Conférence Octopus 2018

Coopération contre la cybercriminalité

11 – 13 juillet 2018

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

Version 2 juillet 2018

Projet de

Programme de la Conférence

La Conférence Octopus fait partie du projet Cybercrime@Octopus, qui est financé au moyen de contributions volontaires de l'Estonie, de la Hongrie, du Japon, de Monaco, de la Roumanie, de la Slovaquie, du Royaume-Uni et des États-Unis, ainsi que par le budget du Conseil de l'Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Vue d'ensemble du programme

MERCREDI 11 JUILLET		
Séance plénière	*Hémicycle (E/F/S/R)*	
14h00	**Séance d'ouverture** **La justice pénale dans le cyberespace : principales difficultés 2017/2019** **Présentation des ateliers**	
20h00 Dîner-réception		
JEUDI 12 JUILLET		
Ateliers	*Hémicycle (E/F/S/R)*	*Salle 11 (E/S/F)*
9h00	**Atelier 1 :** ► Preuve et compétence dans le cyberespace : consultation multipartite sur le Protocole à la Convention de Budapest	**Atelier 2 :** ► Situation mondiale en matière de législation sur la cybercriminalité 2013 – 2018
12h30 – 14h00	*Pause-déjeuner*	
Ateliers	*Hémicycle (E/F/S/R)*	*Salle 11 (E/F/S)*
14h00	**Atelier 1** (suite) **:** ► Preuve et compétence dans le cyberespace : consultation multipartite sur le Protocole à la Convention de Budapest	**Atelier 3 :** ► Renforcement des capacités sur la cybercriminalité et les preuves électroniques : quel impact ?
VENDREDI 13 JUILLET		
Ateliers	*Hémicycle (E/F/S/R)*	*Salle 11 (E/F/S)*
9h00	**Atelier 4 :** ► WHOIS : Et maintenant ?	**Atelier 5 :** ► Cyberviolence : problèmes et solutions
12h30 – 14h00	*Pause-déjeuner*	
Séance plénière	*Hémicycle (E/F/S/R)*	
14h00	**Plénière :** ► Résultats des ateliers ► Regard sur l'avenir : intelligence artificielle et cybercriminalité ► Allocutions de clôture	
17h00	*Fin de la conférence*	

Veuillez noter que les règles de Chatham House s'appliqueront tout au long de la Conférence afin de permettre la tenue de débats ouverts.

Programme détaillé

MERCREDI 11 JUILLET	
Séance plénière	*Hémicycle (E/F/S/R)*
14h00 Pause-café 15h45-16h00	**Plénière** ► **Séance d'ouverture** [14h00 – 14h45] – Jan Kleijssen (directeur de la Direction de la société de l'information et de la lutte contre la criminalité, Conseil de l'Europe) – Ursula Owusu-Ekuful (ministre des Communications, Ghana) – Marcela Ordonez Fernandez (ministre plénipotentiaire, coordinatrice de la prévention de la criminalité, ministère des Affaires étrangères, Colombie) [à confirmer] – Bessolé René Bagoro (ministre de la Justice, des Droits humains et de la Promotion civique, Garde des Sceaux du Burkina Faso) – Ronald Kay Warsal (ministre de la Justice et des Services de communication Services, Vanuatu) [à confirmer] ► **La justice pénale dans le cyberespace : principales difficultés 2017/2019** – Menaces et réponses : la justice pénale est-elle à la hauteur des enjeux ? [14h45 – 15h45] – Antonio Lopez Melgarejo (Police nationale espagnole) – Une cyberattaque bancaire à un milliard d'euros – Axel Petri (premier vice-président, gouvernance de la sécurité du groupe, Deutsche Telekom) – point de vue de TELCO sur les propositions en matière de preuves électroniques – Jean-Paul Laborde (Directeur du centre d'expertise sur la lutte contre le terrorisme, Titulaire de la Chaire Cybersécurité/cyberdéfense, St-Cyr, France) – Terrorisme, cybercriminalité et preuves électroniques – Daniel Grubb (Action contre la cybercriminalité, Home Office, Royaume-Uni) – la Convention de Budapest en application – Discussion – La démocratie attaquée [16h00-16h45] – Alexander Seger (Chef de la Division Cybercriminalité, Conseil de l'Europe) – Simona Granata-Menghini (Secrétaire adjointe de la Commission de Venise, Conseil de l'Europe) – Facebook [à confirmer] – Cybercriminalité et preuves électroniques : menaces pour les droits de l'homme [16h45-17h30] – Katitza Rodriguez (directeur des Droits internationaux, fondation Electronic Frontier, États-Unis) – Maryant Fernandez Perez (conseillère principale, European Digital Rights (EDRI), Bruxelles, Belgique) – Andrea Tamietti (Greffier adjoint, Section IV, Cour européenne des droits de l'homme, Conseil de l'Europe, Strasbourg) – Cour européenne des droits de l'homme : Benedik c. Slovénie ► **Présentation des ateliers** [17h30-18h00]

