Conférence Octopus 2016

Coopération contre la cybercriminalité

16 – 18 novembre 2016

Palais de l'Europe, Conseil de l'Europe, Strasbourg, France

Version 16 novembre 2016

Projet

Programme de la Conférence

La conférence Octopus fait partie du projet Cybercrime@Octopus financé par les contributions volontaires de l'Estonie, du Japon, de Monaco, de la Roumanie, du Royaume-Uni, des Etats-Unis d'Amérique et de Microsoft ainsi que du budget du Conseil de l'Europe. L'Estonie, le Japon et les Etats-Unis d'Amérique ont fait une contribution volontaire spécifique pour cette conférence Octopus.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Aperçu du programme

MER, 16 NOVEMBRE			
Plenary session	*Hemicycle*		
9h00	Session spéciale: CONVENTION DE BUDAPEST – 15e ANNIVERSAIRE (anglais/français/russe/espagnol)		
Ateliers	*Salle 1 (EN/FR/ES/RU)*	*Salle 2 (EN/FR)*	*Salle 3 (EN)*
14h30	Atelier 1: ► Renforcement des capacités en cybercriminalité: les bonnes pratiques, les réussites et les enseignements tirés	Atelier 2: ► Législation en matière de cybercriminalité et de preuve électronique en Asie/Pacifique	Atelier 3: ► Coopération entre fournisseurs de service et services répressifs en cybercriminalité et preuve électronique
20h00 Diner dans un restaurant alsacien			
JEU, 17 NOVEMBRE			
Ateliers	*Salle 1 (EN/FR/ES/RU)*	*Salle 2 (EN/S/F)*	*Room 3 (EN)*
9h30	Atelier 4: ► Terrorisme et technologie de l'information: la perspective de la justice pénale	Atelier 5: ► Législation en matière de cybercriminalité et de preuve électronique en - Afrique - Amérique latine	Atelier 6: ► Coopération internationale: atelier pour les autorités des points de contact 24/7 et les autorités d'entraide judiciaire
Ateliers	*Salle 1 (EN/FR/ES/RU)*	*Salle 2 (EN/FR)*	*Salle 3 (EN)*
14h30	Atelier 7: ► A la recherche des synergies: politiques et initiatives en cybercriminalité des organisations internationales et du secteur privé	Atelier 8: ► Cibler les revenus des activités criminelles en ligne	Atelier 9: ► Criminalité et juridiction dans le cyberespace : accès à la preuve électronique
VEN, 18 NOVEMBRE			
Session plénière	*Salle 1 (EN/FR/ES/RU)*		
9h30	Plenière: ► Les résultats des ateliers ► Panels: - Criminalité et preuves dans le cloud: quelle est la suite? - Perspective – Cybercriminalité en 2026 - Les actions en cybercriminalité dans mon pays: comment faire la différence? ► Conclusions		
13h00	*Fin de la conférence*		

Programme détaillé

MER, 16 NOVEMBRE	
Session plénière	*Hemicycle (anglais/français/russe/espagnol– Live webcast)*
9h00	**Session spéciale: CONVENTION DE BUDAPEST– 15e ANNIVERSAIRE** *La Convention de Budapest sur la cybercriminalité a été ouverte à la signature en 2001 et quinze ans plus tard, demeure l'instrument international le plus pertinent. Cette session a pour objet d'examiner les réalisations accomplies à ce jour et de débattre de l'évolution ultérieure de la Convention de Budapest, à la lumière des défis et des nouvelles menaces.* ► Ouverture (9h00 – 9h20) - Thorbjørn Jagland (Secretary General of the Council of Europe) - Deposit of instrument of accession by Andorra ► Impact et potentiel de la Convention de Budapest (9h20-10h00) Président: Philippe Boillat (Directeur Général Droits de l'Homme et Etat de droit) - 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 ► Panel: Cybercriminalité– Les perspectives internationales (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: Les perspectives du secteur privé en matière de cybercriminalité et Etat de droit (11h00-11h40) - Google - Microsoft ► L'Etat de droit dans le cyberspace: le problème de l'exécution (11h40-12h15) - Maria Elvira Tejada de la Fuente (Chief, Cybercrime Prosecution Office, Spain) - Yvonne Atakora Obuobisa (Director of Public Prosecutions, Ghana) ► La Convention de Budapest: passé, présent, future – le point de vue des fondateurs et partisans (12h15 – 13h00) - Table ronde: Rik Kaspersen (Netherlands), Betty Shave (USA), Pedro Verdelho (Portugal), Martha Stansell-Gamm (USA) ► Conclusions
Pause café 10h45-11h00	
13h00	*Pause déjeuner*
MER, 16 NOVEMBRE	

