

Octopus Conference 2016

Cooperation against Cybercrime

16 – 18 November 2016

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

Version 16 November 2016

Draft

Conference Programme

The Octopus Conference is part of the Cybercrime@Octopus project which is funded by voluntary contributions from Estonia, Japan, Monaco, Romania, United Kingdom, USA and Microsoft. Estonia, Japan and USA have made funding specifically available for the Octopus conference.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Programme overview

WED, 16 NOVEMBER			
Plenary session	*Hemicycle*		
9h00	Special Session: BUDAPEST CONVENTION – 15th ANNIVERSARY *(English/French/Russian/Spanish)*		
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/F)*	*Room 3 (E)*
14h30	Workshop 1: ► Capacity building on cybercrime: good practices, success stories and lessons learnt	Workshop 2: ► Legislation on cybercrime and capacity building in the Asia/Pacific region	Workshop 3: ► Service provider/law enforcement cooperation on cybercrime and electronic evidence
20h00 Social dinner in an Alsatian restaurant			
THU, 17 NOVEMBER			
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/S/F)*	*Room 3 (E)*
9h30	Workshop 4: ► Terrorism and information technology: the criminal justice perspective	Workshop 5: ► Legislation on cybercrime and electronic evidence in - Africa - Latin America	Workshop 6: ► International cooperation: workshop for 24/7 points of contact and MLA authorities
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/F)*	*Room 3 (E)*
14h30	Workshop 7: ► Seeking synergies: Initiatives of international and private sector organisations	Workshop 8: ► Targeting proceeds from crime online	Workshop 9: ► Crime and jurisdiction in cyberspace: access to electronic evidence
FRI, 18 NOVEMBER			
Plenary session	*Room 1 (E/F/S/R)*		
9h30	Plenary: ► Results of workshops ► Human rights and rule of law in cyberspace: threats and safeguards ► Conclusions		
13h00	*End of conference*		

Detailed programme

WED, 16 NOVEMBER	
Plenary session	*Hemicycle (English/French/Russian/Spanish – Live webcast)*
9h00	**Special Session: BUDAPEST CONVENTION – 15th ANNIVERSARY** *The Budapest Convention on Cybercrime was opened for signature in 2001 and fifteen years later remains the most relevant international instrument. The aim of this session is to review achievements to date and to discuss the further evolution of the Budapest Convention in the light of new threats and challenges.* ► Opening (9h00 – 9h20) - Thorbjørn Jagland (Secretary General of the Council of Europe) - Deposit of instrument of accession by Andorra ► Impact and potential of the Budapest Convention (9h20-10h00) Chair: Philippe Boillat (Director General of Human Rights and Legal Affairs, Council of Europe) - Norman Aas (Secretary General, Ministry of Justice of Estonia, Estonian Chairmanship of the Committee of Ministers) - Eva Descarrega (Secrétaire d'État à la Justice et Intérieur, Andorra) - Koichi Mizushima (Ambassador in charge of Cyber Policy, Ministry of Foreign Affairs, Japan) - Papa Assane Touré (Papa Assane Touré, Secrétaire général Adjoint du Gouvernement Primature du Sénégal) ► Panel: Cybercrime – International perspectives (10h00 – 10h45) - Daniela Buruiana (Chair of the Task Force on Cybercrime, EUROJUST) - Ahmed S. El-Dawla (Chief of Europe and Middle-East Section, Counter-Terrorism Committee Executive Directorate (CTED), United Nations) - Christophe Durand (Head of Strategy and Outreach, IGCI, INTERPOL) - Erik Planken (Chair, Cybercrime Convention Committee, Ministry of Justice and Security, Netherlands) ► Panel: Private sector perspectives on cybercrime and the rule of law (11h00-11h40) - Google - Microsoft ► The rule of law in cyberspace: the problem of enforcement (11h40-12h15) - Maria Elvira Tejada de la Fuente (Chief, Cybercrime Prosecution Office, Spain) - Yvonne Atakora Obuobisa (Director of Public Prosecutions, Ghana) ► Budapest Convention: Past, present and the future – The view of founders and followers (12h15 – 13h00) - Panel discussion: Rik Kaspersen (Netherlands), Betty Shave (USA), Pedro Verdelho (Portugal), Martha Stansell-Gamm (USA) , Uldis Ķinis (Latvia) ► Conclusions
Coffee break 10h45-11h00	
13h00	*Lunch break*

