ Marvi Memon, Member of National Assembly, Pakistan ▪ Jayantha Fernando, Director & Legal Advisor ICTA Sri Lanka ▪ Mariyam Shahula, Assistant Public Prosecutor, Prosecutor General's Office, Maldives
16h00-16h30	*Tea break*
Session 4:	**Public-private cooperation against cybercrime**
16h30 – 17h30	Guidelines on law enforcement – Internet service provider cooperation in the investigation of cybercrime ▪ Alexander Seger, Council of Europe Discussion on strengths, weaknesses, opportunities and risks regarding public-private cooperation against cybercrime in South Asia ▪ Interventions by Government and private sector participants
17h30	**End of session**

Wednesday, 6 April 2011	
9h30 – 10h00	**Key Note Address by Chief Guest** Hon Mohan Pieris, President's Counsel – Attorney General of Sri Lanka
Session 5:	**Institution building**
9h45 – 11h00	Moderator: Jayantha Fernando, Director & Legal Advisor ICTA Sri Lanka The role of high-tech crime units ▪ R.R. Sahay, Senior Superintendent of Police, Central Bureau of Investigation, India ▪ Shahid Nadeem Baloch, Director for Cyber-crime, Federal Investigation Agency, Pakistan The role of incident response teams ▪ Pankaj Sharma, Joint Director, CERT-IN, India (via video link) ▪ Lakshan Soysa, Manager Operations, Sri Lanka CERT The role of prosecution services ▪ Mariyam Shahula, Assistant Public Prosecutor, Prosecutor General's Office, Maldives The role of judges and judicial training ▪ Cristina Schulman, Council of Europe
11h00-11h30	*Tea break*
Session 6:	**Cybercrime and emerging challenges**
11h30 – 12h30	Intervention followed by discussions: ▪ Wipul Jayawickrama, Managing Director, Infoshield Consulting, Australia: The Role of Information Security in Combating Money Laundering and Terrorism Financing
Lunch	
Session 7:	**International Cooperation**
13h30 – 15h00	International cooperation under the Budapest Convention on Cybercrime ▪ Erik Planken, Netherlands, Cybercrime Convention Committee International judicial cooperation: ▪ Hon. Justice Suresh Chandra - Judge of the Supreme Court, Sri Lanka

	Cooperation between incident response teams: ▪ Rohana Palliyaguru, Snr Information Security Engineer, SLCERT ▪ Anil Sagar, Director, CERT-IN, India Police to police cooperation ▪ Saiful Alam, Deputy Inspector General, CID, Bangladesh ▪ R.R. Sahay, India ▪ Shahid Nadeem Baloch, Pakistan ▪ M K D Wijaya Amerasinghe, SSP, Director CID, Sri Lanka
Tea break	
Session 8:	**Current strategies and future plans on measures against cybercrime and for cybersecurity**
15h30 – 17h00	Legislation – institution building – training – coordination – incident response – investigation – prosecution – adjudication – interagency cooperation – public private cooperation – international cooperation Statements by representatives from: ▪ Bangladesh ▪ India ▪ Maldives ▪ Pakistan ▪ Sri Lanka (Mr Wasantha Bandara, DSG, Attorney General's Dept) Discussion
Session 9:	**Concluding session**
17h00	Chair: Hon Justice Suresh Chandra (Judge of the Supreme Court) Discussion and adoption of conclusions
18h00	**End of meeting**
18h30	Cocktail Reception

4 List of participants

Name	Organization
International participants	
Alamgir Mohammed Monsurul Alam	Ministry of Home Affairs Government of Bangladesh
Alexander Seger	Council of Europe
Cristina Schulman	Council of Europe
Dr Md. Kamal Uddin Ahmed	Ministry of Home Affairs, Government of Bangladesh
Erik Planken	Cybercrime Convention Committee/Council of Europe
Jehan Ara	Pakistan Software Houses Association for IT & ITES, Pakistan
Mariyam Shahula	Prosecutor General's Office, Maldives
Marvi Memon	Member of National Assembly, Pakistan
Md. Saiful Alam	CID, Bangladesh Police, Bangladesh
Mohamed Adil Khan	Member of Pronvicial Assembly, Sindh, Pakistan
Nadeem Baloch	Federal Investigation Agency, Islamabad, Pakistan
Pavan Dugal	Lawyer at Supreme Court, India
Pratap Reddy	Data Security Council of India/NASSCOM, India
R R Sahay	Central Bureau of Investigations/India
Zahid Jamil	Lawyer, Council of Europe speaker, Pakistan
Sri Lankan participants	
Jayantha Fernando	ICTA
Sharmini Wickramasekara	Lanka Orix Leasing Co
Ms Vasana Edirisuriya	Ministry of Education
Mrs Dilhara Amerasinghe	Ministry of Justice
Hon. & Mrs Mohan Pieris	Ministry of Justice
Mr Rohan Seneviratne	Ministry of Defence
Maj Gen (Rtd) H K G Hendawitharana	Ministry of Defence
Mr Nimal Athukorala	Ministry of Telecom & IT
Dr. Manodha Gamage	TRCSL
Mr M C M Farook	TRCSL
Ms Sanjika Wijesundera	Sri Lanka Telecom
Mr P A Dias	Sri Lanka Customs
Mr. Kavana Ratnayake	Dialog Telecom PLC
Susantha Senaratne	Dialog Telecom PLC
Ms Nadira Siriwardana	Etisalat Lana (Pvt) Ltd
Mr Namal Ratnayake	Mobitel (Pvt) Ltd
Brigd Sarath Wickramasinghe	SL Army
Capt P D K Peiris	SL Navy
Mr Jayantha Kulatilaka	SL Police - CID
Mr M K D W Amarasinghe (SSP)	SL Police - CID