	– Chaque modérateur présente brièvement les questions qui seront évoquées lors de son atelier.
19h00	***Dîner-réception***

JEUDI 12 JUILLET	
Ateliers	*Hémicycle (E/F/S/R)*
9h00 *Pause-café* *10h45 – 11h00*	**Atelier 1 – Preuve et compétence dans le cyberespace : consultation multipartite sur le Protocole à la Convention de Budapest** Le Comité de la Convention sur la cybercriminalité (T-CY) a décidé en juin 2017 de préparer un projet de 2e Protocole additionnel à la Convention de Budapest sur la cybercriminalité. Les négociations ont débuté en septembre 2017 et devraient durer jusque fin 2019. Lors du processus de rédaction, le T-CY souhaite travailler en concertation étroite avec la société civile, les organisations de protection des données et les acteurs du secteur, afin de solliciter leur avis et de bénéficier de leur expérience. Cet atelier sera l'occasion d'une telle concertation. D'autres réunions seront organisées au fur et à mesure que les projets de concepts et de textes seront disponibles. Un guide de discussion a été conçu en vue de structurer l'atelier. Modérateur/trice/s : Cristina Schulman (ministère de la Justice, Roumanie) / Pedro Verdelho (Bureau du procureur général, Portugal) Rapporteure : Betty Shave (consultante, États-Unis) Secrétariat : Alexander Seger (Secrétaire exécutif, Comité de la Convention sur la cybercriminalité, Conseil de l'Europe) ► **Contexte : Objet du Protocole – Rappel et développements récents** – Historique – Développements internationaux pertinents – Propositions de l'UE sur les preuves électroniques – Loi CLOUD des États-Unis ► **Dispositions pour une entraide judiciaire plus efficace** – Introduction : Recommandations du T-CY 2014 et suites données par les Parties – Informations et échange de vues sur les propositions de dispositions relatives à l'entraide judiciaire ► **Coopération directe avec les fournisseurs par-delà les juridictions** – Divulgation volontaire [d'informations sur les abonnés] par les fournisseurs de services – Demandes de conservation
12h30 – 14h00	*Pause-déjeuner*
14h00 *Pause-café* *15h45 – 16h00*	**Atelier 1 (suite)** ► **Coopération directe avec les fournisseurs par-delà les juridictions** – Ordonnances de communication ► **Accès aux données du cloud/« accès transfrontalier » aux données** – Concepts de compétence : critères de rattachement – Portée de l'article 32 de la Convention de Budapest – Extension des recherches et autres options et scénarios ► **Étapes suivantes et autres consultations**
18h00	*Fin de la journée 2*

JEUDI 12 JUILLET	
Ateliers	*Salle 11 (E/F/S)*
9h00 *Pause-café* *10h45 – 11h00*	**Atelier 2 – Situation mondiale en matière de législation sur la cybercriminalité 2013 – 2018** L'existence d'une législation spécifique, conforme aux droits de l'homme et aux exigences de l'État de droit, est le fondement de l'action pénale relative à la cybercriminalité et aux preuves électroniques. De nombreux gouvernements dans le monde ont entrepris des réformes juridiques au cours des cinq dernières années, s'inspirant souvent de la Convention de Budapest sur la cybercriminalité. L'adoption d'une législation matérielle incriminant les infractions commises à l'encontre et au moyen d'ordinateurs et de compétences procédurales permettant la collecte de preuves électroniques est souvent le point de départ ouvrant la voie à d'autres mesures de renforcement des capacités. Des progrès quantifiables sont observés et d'importants enseignements peuvent être tirés de cette expérience. Cet atelier a pour but d'examiner les progrès réalisés à l'échelle mondiale au cours des cinq dernières années, et notamment des exemples de bonnes pratiques et de points posant problème. Modérateurs : Zahid Jamil (avocat, Jamil & Jamil, Pakistan) / Karuna Devi Gunesh-Balaghee (conseillère parlementaire, Bureau du procureur général, île Maurice) Rapporteur : Jayantha Fernando (conseiller juridique/directeur de programme – Policy & e-Leadership, Agence des TIC du Sri Lanka) Secrétariat : Giorgi Jokhadze (chargé de projet, C-PROC, Conseil de l'Europe) / Ana Elefterescu (chargée de projet, C-PROC) ► **De 2013 à 2018 : examen des progrès réalisés concernant l'adoption de textes législatifs sur la cybercriminalité et les preuves électroniques** [9h00 – 9h30] – Résultats préliminaires d'une enquête du Bureau de programme sur la cybercriminalité du Conseil de l'Europe (C-PROC) – Discussion ► **Droit pénal matériel** [9h30 – 10h30] – Introduction : exigences de la Convention de Budapest concernant le droit matériel (Zahid Jamil) – Exemples de bonnes pratiques – courtes présentations des pays (*15 min*) : – Botswana (Khursheed Rossenkhan, Chambres du procureur général) (*à confirmer*) – Argentine (Marcos Salt, Comité consultatif contre la criminalité informatique) (*à confirmer*) – Singapour (Kannan Gnanasihamani, Chambres du procureur général) (*à confirmer*) – Problèmes rencontrés et risques pour les droits de l'homme – discussion ouverte avec les pays participant à l'atelier sur : – Liberté d'expression et définition générale de l'incrimination des