WED, 16 NOVEMBER	
14h30	*Room1 (Languages: English/French/Spanish/Russian – Live webcast)* **Workshop 1 – Capacity building on cybercrime: ingredients for success** *Capacity building has become the privileged international approach to address the challenges of cybercrime and electronic evidence. This is reflected, among other things, in the establishment of the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania (April 2014), the outcome of the UN Congress on Crime Prevention and Criminal Justice (Qatar, April 2015), the Global Cyber Space Conference (The Hague, Netherlands, April 2015), the establishment of the Global Forum for Cyber Expertise GFCE) and in the policies and programmes of a number of international organisations.* *The aim of this workshop is to identify ingredients for success, impact and sustainability of capacity building programmes.* Moderator/s: Panagiota-Nayia Barmpaliou (Programme Manager Cybersecurity and Organised Crime, Directorate General for International Cooperation and Development, European Commission) Rapporteur: Esther George (GPEN, United Kingdom) Secretariat: Matteo Lucchetti (Cybercrime Programme Office, Council of Europe) ► Panel: What is capacity building and what makes a successful capacity building project? (45 min) *16h00-16h15* *Coffee break* ► Update: Overview of new projects and good practices (45 min) ► Panel: How to set up sustainable criminal justice training programmes? (45 min) ► Panel: Public/private cooperation for capacity building – How does this work? (45 min) ► Conclusions: Ingredients for success (15 min)

WED, 16 NOVEMBER	

14h30	*Room 2 (E/F)*
	
	Workshop 2 – Legislation on cybercrime and capacity building in the Asia/Pacific region
	
	In recent years, reforms of legislation on cybercrime and electronic evidence have accelerated in the Asia/Pacific region, often with the Budapest Convention serving as a guideline to ensure compatibility with international standards. Legal reforms are accompanied by capacity building efforts. The aim of this workshop is to share good practices and discuss problems encountered as well as promote accession to the Budapest Convention. The workshop is co-organised by the Government of Japan.
	
	Moderator/s: Koichi Mizushima (Ambassador in charge of Cyber Policy, Ministry of Foreign Affairs) / Shinsuke Shimizu (Consul General of Japan in Strasbourg and Ambassador, Permanent Observer to the Council of Europe) / Jayantha Fernando (Director, ICTA, Sri Lanka)
	
	Rapporteur: Zahid Jamil (Pakistan)
	
	Secretariat: Manuel Almeida Pereira (Cybercrime Programme Office, Council of Europe)
	
	► Legislation on cybercrime and electronic evidence and rule of law safeguards
	
	- Tour de table/brain storming session: the current state of cybercrime legislation in the Asia/Pacific region (25 min)
	
	16h00-16h15
	Coffee break
	
	- Legislation on cybercrime in Japan (25 min):
	  - How did Japan amend cybercrime legislation to become a party to the Budapest Convention? (Mayumi Tsuboi, Attorney, International Affairs Division, Criminal Affairs Bureau, Ministry of Justice of Japan)
	  - Domestic practice (Fumitake Masukawa, Superintendent, Cybersecurity Office, National Police Agency, Japan)
	
	- Case studies, do's and don'ts (40 min)
	  - Panel with speakers from Pakistan, Philippines, Sri Lanka and Tonga
	  - Discussion
	
	- Discussion: The process – How to go about preparing cybercrime legislation? Who decides, who is involved, who takes the lead, what is the procedure? (30 min)
	
	► Capacity building: examples of good practice (45 min)
	
	- Capacity building projects on cybercrime in Japan (Fumitake Masukawa, Superintendent, Cybersecurity Office, National Police Agency, JAPAN)
	- Capacity building by the UN Office on Drugs and Crime (Neil J. Walsh, Senior Expert (Cyber and Emerging Crime), UNODC)
	- The experience of GLACY countries in Asia: Philippines, Sri Lanka and Tonga
	
	► Conclusions: How to support legal reforms and accession to the Budapest Convention in the Asia/Pacific region? (15 min)

WED, 16 NOVEMBER	

14h30	*Room 3 (E) – Chatham House Rules apply*
	
	Workshop 3 – Service provider/law enforcement cooperation on cybercrime and electronic evidence
	
	Some providers – in particular US service providers – may respond directly to lawful requests for subscriber information and traffic data by criminal justice authorities in other jurisdictions where they are offering a service. The T-CY Cloud Evidence Group has documented policies and practices in a background paper. In 2015, Parties to the Budapest Convention – other than the USA - sent more than 135,000 requests to six major providers with a response rate of some 60%. This workshop is to discuss how such cooperation could be further improved and put on a clearer legal basis.
	