Mr B A N Priyadarshana (IP)	SL Police - CID
Mr B M A F K Senaratne (IP)	SL Police - CID
Mr Lasantha Dharmaratne (SI)	SL Police - CID
Ms Nadeeka Dissanayake (WSI)	SL Police - CID
Mr P Ampawila (ASP)	SL Police - CID
Mr Rohan Masimbula	SL Police - CID
Mrs T T Umagiliyage	SL Police - TID
Mr U Y B Udukumbura	SL Police - TID
Mr J A J C Jayasooriya	SL Police - TID
Ms L B Nimali Shanthi	SL Police - TID
Ms Nadeesha Mallawarachchi	SL Police - TID
Mr Oshan Hewavitarana	SL Police - TID
Hon. Justice. P A Ratnayeke, *President's Counsel*	Supreme Courts
Mr Suhada Gamlath, *President's Counsel*	Supreme Courts
Hon. Justice. Suresh Chandra	Supreme Courts
Mrs M M Jayasekara	Supreme Courts
Mr Uchitha Wickemasinghe	Supreme Courts
Mr Ashan Stanislaus	Supreme Courts
Mr S.C. Abhayaratne	Judicial Service Commission
Mr P.M. Amarasena	Judicial Service Commission
Ms K.U.T. De Silva	Judicial Service Commission
Mr K.P.S. Harshan	Judicial Service Commission
Mr K.T. Kekirideniya	Judicial Service Commission
Ms D.M. Kodithuwakku	Judicial Service Commission
Mr K.R.H.M.U. Kulathunga	Judicial Service Commission
Ms K.A.D.S.C. Perera	Judicial Service Commission
Mr M.G.K. Perera	Judicial Service Commission
Ms M.S Primki	Judicial Service Commission
Mr L.M. Rathnayaka	Judicial Service Commission
Ms B. Sirisena	Judicial Service Commission
Mr W.R.M.A. Wickramasinghe	Judicial Service Commission
Mr S.G.C.Wickramanayaka	Judicial Service Commission
Hon. Priyasath Dep, *President's Counsel*	AG s Department
Mr Jayantha Jayasuriya	AG s Department
Mr N.M.W.N. Bandara	AG s Department
Mr K.M. Waidyaratne	AG s Department
Mr. Chethiya Goonasekara	AG s Department
Mrs Varunika Hettige	AG s Department
Mr. T Kumarage	AG s Department
Mr M P S S De Silva	AG s Department
Mr Riyaz Bary	AG s Department
Ms Suganthi Kandasamy	AG s Department
Mr G S A De Silva	Legal Draftsman
Mr V Vimaleswaran	Legal Draftsman
Ms C B Illesinghe	Legal Draftsman
Ms H V C U Withanage	Legal Draftsman
Ms R P Kodithuwakku	Legal Draftsman
Ms UM Sapukotana	Legal Draftsman
Ms V L Dayaratna	Legal Draftsman

Mr U P Alawattage	Central Bank
Mr Hemakumara Karunaratne	Central Bank
Mrs Janakie Mampitiya	Central Bank
Mrs Mala Dayaratne	Central Bank
Mr Harsha Wanigatunga	Lanka Clear
Mr Rohan Peiris	Bank of Ceylon
Mr Rohan Muttiah	Commercial Bank
Mr Amal Hettige	HSBC
Mr Nalin Wijeratne	NDB
Mr Asiri Dharmaratne	People's Bank
Mr Chrisantha Silva	Computer Society of SL
Ms Samanthi Sudurikku	ISACA
Mr Anushka Silva	ISACA
Mr Chamindra De Silva	ISSA
Mr Thilak Pathirage	ISSA
Mr Ershad Hallaldeen	DMS Electronics
Mr Hemasiri Karunanayake	DMS Lanka
Mr Viraj Mudalige	Epic Lanka
Mr Wipul Jayewickrema	Inforshield Australia
Mrs Mano de Silva	Inforshield Australia
Mr Kapila Weerasekara	Lanka Logistics
Mr Bimal Gunapala	Millenium IT
Mr Janindu De Silva	Price Waterhouse Coopers
Keerthi Goonatilaka	University of Colombo School of Computing
Mr Harsha Wijewardene	University of Colombo School of Computing
Mr Lakshan Soysa	SLCERT Staff
Mr Rohana Palliyaguru	SLCERT Staff
Mr Kanishka Yapa	SLCERT Staff
Mr Demisha De Silva	SLCERT Staff
Mr Prasad De Silva	SLCERT Staff
Roshan Chandragupta	SLCERT Staff
Mithila Somaweera	SLCERT Staff
Ms Nilusha Goonetilleke	SLCERT Staff