14h30	*Salle 1 (Langues: (anglais/français/russe/espagnol – Retransmission directe)* **Atelier 1 –Renforcement des capacités en cybercriminalité : les ingrédients de la réussite** *Le renforcement des capacités est devenu l'approche internationale privilégiée pour relever les défis en cybercriminalité et preuve électronique. Cela se reflète, entre autres, par la mise en place du Bureau de Programme sur la cybercriminalité du Conseil de l'Europe (C-PROC) en Roumanie (avril 2014), par le résultat du Congrès des Nations Unies sur la Prévention du Crime et de la Justice pénale (Qatar, avril 2015), par la Conférence mondiale de l'espace Cyber (la Haye, avril 2015), par la création du Global Forum for Cyber Expertise (GFCE) et par les politiques et les programmes d'un certain nombre d'organisations internationales.* *L'objet de cet atelier est d'identifier les ingrédients de la réussite, l'impact et le développement durable des programmes de renforcement des capacités.* Modérateur (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) Secrétariat: Matteo Lucchetti (Cybercrime Programme Office, Council of Europe)
16h00-16h15 *Pause café*	► Panel: Que signifie renforcer les capacités et qu'est-ce qui fait la réussite d'un projet de renforcement des capacités? (45 min) ► Actualité: Aperçu des nouveaux projets et bonnes pratiques (45 min) ► Panel: Comment mettre en place des programmes de formation durable pour la justice pénale ? (45 min) ► Panel: La coopération public/privé pour le renforcement des capacités – Comment cela fonctionne ? (45 min) ► Conclusions: ingrédients pour la réussite (15 min)

MER, 16 NOVEMBRE	

14h30	*Salle 2 (EN/FR)*
	
	Atelier 2 – Législation en matière de cybercriminalité et de preuve électronique en Asie/Pacifique
	
	Ces dernières années, les réformes législatives sur la cybercriminalité et la preuve électronique se sont accélérées dans la région Asie/Pacifique, souvent en utilisant la Convention de Budapest comme ligne directrice afin d'assurer la compatibilité avec les normes internationales. Les réformes juridiques se sont accompagnées par des efforts de renforcement de capacité. Cet atelier vise à partager les bonnes pratiques et discuter des problèmes rencontrés ainsi que de promouvoir l'adhésion à la Convention de Budapest. L'atelier est organisé conjointement avec le gouvernement du Japon.
	
	Modérateurr/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)
	
	Secrétariat: Manuel Almeida Pereira (Cybercrime Programme Office, Council of Europe)
	
	► Législation en cybercriminalité et preuve électronique et les garanties de l'Etat de droit
	
	- Tour de table/session de brain storming: l'état de la législation en cybercriminalité dans la région Asie/pacifique (25 min)
	
	- Législation en cybercriminalité au Japon (25 min):
	  - Comment le Japon a réformé sa législation afin de devenir Partie à la Convention de Budapest? (Mayumi Tsuboi, Attorney, International Affairs Division, Criminal Affairs Bureau, Ministry of Justice of Japan)
	  - Pratique au niveau national (Fumitake Masukawa, Superintendent, Cybersecurity Office, National Police Agency, Japan)
	
	- Etudes de cas, à faire et à ne pas faire (40 min)
	  - Panel avec des conférenciers du Pakistan, des Philippines, du Sri Lanka et de Tonga
	  - Discussion
	
	- Discussion: le processus– Comment préparer une législation en matière de cybercriminalité? Qui décide, qui est impliqué, qui prend la direction des opérations et quelle est la procédure? (30 min)
	
	► Renforcement des capacités: exemples de bonnes pratiques (45 min)
	
	- Renforcement des capacités en cybercriminalité au Japon (Fumitake Masukawa, Superintendent, Cybersecurity Office, National Police Agency, JAPAN)
	- Renforcement des capacités par le UN Office on Drugs and Crime (Neil J. Walsh, Senior Expert (Cyber and Emerging Crime), UNODC)
	- L'expérience des pays GLACY en Asie: les Philippines, le Sri Lanka et Tonga
	
	► Conclusions: Comment appuyer les réformes législatives et adhérer à la Convention de Budapest dans la région Asie/pacifique? (15 min)