	Moderator/s: Pedro Verdelho (Prosecutor, Portugal)
	
	Rapporteur: Markko Künnapu (Ministry of Justice, Estonia)
	
	Secretariat: Pierluigi Perri (Cybercrime Division, Council of Europe)
	
	► The voluntary cooperation model (90 min)
	
	- Policies and procedures by providers
	  - Panel Apple, Facebook, Google, Microsoft, Telecom Providers, EuroISPA
	- Experience of law enforcement
	  - Italy (Francesco Cajani, Deputy Public Prosecutor, High tech crime unit - Counter terrorism department, Milan)
	  - Portugal (Pedro Verdelho, Public Prosecutor)
	- Issues

16h00-16h15 *Coffee break*	► Solutions (75 min) - Proposals by Cloud Evidence Group - Proposals under consideration by European Union (Tjabbe Bos, Policy Officer European Commission) - Proposals by service providers - Discussion ► Conclusions: the way ahead (15 min)

THU, 17 NOVEMBER	
9h30	*Room1 (E/F/S/R)* **Workshop 4 – Terrorism and information technology: the criminal justice perspective** *Terrorist misuse of information technology may include cyberattacks against computer systems, including critical infrastructure, or their use for logistical purposes, including the planning of terrorist attacks. The dissemination – often via social media - of illegal contents, including threats, promotion of or incitement to terrorism, recruitment or training, xenophobia, racism or other forms of hate speech contributing to violent extremism, radicalisation and terrorism has increased significantly. The aim of the workshop is to review problems encountered from a criminal justice perspective and to discuss solutions, including improved cooperation with social media and other service providers.* Moderator/s: Catherine Smith (Australia) Rapporteur: Andrea Candrian (Deputy Head of Criminal Law, Federal Office of Justice, Switzerland) Secretariat: Marie Agha-Wevelsiep and Pierluigi Perri (Cybercrime Division, Council of Europe) ► Update on agreed upon international standards on terrorism (30 min) - Aspects of terrorism covered by the Budapest Convention on Cybercrime (T-CY Guidance Note) - Protocol to the Budapest Convention on Xenophobia and Racisms - Protocol to the Convention on Terrorism on foreign terrorist fighters (CETS 217) - European Convention on Offences relating to Cultural Property and the financing of terrorism - International standards by United Nation Counter-Terrorism Committee ► Terrorist use of ICT – major threats and difficulties encountered: the criminal justice perspective (90 min) - Examples of cyberattacks (Eric Freyssinet, Senior Advisor / Taskforce against cyberthreats, Ministry of Interior) - Regulating encryption - Cooperation in emergency situations ► Hate speech online (40 min) - Hate speech versus freedom of expression: from theory to judicial practice (Jennifer Daskal, Associate Professor, American University Washington College of Law - Rachael KONDAK, Adviser, Office of the Commissioner for Human Rights) - Cooperation with service providers and the development of code of conducts ► Conclusions (15 min)
11h00-11h15 *Coffee break*	

