



Octopus Conference



Cooperation against Cybercrime

6 – 8 June 2012

Palais de l'Europe, Council of Europe, Strasbourg, France

Version 8 June 2012

Agenda

Overview

WED, 6 JUNE		
Plenary session	Room 1	
9h30	Opening session	
10h30	Update	
Workshop sessions	Room 1	Room 2
14h30	Workshop 1: Cybercrime legislation	Workshop 2: Private/public information sharing
20h00	Social dinner	
THU, 7 JUNE		
Workshop sessions	Room 1	Room 2
9h30	Workshop 3: Online child protection legislation	Workshop 4: Transborder access and jurisdiction
Workshop sessions	Room 1	Room 2
14h30	Workshop 5: Rule of law and human rights safeguards and data protection	Workshop 4 cont'd: Transborder access and jurisdiction
		Room 14 Meeting on electronic evidence guide (restricted)
FRI, 8 JUNE		
Plenary session	Room 1	
9h30	Plenary: ► Results of workshops ► Panel: Future of cooperation against cybercrime: visions and wish lists ► Conclusions	
13h00	End of conference	

Detailed Agenda

WED, 6 JUNE	
Plenary session	
9h30 Room 1 <i>English, French, Russian, Spanish</i>	Opening session <ul style="list-style-type: none"> ▶ Opening: Thorbjørn Jagland, Secretary General of the Council of Europe ▶ Panel: Setting the scene <ul style="list-style-type: none"> ▪ Athaliah L. Molokomme, Attorney General, Botswana ▪ Sigrid Arzt, Commissioner, Federal Institute for Public Access to Information and Data Protection of Mexico (IFAI) ▪ Béla Szombati, Ambassador, Head of Cyber Conference Secretariat, Ministry of Foreign Affairs, Hungary ▪ Bill Harmon, Head of Digital Crimes Unit, Microsoft, Redmond, USA
10h30 Room 1 <i>English, French, Russian, Spanish</i> 11h00-11h15 <i>Coffee break</i>	Update <ul style="list-style-type: none"> ▶ From Octopus to Octopus: developments since November 2011 (Alexander Seger, Head of Data Protection and Cybercrime Division, Council of Europe) ▶ Cybercrime: key threats and trends <ul style="list-style-type: none"> ▪ InHope (Adrian Dwyer, Executive Director, Netherlands) ▪ Kaspersky Lab (Igor Chekunov/Andrey Yarnikh) ▪ Symantec (Adam Palmer, Norton Lead Cyber Security Advisor Symantec, POLCYB Director, USA) ▪ Group-IB (Sergey Grudinov, Russian Federation) ▪ Discussion ▶ Policies and initiatives on cybercrime by international organisations <ul style="list-style-type: none"> ▪ European Union (Jakub Boratynski, Head of Unit Fight against Organised Crime, Directorate-General Justice, Freedom and Security, EU Commission) ▪ African Union Commission ▪ ENISA (Silvia Portesi, European Network and Information Security Agency) ▪ UNODC (Gillian Murray, Chief Focal Point for Cybercrime, United Nations Office on Drugs and Crime) ▪ OSCE (Nemanja Malisevic, Cyber Security Officer) ▪ Organisation of American States (Belisario Contreras, Program Manager, OAS) ▪ Secretariat of the Pacific Community (Siaosi Sovaleni, Manager, Pacific ICT Outreach) ▪ Interpol ▪ Commonwealth Cybercrime Initiative (Lara Pace, Communications Officer, Comnet Foundation for ICT Development) ▪ GUAM – Organization for Democracy and Economic Development (Oleg Klynchenko, Programme Coordinator) ▪ Eurojust (Francesco Lo Voi, National Member Eurojust, Italy) ▪ Cybercrime Convention Committee (Markko Künnapu, Chair, T-CY) ▪ Internet Governance Strategy 2012 - 2015 of the Council of Europe (Lee Hibbard)
13h00 Lunch break	