16h00-16h15 *Pause café*	

MER, 16 NOVEMBRE	
14h30	*Salle 3 (E) – les règles du Chatham House sont en vigueur* **Atelier 3 – Coopération entre fournisseurs de service et services répressifs en cybercriminalité et preuve électronique** *Certains fournisseurs – en particulier américains fournisseurs de services – peuvent répondre directement aux demandes légitimes pour les données relatives à l'abonné et les données de trafic, provenant des autorités de justice pénale dans d'autres juridictions où ils offrent un service. Le Cloud Evidence Group du T-CY a consigné les politiques et les pratiques dans un document d'information. En 2015, les Parties à la Convention de Budapest – autres que les Etats-Unis d'Amérique. – se sont adressées à plus de 135 000 reprises aux six principaux fournisseurs avec un taux de réponse d'environ 60 %. Cet atelier doit permettre d'examiner comment cette coopération pourrait être encore améliorée et grâce à une base juridique plus claire.* Modérateur/s: Pedro Verdelho (Prosecutor, Portugal) Rapporteur: Markko Künnapu (Ministry of Justice, Estonia) Secrétariat: Pierluigi Perri (Cybercrime Division, Council of Europe)

16h00-16h15
Pause-café
	► Le modèle de coopération volontaire (90 min)
	
	- Les politiques et procédures des fournisseurs
	  - Panel Apple, Facebook, Google, Microsoft, fournisseurs de téléphonie
	- Expérience des forces de l'ordre
	  - Italie (Francesco Cajani, Deputy Public Prosecutor, High tech crime unit - Counter terrorism department, Milan)
	- Les problèmes
	
	► Les solutions (75 min)
	- Les propositions du Cloud Evidence Group
	- Les propositions examinées par l'Union européenne (Tjabbe Bos, Policy Officer European Commission)
	- Les propositions des fournisseurs de service
	- Discussion
	
	► Conclusions: la voie à suivre (15 min)

JEU, 17 NOVEMBRE	
9h30	*Salle 1 (EN/FR/ES/RU– retransmission en direct)* Atelier 4 – ► Terrorisme et technologie de l'information: la perspective de la justice pénale *L'utilisation à des fins terroristes des technologies de l'information peut comprendre des cyberattaques contre des systèmes informatiques, y compris les infrastructures critiques, ou leur utilisation à des fins logistiques, y compris pour la planification d'attentats terroristes. La diffusion – souvent via les médias sociaux - des contenus illégaux, y compris la menace, la promotion ou l'incitation au terrorisme, le recrutement ou la formation, la xénophobie, le racisme ou d'autres formes de discours de haine qui contribuent à la radicalisation, au terrorisme et à l'extrémisme violent a considérablement augmenté. L'atelier vise à examiner les problèmes rencontrés du point de vue de la justice pénale et de discuter des solutions, notamment l'amélioration de la coopération avec les médias sociaux et autres fournisseurs de services* Modérateur/s: Catherine Smith (Australia) Rapporteur: Andrea Candrian (Deputy Head of Criminal Law, Federal Office of Justice, Switzerland) Secrétariat: Marie Agha-Wevelsiep and Pierluigi Perri (Cybercrime Division, Council of Europe) ► Actualité sur les standards internationaux en matière de terrorisme (30 min) - Les aspects du terrorisme traités par la Convention de Budapest sur la cybercriminalité (Note d'orientation du T-CY) - Le Protocole de la Convention de Budapest sur la Xénophobie et le racisme - Le Protocole additionnel à la Convention du Conseil de l'Europe pour la prévention du terrorisme sur les combattants terroristes étrangers (CETS 217) - Les standards internationaux, United Nation Counter-Terrorism Committee ► L'usage terroriste des TIC – les risques importants et les difficultés rencontrées: la perspective de la justice pénale (90 min) - Exemples de cyberattaque - Réglementer le cryptage - La coopération dans les situations d'urgence ► Le discours de haine en ligne (40 min) - Discours de haine et liberté d'expression: de la théorie à la pratique juridique - Coopération avec les fournisseurs de service et le développement des codes de conduites. ► Conclusions (15 min)
11h00-11h15 *Coffee break*	