THU, 17 NOVEMBER	
9h30	*Room 2 (E/S/F)* **Workshop 5a – Legislation on cybercrime and electronic evidence in Africa** *Cybercrime is an increasing challenge for countries of Africa, but at present only some 20% of African States have cybercrime legislation in place while a further 25-30% are in the process of legislative reform. The Budapest Convention is serving as a guideline but African States also consider the African Union Convention on Cyber Security and Personal Data Protection adopted in Malabo in June 2014. The aim of this workshop is to share good practices but also information on problems encountered.* Moderator/s: Irene Kabua, Kenya Law Reform Commission Rapporteur: Patrick Mwaita (United Nations African Institute for the Prevention of Crime and the Treatment of Offenders, Uganda) Secretariat: Manuel Almeida Pereira (Cybercrime Programme Office, Council of Europe) ► The current state of cybercrime legislation in Africa: Update by participants from Africa countries (30 min) ► Stop and go: Problems encountered and solutions proposed to accomplish reforms – Discussion based on experience by participants from African countries (30 min) ► Budapest and Malabo Conventions: Complementarity? (30 min) - Presentation (Zahid Jamil, Pakistan) - Discussion
11h00-11h15 *Coffee break*	► Conclusions (5 min) **Workshop 5b – Cybercrime legislation in Latin America – the problem of procedural law** *Many countries of Latin America successfully adopted substantive criminal law on cybercrime in recent years but encountered difficulties with regard to procedural law powers. This has also delayed accession to the Budapest Convention. The aim of the workshop is to identify the reasons and possible solutions.* Moderator/s: Rodolfo Orjales (Chair, REMJA Working Group on Cybercrime, Organisation of American States) Rapporteur: Pablo Castro (Subdirector para Seguridad Internacional Ministerio de Relaciones Exteriores Dirección de Seguridad Internacional y Humana) Secretariat: Manuel Almeida Pereira (Cybercrime Programme Office, Council of Europe) ► The state of cybercrime legislation in Latin America (30 min) ► The question of procedural law (45 min) - Presentation of the problem (Marcos Salt, Argentina) - Discussion of solutions - Conclusions

THU, 17 NOVEMBER	
9h30	*Room 3 (E – workshop restricted to criminal justice authorities)* **Workshop 6 – International cooperation: workshop for 24/7 points of contact and MLA authorities** *Efficient international cooperation is essential for the investigation and prosecution of cybercrime and other offences involving electronic evidence. This includes police-to-police cooperation, mutual legal assistance, and expedited measures to preserve electronic evidence. The Cybercrime Convention Committee (T-CY) in December 2014 completed a detailed assessment of the functioning of the mutual legal assistance provisions and adopted a set of recommendations to make MLA more efficient, strengthen the role of 24/7 points of contact and provide for direct cooperation across borders. The final report of the T-CY Cloud Evidence Group also comprises recommendations on MLA. The aim of this workshop is to discuss follow up to these recommendations.* Moderator/s: Claudio Peguero (Director Planning, Development and International Cooperation, National Police, Dominican Republic) / Ioana Albani (Deputy Chief Prosecutor, DIICOT, Romania) Rapporteur: Aleksandra Tukisa (International Cooperation Bureau, State Police, Latvia) Secretariat: Giorgi Jokhadze (Cybercrime Programme Office of the Council of Europe) and Alexandru Frunza (Cybercrime Division, Council of Europe) ► Strengthening the role of 24/7 points of contact (draft guide, GLACY and EAP results) (90 minutes) - T-CY Recommendations of December 2014 – Claudio Peguero (Director Planning, Development and International Cooperation, National Police, Dominican Republic) / (Ioana Albani, Deputy Chief Prosecutor, DIICOT, Romania) - Contact points of Parties to the Budapest Convention, results of the ping test – Alexandru Frunza (Cybercrime Division, Council of Europe) - Requests sent/received (examples by Parties), good practices, problems encountered – CEAP Eastern Partnership country examples ; - G7 Network experience (Albert Rees, Senior Counsel International Programs Computer Crime & Intellectual Property Section, US and Gianluigi Umetelli, Chief Inspector, Italian National Police Italian judicial police) - Developing a best practice model for the preservation of data – Canada's experience (Gareth Sansom, Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice Canada) - Capacity building activities and Guide for 24/7 POC – Giorgi Jokhadze (Cybercrime Programme Office of the Council of Europe) - Experience of INTERPOL (Christophe Durand, Head of Strategy and Outreach IGCI) - Results of the EU funded project "Effective 24/7 Points of Contact: promotion of good practice" (Nigel Jones, Canterbury University). ► Rendering MLA more efficient (60 min) - T-CY Recommendations 2014 and findings of the Cloud Evidence Group (Gareth Sansom, Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice Canada) - EUROJUST role and tasks in fighting cybercrime (Peter Gouwy, Case Analysis Unit and Mieke de Vlaminck, Analyst, Case Analysis Unit) - Experience of UNODC (Olga Zudova, Senior Legal Officer) - Capacity building activities (Cybercrime@EAP II) – Eastern Partnership example - European Commission, European Investigation Order (EIO) and cross-border access to electronic evidence (Tjabbe BOS, Policy officer, DG Migration and Home Affairs) - Capacity building activities (Cybercrime@EAP II) – Eastern Partnership examples
11h00-11h15 *Coffee break*	

