Octopus Conference 2018 Cooperation against Cybercrime

11 – 13 July 2018 Palais de l'Europe, Council of Europe, Strasbourg, France



Version 6 July 2018

Conference Programme

The Octopus Conference is part of the Cybercrime@Octopus project which is funded by voluntary contributions from Estonia, Hungary, Japan, Monaco, Romania, Slovakia, United Kingdom and USA as well as the budget of the Council of Europe.



www.coe.int/cybercrime

Programme overview



14h00 20h00 Social dinner THU, 12 JULY	Hemicycle (E/F/S/R) Opening session Criminal justice in cyberspace: key cl Introduction to the workshops	hallenges 2017/2019
20h00 Social dinner THU, 12 JULY	Criminal justice in cyberspace: key cl	hallenges 2017/2019
20h00 Social dinner THU, 12 JULY		hallenges 2017/2019
20h00 Social dinner THU, 12 JULY	Introduction to the workshops	
THU, 12 JULY		
Workshop sessions		
	Hemicycle (E/F/S/R)	Room 11 (E/S/F)
9h00	Workshop 1:	Workshop 2:
1	 Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention 	 Global state of cybercrime legislation: progress 2013 – 2018
12h30 – 14h00	Lunch break	
Workshop sessions	Hemicycle (E/F/S/R)	Room 11 (E/F/S)
14h00	Workshop 1 (cont'd):	Workshop 3:
	 Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention 	Capacity building on cybercrime and e- evidence: what impact?
FRI, 13 JULY		
Workshop sessions	Hemicycle (E/F/S/R)	Room 11 (E/F/S)
9h00	Workshop 4:	Workshop 5:
1	► WHOIS: What now?	 Cyberviolence: challenges and responses
12h30 – 14h00	Lunch break	
Plenary session	Hemicycle (E/F/S/R)	
14h00	Plenary:	
,	 Results of workshops 	
	 Futures: artificial intelligence and cyt Concluding panel 	percrime

Please note that Chatham House rules apply to permit open discussions throughout the Conference.

Detailed programme

WED, 11 JULY		
Plenary session	Hemicycle (E/F/S/R)	
14h00	Plenary	
	Opening session [14h00 – 14h45]	
	 Jan Kleijssen (Director of Information Society and Action against Crime, Council of Europe) Ursula Owusu-Ekuful (Minister of Communications, Ghana) Marcela Ordonez Fernandez (Minister Plenipotentiary, Coordinator of Crime Prevention, Ministry of Foreign Affairs, Colombia) Bessolé René Bagoro (Ministre de la Justice, des Droits Humains et de la Promotion Civique, Garde des Sceaux de Burkina Faso) Ronald Kay Warsal (Minister for Justice and Communication Services, Vanuatu) 	
	Criminal justice in cyberspace: key challenges 2017/2019	
	 Threats and responses: Is criminal justice up to the challenges? [14h45 - 15h45] Antonio Lopez Melgarejo (National Police of Spain) - <u>A 1 billion EUR cyber</u> 	
Coffee break 15h45- 16h00	 bank robbery Axel Petri (Senior Vice President, Group Security Governance, Deutsche Telekom) – TELCO perspective on e-evidence proposals Jean-Paul Laborde (Directeur du centre d'expertise sur la lutte contre le terrorisme, Titulaire de la Chaire Cybersécurité/cyberdéfense, St-Cyr, France) – Terrorism, cybercrime and e-evidence Daniel Grubb (Cyber Crime Policy, Home Office, UK) – the Budapest Convention in operation Discussion 	
	 Democracy under attack [16h00-16h45] Alexander Seger (Head of Cybercrime Division, Council of Europe) Simona Granata-Menghini (Deputy Secretary of the Venice Commission, Council of Europe) Gail Kent (Global Security Lead Public Policy, Facebook) 	
	 Cybercrime and electronic evidence: threats to human rights [16h45-17h30] Katitza Rodriguez (International Rights Director, Electronic Frontier Foundation, USA) Maryant Fernandez Perez (Senior Policy Adviser, European Digital Rights (EDRI), Brussels, Belgium) Andrea Tamietti (Deputy Registrar, Section IV, European Court of Human Rights, Council of Europe, Strasbourg) – ECtHR: <u>Benedik vs. Slovenia</u> Robert Golobinek (Head of Division, Ministry of Justice, Slovenia) 	
	Introduction to the workshops [17h30-18h00]	
	 Workshop moderators to briefly present the issues to be addressed in their workshops 	
19h00	Social Dinner	