<i>Workshop sessions</i>	
Wed, 6 June 14h30 Room 1 <p><i>English, French, Russian, Spanish</i></p> <div style="text-align: right;"> <i>16h00-16h15 Coffee break</i> </div>	<h2>Workshop 1: Cybercrime legislation</h2> <p>Countries worldwide have been reforming their domestic cybercrime legislation, many of them on the basis of the Budapest Convention. Success stories and good practices are available. However, progress has sometimes been slow and cybercrime legislation is not always high on the agenda of governments and parliaments.</p> <p>This workshop is to:</p> <ul style="list-style-type: none"> - review the global state of cybercrime legislation - present case studies of recent reforms - identify obstacles encountered in the adoption of legislation <p>Moderator: Jayantha Fernando, Director, ICTA, Sri Lanka</p> <p>Agenda:</p> <ul style="list-style-type: none"> ▶ The global state of cybercrime legislation <ul style="list-style-type: none"> ▪ Overview (Cristina Schulman, Head of Cybercrime Unit/Marie Agha-Wevelsiep, Cybercrime Unit, Council of Europe) ▪ Legislative reform: <ul style="list-style-type: none"> ○ Japan (Yoshimitsu Yamauchi, Senior Attorney for International Affairs, Criminal Affairs Bureau, Ministry of Justice) ○ Costa Rica (Francisco Salas Ruiz, Informatic Law Prosecutor and Director of the Law in Effect System, General Prosecutor Office) ○ Sri Lanka (Jayantha Jayasuria (Additional Solicitor-General, Attorney-General's Department, Sri Lanka)) ▪ Recent legislative developments - Tour de table with short interventions by Argentina, Armenia, Azerbaijan, Bosnia and Herzegovina, Benin, Botswana, Brazil, Cambodia, Chile, Cote d'Ivoire, El Salvador, Israel, Kyrgyzstan, Mexico, Niger, Nigeria, Panama, Paraguay, Philippines, Thailand, Uzbekistan and others ▶ Case law & application of law <ul style="list-style-type: none"> ▪ Presentations by participants on how legislation has been applied in practice (Belgium, Serbia, United Kingdom) ▶ Problems encountered/issues identified in the adoption of legislation – interventions by participants

English only

Private sector organisations and initiatives dispose of large amounts of information on cyber threats. If shared properly with the public sector and among relevant stakeholders from the private sector, this information can help prevent/disrupt botnet activity, fraud and other forms of attack and support law enforcement action.

- explain the need for private/public information sharing
- present experience, practices and opportunities available
- discuss practical, but also legal and data protection challenges

Agenda:

- ▶ Setting the stage: the need for private/public information sharing
 - Recap: Cybercrime and cybersecurity – the threat landscape
 - Defining the issue: what do we mean by private/public information sharing?
 - Case study (Bill Harmon, Digital Crimes Unit & Roger Halbheer, WW Chief Security Advisor, Microsoft Corp.)
- ▶ Discussion: current experience and practices
 - Japan – law enforcement and private sector cooperation
 - Tomoyuki Kurahara, Assistant Director, Cybercrime Division, National Police Agency, Japan
 - Tomohiko Yamakawa, Producer, Cyber Security Project, Research and Development Planning Department - Nippon Telegraph and Telephone Corporation)
 - Russia: Public/private information and cybercrime prosecution in Russia
 - Sergey Grudinov, Deputy-CEO, Group-IB, Russian Federation
 - Andrey Yarnikh & Igor Chekunov, Kaspersky Lab
 - Industry: Anti-Phishing Working Group (Peter Cassidy, Secretary General, APWG, USA)
 - Netherlands: The Dutch Cyber Security Centre (Elly van den Heuvel, General Manager, NCSC, Netherlands)
 - Germany: from Botfrei.de to ACDC (Thorsten Kraft / Ivo A. Ivanov, Head of Department, Professional Services General Corporate Counsel, ECO – Association of German Internet Industry, Cologne, Germany)
 - ENISA – studies on CERT/LEA information exchange (Silvia Portesi, Expert Technical Competence Department)
 - European Commission – DG Home Affairs: The European Cybercrime Centre (Jakub Boratinsky, Head of Unit Fight against Organised Crime)
 - Turkey: Private/public information sharing (Bilal Sen, Cybercrime Department, Turkish National Police)
- ▶ Challenges and opportunities
 - Survey on National Cyber Crime and Online Threats Reporting Centres (Wout de Natris, Natris Consult, Netherlands)
 - Data protection issues: Joe Cannataci, Professor of Information Policy, Security & Technology Law at University of Groningen
- ▶ The way forward
 - Towards documenting good practices and developing guidelines?