JEU, 17 NOVEMBRE	
9h30	*Salle 2 (E/S/F)* **Atelier 5a – Législation en matière de cybercriminalité et de preuve électronique en Afrique** *La cybercriminalité est un défi croissant pour les pays d'Afrique, mais à l'heure actuelle, seuls 20 % des États africains a une législation sur la cybercriminalité en place tandis que 25-30 % d'autres sont dans un processus de réforme législative. La Convention de Budapest peut servir d'orientation. Toutefois les États africains prennent en considération également la Convention de l'Union africaine sur la Cyber-sécurité et la Protection des données personnelles adoptée à Malabo en juin 2014. L'objectif de cet atelier est de partager les bonnes pratiques mais aussi les informations sur les problèmes rencontrés* Modérateur: Irene Kabua, Kenya Law Reform Commission Rapporteur: Patrick Mwaita (United Nations African Institute for the Prevention of Crime and the Treatment of Offenders, Uganda) Secrétariat: Manuel Almeida Pereira (Cybercrime Programme Office, Council of Europe) ► L'état de la législation en cybercriminalité en Afrique: actualité par les participants des pays africains (30 min) ► "Stop and go": les problèmes rencontrés et les solutions proposée afin d'effectuer des réformes– Discussions basées sur l'expérience des participants des pays africains (30 min) ► Les Conventions de Budapest et Malabo: Complémentarité? (30 min) - Présentation (Zahid Jamil, Pakistan) - Discussion ► Conclusions (5 min) **Atelier 5b – Législation en matière de cybercriminalité et de preuve électronique en Amérique latine– le problème du droit procédural** *De nombreux pays d'Amérique latine ont adopté avec succès une législation pénale en matière cybercriminalité ces dernières années mais rencontrent des difficultés en ce qui concerne les pouvoirs de la procédure pénale. Cette situation a aussi retardé l'adhésion à la Convention de Budapest. L'atelier vise à identifier les raisons et les solutions possibles.* Modérateur/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) Secrétariat: Manuel Almeida Pereira (Cybercrime Programme Office, Council of Europe) ► L'état de la législation en matière de cybercriminalité en Amérique latine (30 min) ► La question du droit procédural (45 min) - Exposé du problème (Marcos Salt, Argentina) - Discussion des solutions - Conclusions
11h00-11h15 *Pausé café*	

JEU, 17 NOVEMBRE	
9h30	*Salle 3 (E – atelier réservé aux autorités de la justice pénale)* **Atelier 6 – Coopération internationale: atelier pour les autorités des points de contact 24/7 et les autorités d'entraide judiciaire** *Une coopération internationale efficace est essentielle pour les enquêtes et les poursuites contre la cybercriminalité et autres délits impliquant la preuve électronique. Cela comprend la coopération police-à-police, l'entraide judiciaire et les mesures de conservation rapide de la preuve électroniques. Le Comité de la Convention sur la cybercriminalité (T-CY) en décembre 2014 a terminé une évaluation détaillée du fonctionnement des dispositions d'assistance juridique mutuelle et a adopté une série de recommandations visant à accroître l'efficacité de l'entraide judiciaire, à renforcer le rôle des points de contact 24/7 et y prévoit une coopération directe au-delà des frontières. Le rapport final du Cloud Evidence Group (T-CY) comprend également des recommandations sur l'entraide judiciaire. L'objet de cet atelier est de discuter le suivi de ces recommandations.* Modérateur/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) Secrétariat: Giorgi Jokhadze (Cybercrime Programme Office of the Council of Europe) and Alexandru Frunza (Cybercrime Division, Council of Europe) ► Renforcer le rôle des points de contact 24/7 (Guide provisoire, résultats de GLACY et EAP) (90 minutes) - Recommendations du T-CY en décembre 2014 – Claudio Peguero (Director Planning, Development and International Cooperation, National Police, Dominican Republic) / (Ioana Albani, Deputy Chief Prosecutor, DIICOT, Romania) - Points de contact des Parties à la Convention de Budapest, résultats du test ping – Alexandru Frunza (Cybercrime Division, Council of Europe) - Requêtes envoyées et reçues (exemples par les Parties), les bonnes pratiques, les problèmes rencontrés– CEAP exemple des pays du partenariat oriental ; - L'expérience du réseau G7 (Albert Rees, Senior Counsel International Programs Computer Crime & Intellectual Property Section, US and Gianluigi Umetelli, Chief Inspector, Italian National Police Italian judicial police) - Développer un modèle pratique pour la conservation des données – l'expérience du Canada (Gareth Sansom, Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice Canada) - Activités de renforcement des capacités et Guide pour les points de contact 24/7 – Giorgi Jokhadze (Cybercrime Programme Office of the Council of Europe) - Expérience d'INTERPOL (Christophe Durant, Head of Strategy and Outreach IGCI) - Les Résultats du projet UE "Efficacité des points de contact: promotion de bonnes pratiques" (Nigel Jones, Canterbury University). ► Rendre l'entraide judiciaire plus efficace (60 min) - Recommandations du T-CY de 2014 et les résultats du Cloud Evidence Group (Gareth Sansom, Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice Canada) - Les développements à EUROJUST (Peter Gouwy, Case Analysis Unit and Mieke de Vlaminck, Analyst, Case Analysis Unit) - L'expérience de l'UNODC (Olga Zudova, Senior Legal Officer) - Les activités de renforcement des capacités (Cybercrime@EAP II) – exemples des pays du Partenariat Oriental ► Octopus Community – Outil en ligne sur la coopération internationale (30 min) – Giorgi Jokhadze (Council of Europe)
11h00-11h15 *Coffee break*	