	► Octopus Community – Online tool on international cooperation (30 min) – Giorgi Jokhadze (Council of Europe)

THU, 17 NOVEMBER	
14h30	*Room1 (E/F/S/R – Live webcast)* **Workshop 7 – Seeking synergies: Policies and initiatives on cybercrime of international and private sector organisations** *An increasing number of public and private sector organisations are taking measures on cybercrime. This workshop offers a platform for organisations to present their initiatives. The aim is to favour synergies and multi-stakeholder interaction.* Moderator/s: Cécile Barayre (Economic Affairs Officer, E-Commerce and Law Reform Programme, UNCTAD) Rapporteur: Joyce Hakmeh (Chatham House) Secretariat: Alexandru Frunza (Cybercrime Division, Council of Europe) ► International organisations and their approaches to address cybercrime and cybersecurity - UNODC (Olga Zudova, Senior Legal Officer) - UNCTAD (Cécile Barayre, Economic Affairs Officer E-Commerce and Law Reform Programme) - ITU (Rosheen Awotar-Mauree, Cybersecurity Officer) - Commonwealth (Emma Thwaite, Assistant Legal Officer) - Organisation of American States (Belisario Contreras, Cyber Security Programme Manager) - World Bank (Seunghwan Park, Senior Counsel) - INTERPOL (Christophe Durand, Head of Strategy and Outreach, IGCI) - Council of Europe C-PROC Office (Matteo Lucchetti and Manuel de Almeida Pereira, project managers) - African Union Commission (Auguste Yankey, Senior Policy Officer, Infrastructure and Energy Division) ► Policies and initiatives developed by private sector organisations, national institutions and professional associations - Chatham House (Joyce HAKMEH, Fellow, International Security Department) - City of Milan (Walter VANNINI, Teacher at Municipality of Milan) - CYAN (Nour Eddine ElBouhati, Treasurer) - Evidence project (Mattia Epifani, Researcher) - GPEN (Esther George, Lead Cybercrime Consultant, TBC) - Le Net Expert (Denis Jacopini, Computer forensic expert) ► Conclusions: What synergies?
16h00-16h15 *Coffee break*	

THU, 17 NOVEMBER

14h30	*Room 2 (E/F)* **Workshop 8 – Targeting proceeds from crime online** *Worldwide, most cybercrime reported and investigated by criminal justice authorities is related to different types of fraud and other offences aimed at obtaining illegal economic benefits. Vast amounts of crime proceeds are thus generated – and often laundered – on the Internet and through the use of information and communication technologies (ICT). The challenge is to trace, seize and confiscate proceeds generated on online. The Council of Europe prepared a detailed study on this question on 2012, and in 2016, the Council of Europe and the European Union launched the iPROCEEDS project. INTERPOL, EUROPOL, the UN Office on Drugs on Crime, the Council of Europe and other organisations are developing training materials to link up financial, anti-money laundering and cybercrime investigations, often with a specific focus on "darkmarkets".* *The aim of this workshop is to share experience / good practices with respect to targeting crime proceeds online, including on training programmes.* Moderator/s: Dave O'Reilly (FTR Solutions) Rapporteur: Hein Dries-Ziekenheiner (Vigilo Consult) Secretariat: Mariana Chicu and Alin Tortolea (Cybercrime Programme Office of the Council of Europe) ► Criminal money flows on the Internet: defining the challenge (30 min) - Examples and typologies from Serbia and Turkey (Branko Stamenkovic, Special Prosecutor for High-Tech Crime of Serbia; Ömer Artun Aktimur, Financial Intelligence Unit (MASAK), Ministry of Finance of Turkey, Kürşad Başaran Basoglu, Cybercrime Department Turkish National Police) - Brain storming ► Public/private cooperation to target proceeds from crime online (45 min) Del Pillar and Francesca Cannas (National Crime Agency (NCA), UK) - Money Muling – case study - Business email compromise - NCA engagement with the Banking sector for trusted partnerships ► Building bridges: Financial investigators, financial intelligence units and cybercrime units (30 min) - Case study (Max Braun, Premier Substitute**,** FIU Luxemburg) - Interagency cooperation – examples of good practices (Fadil Abdyli, Chief of Cyber Crime Investigation Sector, Kosovo* Police, Meriton Shoshi, Financial Intelligence Unit of Kosovo*) ► Training programmes (60 min) - EMPACT (EUROPOL, INTERPOL, CEPOL, Council of Europe, ECTEG) (Christophe Landries, Federal Computer Crime Unit, Federal Police, Belgium) - UNODC (Neil J. Walsh, Senior Expert, Cyber and Emerging Crime) - INTERPOL/TNO - iPROCEEDS/Council of Europe ► Conclusions (15 min)
16h00-16h15 *Coffee break*	

*The designation is without prejudice to positions on status, and is in line with the ICJ Opinion on the Kosovo Declaration of Independence.