16h00-16h15
Coffee break

THU, 7 JUNE

Workshop sessions

9h30 Room 1

*English, French,
Russian,
Spanish*

Workshop 3: Online child protection legislation

Measures to identify, rescue and protect child victims of online sexual exploitation and international criminal justice action to prosecute offenders are crucial. Insufficient or incompatible legislation in many countries is a major obstacle to successful action. For that reason, INTERPOL in November 2011 adopted a legislative engagement strategy sponsored by the Virtual Global Taskforce (VGT). The Council of Europe and the VGT agreed to cooperate in the implementation of this strategy.

This workshop is to:

- Explain the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and the Budapest Convention on Cybercrime as benchmarks
- Discuss whether countries are meeting these benchmarks in their domestic legislation
- Present the "legislative engagement" strategy of Interpol and the Virtual Global Taskforce
- Identify specific action to be taken under this strategy

Moderators: Peter Davis, Chief Executive, Child Exploitation and Online Protection Centre (CEOP), United Kingdom / Anjan Bose, ICT and Child Protection, ECPAT International, Thailand

Agenda:

- ▶ The legislative engagement strategy of VGT/Interpol
 - Peter Davis, CEOPS
 - Discussion/Q&A
- ▶ Legislative benchmarks of the Lanzarote and Budapest Conventions
 - Eric Ruelle, Magistrat, Premier vice-président Tribunal de grande instance de MEAUX, France, Chairman of the Lanzarote Convention Committee
 - Discussion/Q&A
- ▶ Implementation
 - Current legislation in place - overview of implementation (Cristina Schulman, Head of Cybercrime Unit, Council of Europe)
 - Problems of implementation in the Asia/Pacific region (Anjan Bose, ECPAT)
 - Interventions/examples from different countries: legislation and operational cooperation
- ▶ Identification of countries and specific measures for legislative engagement

*11h00-11h15
Coffee break*

<p>Thu, 7 June 14h30 Room 2</p> <p><i>Not open to the media</i></p> <p><i>Chatham House rules apply</i></p> <p><i>16h00-16h15 Coffee break</i></p>	<p>Workshop 4 cont'd: Transborder access and jurisdiction</p> <ul style="list-style-type: none"> ▶ Access via service providers or private companies: scenarios, practices, concerns (90 min) <ul style="list-style-type: none"> ▪ Government access to data in the clouds – Hogan Lovells White Paper (Winston Maxwell, Hogan Lovells) ▪ AFA, APWG, ECO, Group-IB, Kaspersky Lab, Microsoft, Symantec and others ▪ Discussion ▶ Implications and possible concerns <ul style="list-style-type: none"> ▪ Jurisdiction and national sovereignty <ul style="list-style-type: none"> - Jurisdiction over crimes committed through computer systems and Internet (Cristos Velasco San Martin, Ciberdelincuencia.org, Mexico) ▪ Data protection, privacy and rule of law safeguards <ul style="list-style-type: none"> - Comments by Joe Cannataci, Chair in European Information Policy & Technology Law, University of Groningen, Netherlands ▪ Discussion ▶ Options
<p>14h30 Room 1</p> <p><i>English, French, Russian, Spanish</i></p>	<p>Workshop 5: Rule of law and human rights safeguards and data protection</p> <p>Governments have the positive obligation to protect people against crime and to make their laws enforceable. However, when doing so, human rights and rule of law requirements must be met. This includes the principles set forth in Article 15 of the Budapest Convention on Cybercrime but also data protection standards such as those of Convention 108.</p> <p>This workshop is to:</p> <ul style="list-style-type: none"> - Present the benchmarks of Article 15 and examples of implementation - Present Data Protection Convention 108 as an option also for non-European countries - Inform of the state of the modernisation of Convention 108 - Present case studies of recent data protection laws <p>Moderators: Mouhamadou Lo, Président de la Commission de protection des données personnelles du Sénégal / Sophie Kwasny, Secretary Data Protection Committee, T-PD, Council of Europe</p> <p>Agenda:</p> <ul style="list-style-type: none"> ▶ Applying article 15 of the Budapest Convention <ul style="list-style-type: none"> ▪ Introducing the meaning and scope of Article 15 (Betty Shave, Computer Crime and Intellectual Property Crime Section, Department of Justice, USA) ▪ The example of Croatia (Drazen Dragicevic, Professor, Croatia) ▪ Examples of implementation (interventions by countries) ▪ Discussion ▶ Data protection and cybercrime investigations: challenges <ul style="list-style-type: none"> ▪ Overview (Joe Cannataci, Chair in European Information Policy & Technology Law, University of Groningen, Netherlands) ▪ The global cybercrime ecosystem: personal data, digital privacy, and the future of judicial investigations (Solange Ghernaouti-Hélie, Swiss Cybersecurity Advisory and Research Group, University of Lausanne, Switzerland) ▪ Data protection and cybercrime investigations (Jean-Philippe Moïny, Centre de recherches informatique et droit, Belgium)