JEU, 17 NOVEMBRE	
14h30	*Salle 1 (EN/FR/ES/RU – Retransmission directe)* Atelier 7 – A la recherche des synergies: politiques et initiatives en cybercriminalité des organisations internationales et du secteur privé *Un nombre croissant d'organisations publiques et privées prennent des mesures en matière de cybercriminalité. Cet atelier offre une plate-forme aux organisations afin de présenter leurs initiatives. L'objet est de favoriser les synergies et l'interaction des multiples parties prenantes.* Modérateur/s: Cécile Barayre (Economic Affairs Officer, E-Commerce and Law Reform Programme, UNCTAD) Rapporteur: Joyce Hakmeh (Chatham House) Secrétariat: Alexandru Frunza (Cybercrime Division, Council of Europe) ► Organisations internationales et leurs approches pour traiter la question de la cybercriminalité et de la cybersecurité - 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) ► Les politiques et initiatives développées par les organisations du secteur privé, des instituts nationales et des associations professionnelles - 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: quelles synergies?
16h00-16h15 *Pause café*	

JEU, 17 NOVEMBRE

14h30	*Salle 2 (E/F)* **Atelier 8 – Cibler les revenus des activités criminelles en ligne** *Dans le monde entier, la plupart des actes de cybercriminalité signalés et faisant l'objet de poursuite par les autorités de la justice pénale est lié aux différents types de fraude et autres infractions visant à obtenir des avantages économiques illégaux. De grandes quantités de revenu de la criminalité sont ainsi produites – et souvent lavées – sur Internet et par l'utilisation de technologies de l'information et de la communication (TIC). Le défi est de retracer, saisir et confisquer les revenus générés en ligne. Le Conseil de l'Europe a préparé une étude détaillée sur cette question en 2012 et en 2016 le Conseil de l'Europe et l'Union européenne ont lancé le projet iPROCEEDS. INTERPOL, EUROPOL, l'Office des Nations Unies contre la drogue et la criminalité, le Conseil de l'Europe et d'autres organisations mettent au point des supports de formation pour relier les enquêtes sur le blanchiment d'argent et la cybercriminalité financière, souvent avec une attention particulière sur le « darkmarkets ». L'objet de cet atelier est de partager l'expérience / les bonnes pratiques concernant le ciblage des revenus des activités criminelles en ligne, y compris les programmes de formation.* Modérateur/s: Dave O'Reilly (FTR Solutions) Rapporteur: Hein Dries-Ziekenheiner (Vigilo Consult) Secrétariat: Mariana Chicu and Alin Tortolea (Cybercrime Programme Office of the Council of Europe) ► Le flux monétaire criminel sur internet: définir les défis (30 min) - Les exemples et les typologies de la Serbie et de la Turquie (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
16h00-16h15 *Pause café*	► La coopération public/privé afin de cibler les revenus de la criminalité en ligne (45 min) Del Pillar and Francesca Cannas (National Crime Agency (NCA), UK) - Les mules d'argent – étude de cas - Péril de l'adresse email professionnel - L'engagement de la NCA avec le secteur bancaire pour un partenariat de confiance ► Construire des passerelles: enquêteurs dans le domaine financier, unités de renseignement et unité de la cybercriminalité (30 min) - Etat de cas (Max Braun, Premier Substitute, FIU Luxemburg) - Coopération interagence– exemples de bonnes pratiques (Fadil Abdyli, Chief of Cyber Crime Investigation Sector, Kosovo* Police, Meriton Shoshi, Financial Intelligence Unit of Kosovo*) ► Programme de formation (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)