THU, 17 NOVEMBER	
14h30	*Room 3 (E) – Chatham House Rules apply* **Workshop 9 – Crime and jurisdiction in cyberspace: access to electronic evidence** *In the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations. In December 2014, the Cybercrime Convention Committee (T-CY) established a Cloud Evidence Working Group to explore solutions. The topic was also a priority of the Netherlands Presidency of the European Union. This workshop is to discuss the feasibility of solutions currently under consideration, including results of the Cloud Evidence Group.* Moderator/s: Erik Planken (Chair, Cybercrime Convention Committee, Ministry of Justice and Security, Netherlands) Rapporteur: Betty Shave (USA) Secretariat: Pierluigi Perri (Cybercrime Division, Council of Europe) ► Recap: Crime and evidence in the cloud – challenges (30 min) - Summary of "Challenges report" of Cloud Evidence Group - Comments by EUROJUST, INTERPOL, private sector ► Concepts of jurisdiction (30 min) - Introductory presentations - Jennifer Daskal (Associate Professor, American University Washington College of Law) - Comments ► Towards solutions (120 min) *16h00-16h15* *Coffee break* - Crossing-borders: jurisdiction in cyberspace – follow up to the NL Presidency of the European Union (Erik Planken, Senior Policy Advisor Cybercrime, Law Enforcement Department, Ministry of Justice - Discussion - Results of the Cloud Evidence Group of the Cybercrime Convention Committee – Presentation and discussion of: - Legal and practical measures to render MLA more efficient - Guidance Note on production orders (Article 18 Budapest Convention) - Domestic rules for production order for subscriber information - Practical measures for cooperation with providers - Protocol to the Budapest Convention ► Conclusions (15 min)

FRI, 18 NOVEMBER	
9h30	**Plenary** *Room 1 (E/F/S/R)* ► Results of workshops (45 min) - WS 1 – Capacity building (Esther George, United Kingdom) - WS 2 – Legislation in Asia/Pacific (Zahid Jamil, Pakistan) - WS 3 – Service provider/law enforcement cooperation (Markko Künappu, Estonia) - WS 4 – Terrorism and information technology (Andrea Candrian, Switzerland) - WS 5 – Legislation in Africa (Patrick Mwaita) and Latin America (Pablo Castro, Chile) - WS 6 – International cooperation (Aleksandra Tukisa, Latvia) - WS 7 – Synergies (Joyce Hakmeh, Chatham House) - WS 8 – Crime proceeds (Hein Dries-Ziekenheiner, Netherlands) - WS 9 – Crime and jurisdiction in cyberspace (Betty Shave, USA)

10h30-10h45
Coffee break
	► Human rights and rule of law in cyberspace: threats and safeguards (75 min)
	
	- Keynotes:
	  - Ravi Raj Yerrigadoo (Attorney General, Mauritius)
	  - Judge Robert Spano (European Court of Human Rights)
	
	- Comments by data protection community and civil society
	  - Jean-Philippe Walter (Vice-Chair Data Protection Committee T-PD)
	  - Romain Robert (Legal Officer, European Data Protection Supervisor)
	  - Greg Nojeim, (Director of Freedom, Security and Technology Project, Center for Democracy & Technology, Washington, USA)
	
	- Comments by criminal justice authorities – safeguards in practice
	  - Emmanuelle Legrand (Investigative judge, First instance court of Nanterre, France)
	  - Daniel Petrone (Juez Poder Judicial de la Nación/ Ministerio de Justicia y Derechos Humanos de la República, Argentina)
	  - Papa Assane Touré (Secrétaire général Adjoint du Gouvernement Primature du Sénégal)
	
	► Concluding session: Octopus take-aways (45 min)
	
	Moderator: Jan Kleijssen (Director of Information Society and Action against Crime, Council of Europe)
	
	- Panel discussion
	- Closing

13h00	*End of conference*