16h00-16h15 <i>Coffee break</i>	<ul style="list-style-type: none"> ▶ Promoting data protection standards globally: Convention 108 <ul style="list-style-type: none"> ▪ Introducing Convention 108 and Protocol 181 (Jean-Philippe Walter, Chair of the Data Protection Committee, T-PD, Switzerland) <ul style="list-style-type: none"> - The state of modernisation of Convention 108 - Relations between Convention 108 and the EU draft Regulation and draft Directive on data protection in the criminal justice sector ▪ Costa Rica: Data protection legislation (Francisco Salaz Ruiz, General Prosecutor's Office, Costa Rica) ▪ Senegal: data protection legislation (Mouhamadou Moustapha LO, Président de la Commission de protection des données personnelles du Sénégal) ▪ India: data protection legislation (Pavan Duggal, Advocate, Supreme Court of India, President Cyberlaw Asia, India) ▪ USA: Lara Ballard, Special Advisor for Privacy and Technology, U.S. Department of State ▶ Conclusions
Thu, 7 June 14h30 Room 14	<p>Side meeting: CyberCrime@IPA working group on the electronic evidence guide</p> <ul style="list-style-type: none"> ▶ Moderator: Nigel Jones, United Kingdom
FRI, 8 JUNE	
Plenary session	
9h30 Room 1 <i>English, French, Russian, Spanish</i> 11h00-11h15 <i>Coffee break</i>	<p>Results and visions</p> <ul style="list-style-type: none"> ▶ Results of workshops (summaries by moderators) <ul style="list-style-type: none"> ▪ Workshop 1: Legislation (Jayantha Fernando, Sri Lanka) ▪ Workshop 2: Private/public information sharing (Zahid Jamil, Pakistan) ▪ Workshop 3: Online child protection legislation (Anjan Bose, Thailand) ▪ Workshop 4: Transborder access to data (Markko Künnapu, Estonia) ▪ Workshop 5: Safeguards and data protection (Mouhamadou Lo, Senegal) ▪ Side meeting: Electronic evidence guide (Nigel Jones, United Kingdom) ▶ Panel: The future of cooperation against cybercrime – visions and wish lists <ul style="list-style-type: none"> ▪ Tom Dukes, Office of the Coordinator for Cyber Issues, State Department, USA, Chair G8 High-tech Crime Sub-group ▪ Harsh Jain, Ministry of Foreign Affairs, India ▪ Ernest Chernukhin, Ministry of Foreign Affairs, Russian Federation ▪ Monika Josi, Chief Security Advisor Europe, Middle East and Africa, Microsoft ▪ Peter Coronoes, ICODE, Australia ▶ Conclusions <ul style="list-style-type: none"> ▪ Concluding remarks by representatives of different regions <ul style="list-style-type: none"> ○ Kerry-Ann Barrett, Ministry of National Security, Trinidad and Tobago ○ George-Maria Tyendezwa, Federal Ministry of Justice, Nigeria ○ George Jokhadze, Ministry of Justice, Georgia ○ Zuleika Moore, Public Ministry, Panama ○ Yoshimitsu Yamauchi, Ministry of Justice, Japan ▪ Maud de Boer-Buquicchio, Deputy Secretary General of the Council of Europe
13h00	<i>End of conference</i>