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

JEU, 17 NOVEMBRE	
14h30	*Salle 3 (E) – les règles du Chatham House s'appliqueront* **Atelier 9 –Criminalité et juridiction dans le cyberespace : accès à la preuve électronique** *Compte tenu de la prolifération de la cybercriminalité et des autres infractions comprenant la preuve électronique et dans un contexte de changement technologique et d'incertitude concernant la compétence, des solutions supplémentaires sont nécessaires pour permettre aux autorités de la justice pénale d'obtenir des éléments de preuve électronique spécifiques dans les enquêtes criminelles spécifiques. En décembre 2014, le Comité de la Convention sur la cybercriminalité (T-CY) mis en place un groupe de travail le « Cloud Evidence Group » afin d'explorer des solutions. Le sujet était également une priorité de la présidence néerlandaise de l'Union européenne.* *Cet atelier vise à discuter de la faisabilité des solutions actuellement à l'étude, y compris les résultats du Cloud Evidence Group.* . Modérateur/s: Erik Planken (Chair, Cybercrime Convention Committee, Ministry of Justice and Security, Netherlands) Rapporteur: Betty Shave (USA) Secrétariat: Pierluigi Perri (Cybercrime Division, Council of Europe) ► Récapitulatif: Criminalité et preuve dans le nuage – les défis (30 min) - Résumé du rapport sur les défis du Cloud Evidence Group - Commentaires par EUROJUST, INTERPOL, secteur privé ► Les concepts de la compétence (30 min) - Exposé - Jennifer Daskal (Associate Professor, American University Washington College of Law) - Commentaires
16h00-16h15 *Coffee break*	► Vers des solutions (120 min) - Au-delà les frontières: la compétence dans le cyberspace – suivi par la présidence néerlandaise de l'Union européenne (Erik Planken, Senior Policy Advisor Cybercrime, Law Enforcement Department, Ministry of Justice) - Discussion - Les résultats du Cloud Evidence Group du Comité de la Convention sur la cybercriminalité– Présentation et discussion sur: - Les mesures juridiques et pratiques afin de rendre l'entraide judiciaire plus efficace - La note d'orientation sur l'injonction de produire (article 18 Convention de Budapest) - Les règles nationales pour l'injonction de produire des données relatives aux abonnées - Les mesures pratiques pour la coopération avec les fournisseurs - Protocole à la Convention de Budapest ► Conclusions (15 min)

VEN, 18 NOVEMBRE	
9h30	Plénière *Salle 1 (EN/FR/ES/RU)* ► Résultats des ateliers (45 min) - Atelier 1 – Renforcement des capacités (Esther George, Royaume-Uni) - Atelier 2 – Législation en Asie/Pacifique (Zahid Jamil, Pakistan) - Atelier 3 – Coopération fournisseur de service et force de l'ordre (Markko Künnapu, Estonie) - Atelier 4 – Terrorisme et ICT (Andrea Candrian, Suisse) - Atelier 5 – Législation en Afrique (Patrick Mwaita) et en Amérique latine (Pablo Castro, Chile) - Atelier 6 – Coopération internationale (Aleksandra Tukisa, Latvia) - Atelier 7 – Synergies (Joyce Hakmeh, Chatham House) - Atelier 8 – Les revenus de la criminalité (Hein Dries-Ziekenheiner, les Pays-Bas) - Atelier 9 – Criminalité et compétence dans le cyberspace (Betty Shave, USA)
10h30-10h45 *Pause café*	

	► Droit de l'homme et Etat de droit dans le cyberspace : les risques et les garanties (75 min)
	
	- Keynotes:
	  - Ravi Raj Yerrigadoo (Ministre de la Justice, Maurice)
	  - Juge Robert Spano (Cour Européenne des Droits de l'Homme)
	
	- Commentaires par les organisations de la protection des données et de la société civile
	  - 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)
	
	- Commentaire par les autorités de la justice pénale – garanties en place
	  - 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
	  - Papa Assane Touré, Secrétaire général Adjoint du Gouvernement Primature du Sénégal
	
	► Session de conclusion: Octopus "à emporter" (45 min)
	
	Modérateur: Jan Kleijssen (Director of Information Society and Action against Crime, Council of Europe)
	
	- Panel de discussion
	- Clôture

13:00	*Fin de la conférence*