THU, 12 JULY	
Workshop sessions	Hemicycle (E/F/S/R)
9h00	Workshop 1 – Evidence and jurisdiction in cyberspace: multi- stakeholder consultation on the Protocol to the Budapest Convention
	The Cybercrime Convention Committee (T-CY) decided in June 2017 to prepare a draft 2 nd Additional Protocol to the Budapest Convention on Cybercrime. Negotiations commenced in September 2017 and are expected to last until the end of 2019. The T-CY wishes to engage in close consultation with civil society, data protection organisations and industry during the drafting process in order to seek their views and benefit from their experience. This workshop will be an opportunity for such consultations. Further meetings will be organised as draft concepts and text become available. A <u>discussion guide</u> has been prepared to structure the workshop.
	Moderator/s: Cristina Schulman (Ministry of Justice, Romania) / Pedro Verdelho (Office of the Prosecutor General, Portugal)
	Rapporteur: Betty Shave (Consultant, USA)
Coffee break 10h45 - 11h00	Secretariat: Alexander Seger (Executive Secretary, Cybercrime Convention Committee, Council of Europe)
10145 - 11100	 Context: Rationale for the Protocol – Recap and recent developments Setting the scene Relevant international developments
	 EU proposals on e-evidence US CLOUD Act
	 Provisions for more efficient mutual legal assistance Introduction: <u>T-CY Recommendations 2014</u> and <u>follow up given</u> by Parties
	 Information and exchange of views on proposed provisions related to mutual legal assistance
	 Direct cooperation with providers across jurisdictions Voluntary disclosure [of subscriber information] by service providers Preservations requests
12h30 – 14h00	Lunch break
14h00	Workshop 1 (cont'd)
	 Direct cooperation with providers across jurisdictions Mandatory production orders
Coffee break	 Access to data in the cloud/"transborder access" to data Concepts of jurisdiction: Connecting factors
15h45 – 16h00	 The scope of Article 32 Budapest Convention Extending searches and other options and scenarios
	 Next steps and further consultations
18h00	End of day 2
101100-	

THU, 12 JULY	
Workshop sessions	Room 11 (E/F/S)
9h00	Workshop 2 – The global state of cybercrime legislation: progress and lessons learnt 2013 – 2018
	Specific legislation, consistent with human rights and rule of law requirements, is the basis for criminal justice action on cybercrime and electronic evidence. Many governments around the world have undertaken legal reforms during the past five years, often using the Budapest Convention on Cybercrime as a guideline. The adoption of substantive legislation to criminalize offences against and by means of computers and of procedural powers to permit the collection of electronic evidence is often the starting point for further capacity building activities. Measurable progress is being noted and important lessons can be drawn from this experience. The aim of this workshop is to review progress made worldwide during the past five years, including examples of good practices and problematic areas.
	Moderators: Zahid Jamil (Barrister-at-law, Jamil & Jamil, Pakistan) / Karuna Devi Gunesh-Balaghee (Ag Parliamentary Counsel, Attorney General's Office, Mauritius)
	Rapporteur: Jayantha Fernando (Legal Advisor/Program Director – Policy & eLeadership, ICT Agency of Sri Lanka)
	Secretariat: Giorgi Jokhadze (Project Manager, C-PROC, Council of Europe) / Ana Elefterescu (Project Officer, C-PROC)
Coffee break 10h45 – 11h00	From 2013 to 2018: overview of progress made in the adoption of legislation on cybercrime and electronic evidence [9h00 - 9h30]
	 Preliminary results of a survey by the Cybercrime Programme Office of the Council of Europe (C-PROC) Discussion
	 Substantive criminal law [9h30 – 10h30]
	 Introduction: Budapest Convention requirements for substantive law (Zahid Jamil)
	 Examples- short presentations by the countries: (15 min): Botswana (Khursheed Rossenkhan, Attorney General's Chambers) (TBC) China (Shenkuo WU, CCLS & Law School, Beijing Normal University, Senior Consultant of United Nations for Cybersecurity and Cybercrime issues, Consultant of Supreme Court of People's Republic of China, Head of Research Centre of Internet Society of China) TBC Singapore (Kannan Gnanasihamani, Attorney-General's Chambers) (TBC)
	 Problems encountered and risks to human rights – open discussion with countries participating in the workshop on: Freedom of speech and broadly defined criminalization of conduct online

	Criminal procedure law: law enforcement powers to secure electronic
	evidence [10h30-10h45, 11h00-12h00]
	- Focus on production orders:
	 Introduction on the recent T-CY Guidance Note on Article 18 of the Convention (Karuna Devi Gunesh-Balaghee)
	 Implementing production orders in national law: examples of good practices
	 Production orders for subscriber information: Dynamic versus static IP addresses – <u>Benedik vs. Slovenia:</u>
	Introduction by Marko Juric, University of Zagreb, Croatia and C-PROC) Comments by Robert Golobinek (Ministry of Justice, Slovenia)
	 Session on rule of law safeguards in the context of procedural powers of the Budapest Convention (Marko Juric)
	- Introduction: Results of Article 15 Safeguards Study in the Eastern
	Partnership region (update 2018)
	 Discussion on implications of court decisions (domestic courts, Court of Justice of the European Union, European Court of Human Rights) regarding data retention, WHOIS data, interception and surveillance
	powers and of new data protection rules (Convention 108+, EU General
	Data Protection Regulation) on procedural powers to secure electronic evidence
	► How to ensure completion of legislative reforms? [12h00-12h20]
	 Open discussion: how to "sell" good cybercrime legislation to decision makers?
	► Conclusions [12h20-12h30]
12h30 – 14h00	Lunch break

THU, 12 JULY	
Workshop sessions	Room 11 (E/F/S)
14h00	Workshop 3 – Capacity building on cybercrime and e-evidence: what impact?
	Capacity building is considered one of the most effective means to address the challenges of cybercrime and electronic evidence. Based on broad international consensus, governments and international organisations, but also civil society and private sector initiatives in recent years have made resources available and supported programmes in all regions of the world to strengthen legislation, provide training to criminal justice officials, promoted public/private cooperation and make international cooperation more efficient. The aim of this workshop is to draw lessons from the experience so far: What has been the impact of capacity building on cybercrime and e-evidence in recent years? Have projects made a difference?
	Moderator: Panagiota-Nayia Barmpaliou (Attorney-at-Law and Cyber Policy Expert, Greece)
Coffee break 15h45 – 16h00	Rapporteur: George-Maria Tyendezwa (Assistant Director, Head, Cybercrime Prosecution Unit, Federal Ministry of Justice, Nigeria)
	Secretariat: Marie Agha-Wevelsiep (Project Manager, CyberSouth, C-PROC, Council of Europe) / Manuel de Almeida Pereira (Project Manager, GLACY+ Project, C-PROC, Council of Europe)
	Introduction and objective of the workshop [14h00-14h15]
	 A case for evaluating impact: why are metrics important, why bother about impact, how to avoid "dead aid"? Introduction (Panagiota-Nayia Barmpaliou) Key note (Zahid Jamil, Barrister-at-Law, Pakistan)
	► How to measure impact [14h15-15h40]
	 What tools and systems do organisations have in place to ensure and measure impact in projects on cybercrime? Short presentations by the following institutions/experts followed by discussion: David E. Satola (Lead Counsel, Technology & Innovation, <u>World Bank</u>) Wouter Veenstra (Manager Outreach and Partnership, <u>GFCE</u>) Patryk Pawlak (Brussels Executive Director, <u>EU-ISS</u>)
	 What are the benchmarks against which to design objectives and expected results and against which to determine impact? (Discussion moderated by Panagiota-Nayia Barmpaliou): Goals and actions foreseen in policy/strategic objectives or cybercrime/security Legislation = Budapest Convention; public/private cooperation Law enforcement capacities = number of investigations; measuring law enforcements' cybercrime outputs
	Short presentations by the following institutions/experts: - Cristos Velasco (External Lecturer at the DHBW University, Founder and Executive Director of Ciberdelincuencia.Org and Evidencia Digital.Lat

 Germany) Hania Helweh (Judge, Cybercrime Focal Point, Ministry of Justice, Lebanon) Henry Bryers (Senior Manager – Threat Response, National Cybercrime Unit, National Crime Agency (NCA), United Kingdom) Karuna Devi-Gunesh (Ag. Parliamentary Counsel, Attorney General's Office, Mauritius) Albert Antwi-Boasiako (National Cyber Security Policy and Strategic Advisor, Ministry of Communications, Ghana) The problem of casual link: how do we know that impact is due to project interventions?
interventions?
 Introduction (Panagiota-Nayia Barmpaliou) Discussion
Impact of projects: case studies [16h00 – 17h00]
 How is impact determined in concrete projects? Introductory presentations followed by discussions: Example UNODC project (Neil J. Walsh, Chief, Cybercrime and Anti-Money Laundering Section, <u>UNODC</u>) Example <u>GLACY+ (</u>Manuel de Almeida Pereira, Council of Europe)
 What is the main risks adversely affecting impact? Introduction (Panagiota-Nayia Barmpaliou) Discussion
Lessons learnt: Ensuring impact in project design and implementation [17h00 - 18h00]
Brainstorming session (moderated by Panagiota-Nayia Barmpaliou and preliminary considerations by the Rapporteur (George-Maria Tyendezwa): - Good and bad lessons learnt? - Take-aways for better projects and impact in the future?
18h00 End of day 2

FRI, 13 JULY	
Workshop sessions	Hemicycle (E/F/S/R)
9h00	Workshop 4 - WHOIS: What now?
Coffee break 10h45 – 11h00	For many years, public access to WHOIS data has been an important tool for criminal justice authorities to identify registrants of websites misused for criminal purposes. For many years, questions regarding the compatibility of this public WHOIS register with data protection requirements have also been raised. In view of the European Union's General Data Protection Regulation (GDPR), ICANN – the organisation responsible for Internet Protocol address space allocation and management of the domain name system – put in place <u>Temporary Specification for gTLD Registration Data</u> effective 25 May 2018 which restricts access to the part of WHOIS information considered personal data. <u>Consultations have been underway for some time</u> to find solutions to permit access to WHOIS data for law enforcement and other legitimate purposes while at the same time meeting data protection requirements. The purpose of this workshop is to help stakeholders obtain a better understanding of issues at stake in order to make informed contributions to solutions.
	Moderators: Jayantha Fernando (Director/Legal Advisor, ICT Agency, Sri Lanka)
	Rapporteur: Tjabbe Bos (Policy Officer Cybercrime, European Commission)
	Secretariat: Matteo Lucchetti (Project Manager, C-PROC, Council of Europe)
	What is WHOIS and why does it matter? [9h00 - 10h00]
	 Background, what is WHOIS? Tjabbe Bos (Policy Officer Cybercrime, European Commission)
	 The entry into force of the GDPR: WHOIS before and after 25 May 2018 Peter Kimpian (Data Protection Unit, Council of Europe) Elena Plexida (Government and IGOs Engagement Sr Director, ICANN)
	- The current situation
	 Caroline Greer (European Public Policy, Cloudflare)
	 WHOIS in cybercrime investigations – Use case Gregory Mounier (Head of Outreach and Prevention – European Cybercrime Center EC3, Europol)
	– Q&A (15 min)
	► Concerns [10h00 - 11h30]
	 Data protection and civil society: protection of personal data and compliance with relevant standards Peter Kimpian (Data Protection Unit, Council of Europe) Representative from an EU DPA [TBC]
	 ICANN and contractual obligations for service providers Elena Plexida (Government and IGOs Engagement Sr Director, ICANN)

	 Registrars and registries
	 Caroline Greer (European Public Policy, Cloudflare)
	 Spencer Payton (Senior Internet Resource Analyst, RIPE Network Coordination Centre)
	 Criminal justice and cyber security organisations: WHOIS "gone dark"? Erica O'Neil (Assistant Deputy Chief for Computer Crime, Computer Crime and Intellectual Property Section, United States Department of Justice) Jaap Van Oss (Senior Expert Cybercrime, Police, The Netherlands) Peter Cassidy/ Pat Cain (Secretary General/ Resident Research Fellow, Anti-Phishing Working Group)
	– Q & A
► 5	Solutions under consideration [11h30 – 12h00]
	 Layered access and accreditation system for legitimate users
	- Elena Plexida (Government and IGOs Engagement Sr Director, ICANN)
	 Public Safety and LEAs
	 Tjabbe Bos (Policy Officer Cybercrime, European Commission)
	 Gregory Mounier (Head of Outreach and Prevention – European Cybercrime Center EC3, Europol)
	 Erica O'Neil (Assistant Deputy Chief for Computer Crime, Computer Crime and Intellectual Property Section, United States Department of Justice)
	- Private sector
	 Peter Cassidy/ Pat Cain (Secretary General/ Resident Research Fellow, Anti-Phishing Working Group)
► 1	Fhe way ahead [12h00 – 12h30]
	- Open discussion
Lunc	h break

FRI, 13 JULY	
Workshop sessions	Room 11 (E/F/S)
9h00	Workshop 5 – Cyberviolence: challenges and responses
	Acts of violence against individuals committed or facilitated by information and communication technologies ("cyberviolence") have become a primary concern for societies and individuals. Although cyberviolence has existed for some years, its specific forms seem to have only recently begun to be identified and understood. Most countries are struggling to recognize the different facets of the problem and to address them in domestic law. The aim of the workshop is to review challenges from a criminal justice perspective and to discuss domestic and international responses, including improved cooperation and possible synergies. This includes better use of the tools available under the Budapest, Lanzarote and Istanbul Conventions of the Council of Europe, as well as the Protocol on Xenophobia and Racism to the Budapest Convention.
	Moderator/s: Betty Shave, USA
	Rapporteur: Briony Daley Whitworth (Department of Home Affairs, Australia)
<i>Coffee break 10h45 – 11h00</i>	Secretariat: Nina Lichtner and Mariana Chicu (Cybercrime Division, Council of Europe)
	Concepts of cyberviolence:
	 Defining cyberviolence: Gareth Sansom (T-CY Bureau member, Director of Technology and Analysis, Criminal Law Policy Section, Department of Justice, Canada) Discussion
	National and international experience and responses to cyberviolence:
	 The threat and impact of cyberviolence: short presentations followed by discussions Aura Freeman (Senior Campaigner, Global Campaigns Team, Amnesty International) Maria José Castello Branco (Lanzarote Convention Bureau Member) Daniela Pichler (Policy and Campaigns Director, European Women's Lobby) Discussion on the following topics What incidents are you seeing in your country? What are the trends? Who are the victims?
	 Case studies on domestic legislation, policies, strategies and other responses: Canada: Legislative approach to cyberbullying (Gareth Sansom, Department of Justice, Canada) Serbia: Case study on child abuse materials and coercion (Tatjana Vasiljevic, Special Cybercrime Prosecution Office, Serbia) Senegal (Papa Assane Touré, Magistrat, Secrétaire général Adjoint du Gouvernement, Primature) [TBC]

	 International responses:
	- ECtHR case-law on cyberviolence (Robert Spano, Judge, President of
	Section II, European Court of Human Rights)
	 Role of the Lanzarote Convention
	(Christel De Craim, Vice-Chair, Lanzarote Convention Committee,
	Maria José Castello Branco, Lanzarote Convention Bureau Member)
	 Role of the Istanbul Convention (representative of GREVIO [TBC])
	- Role of the Budapest Convention and the Protocol on Xenophobia and
	Racism (Gareth Sansom, T-CY Bureau member)
	 Role of service providers
	 Maximilian Schubert (Vice President, EuroISPA)
	- Acadia Senese (Corporate Counsel, Law Enforcement and Information
	Security, Google)
	Lessons learnt: good practices and challenges
	 Participants' advice to other countries
	 Participants' goals for their own countries
	 Participants' advice to victims
	Conclusions: What synergies?
12h30 – 14h00	Lunch break

FRI, 13 JULY	
Plenary session	Hemicycle (E/F/S/R)
14h00	Plenary
	Results of workshops [14h00-14h30]
	 Workshop rapporteurs to present outcome of each workshop
	► Futures: Artificial intelligence and cybercrime [14h30-15h45]
	 The rapid progress of artificial intelligence and machine learning raises fundamental questions on the future of humanity but also specific questions regarding benefits and risks related to cybercrime and criminal justice. The purpose of this panel is to discuss what we need to do today to prepare for the future of AI: AI and machine learning: what is this all about? What are the implications for cybercrime and criminal justice: AI to improve cybersecurity, and facilitate the detection, investigation and attribution of cybercrime? AI to further automate cybercrime (scanning systems for exploiting vulnerabilities, social engineering/ID theft; autonomous cybercrime by machines)? AI, cybercrime and the law: Who is liable for decisions made and crime committed by machines and neural networks? What ethical standards for the use of AI in criminal justice?
	- Al and cyberchine. How to prepare for the future:
	Moderator: – Jan Kleijssen (Director, Information Society and Action against Crime, DG 1, Council of Europe)
	 Panellists: Rebekah Overdorf (Department of Electrical Engineering, KU Leuven, Belgium) Claudia Peersman (Bristol Cyber Security Group, University of Bristol, UK) Pavel Gladyshev (University College Dublin, Ireland) Pavan Duggal (Advocate, Supreme Court of India, Chairman International Commission on Cyber Security Law)
	Concluding panel [16h00 – 17h00]
	 Estela Bernabe (Justice, Supreme Court of the Philippines) Mamadú Iaia Djalo (Ministre de la Justice, Guinea-Bissau) Mohamed R. Swaray (Minister of Information and Communication, Sierra Leone) Gabriel Juarez Lucas (Deputy Minister for Information and Communication Technologies, Guatemala) Agni Prasad Kharel (Attorney General, Nepal)
17h00	End of conference