	comportements en ligne ► **Droit pénal procédural : pouvoirs des forces de l'ordre pour obtenir des preuves électroniques** [10h30-10h45, 11h00-12h00] – Ordonnances de communication : – Introduction sur la récente Note d'orientation du T-CY relative à l'article 18 de la Convention (Karuna Devi Gunesh-Balaghee) – Application des ordonnances de communication dans le droit interne : exemples de bonnes pratiques – Ordonnances de communication d'informations sur les abonnés : adresses IP dynamiques ou statiques – Benedik c. Slovénie (présentation de Marko Juric, Université de Zagreb (Croatie) et du C-PROC) – Séance sur les garanties de l'Etat de droit dans le contexte des pouvoirs procéduraux de la Convention de Budapest (Marko Juric) – Introduction : Résultats de Étude sur les garanties de l'article 15 dans la région du Partenariat oriental (mise à jour en 2018) – Discussion sur les conséquences des décisions judiciaires (juridictions internes, Cour de justice de l'Union européenne, Cour européenne des droits de l'homme) relatives à la conservation des données, aux données WHOIS, aux pouvoirs d'interception et de surveillance et aux nouvelles règles sur la protection des données (Convention 108+, Règlement général sur la protection des données de l'UE) sur les pouvoirs procéduraux permettant d'obtenir des preuves électroniques ► **Comment veiller à l'exécution des réformes législatives ?** [12h00-12h20] – Discussion ouverte : comment « vendre » aux décideurs une bonne législation relative à la cybercriminalité ? ► **Conclusions** [12h20-12h30]
12h30 – 14h00	*Pause-déjeuner*

JEUDI 12 JUILLET	
Ateliers	*Salle 11 (E/F/S)*
14h00 *Pause-café* *15h45 – 16h00*	**Atelier 3 – Renforcement des capacités sur la cybercriminalité et les preuves électroniques : quel impact ?** Le renforcement des capacités est considéré comme l'un des moyens les plus efficaces pour résoudre les problèmes liés à la cybercriminalité et aux preuves électroniques. Sur la base d'un large consensus international, les gouvernements et les organisations internationales, mais aussi la société civile et le secteur privé mettent des ressources à disposition depuis quelques années et soutiennent partout dans le monde des programmes visant à renforcer la législation, proposer une formation aux professionnels de la justice pénale, promouvoir la coopération public/privé et donner plus d'efficacité à la coopération internationale. Cet atelier a pour but de tirer des enseignements de l'action menée à ce jour : quel est l'impact des initiatives de renforcement des capacités en matière de cybercriminalité et de preuves électroniques depuis quelques années ? Les projets ont-ils changé les choses ? Modératrice : Panagiota-Nayia Barmpaliou (avocate et spécialiste du cyberespace, Grèce) Rapporteur : George-Maria Tyendezwa (directeur adjoint, chef du Service de répression de la cybercriminalité, ministère fédéral de la Justice, Nigeria) Secrétariat : Marie Agha-Wevelsiep (chargée de projet, CyberSud, C-PROC, Conseil de l'Europe) / Manuel de Almeida Pereira (chargé de projet, projet GLACY+, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** [14h00-14h15] – L'utilité d'évaluer l'impact : pourquoi les indicateurs sont importants, pourquoi se soucier de l'impact, comment éviter « l'aide inutile » ? – Introduction (Panagiota-Nayia Barmpaliou) – Allocution (Zahid Jamil, avocat, Pakistan) ► **Comment mesurer l'impact** [14h15-15h40] – De quels outils et systèmes les organisations se sont-elles dotées pour garantir et mesurer l'impact des projets relatifs à la cybercriminalité ? Courtes présentations des institutions/experts suivants, suivies d'une discussion : – David E. Satola (Conseil de direction, Technologie & Innovation, Banque mondiale) – Wouter Veenstra (directeur Contacts et Partenariat, GFCE) – Patryk Pawlak (directeur exécutif, Bruxelles, EU-ISS) – Quels sont les critères sur lesquels fonder les objectifs et les résultats attendus et juger de l'impact ? (discussion modérée par Panagiota-Nayia Barmpaliou) : – Buts et actions prévus dans les objectifs politiques/stratégiques en matière de cybercriminalité/sécurité – Législation = Convention de Budapest ; coopération public/privé – Capacités répressives = nombre d'enquêtes, mesure des résultats des

	forces de l'ordre en matière de cybercriminalité Courtes présentations des institutions/experts suivants : – Cristos Velasco (maître de conférences à l'université DHBW, fondateur et directeur exécutif de Ciberdelincuencia.Org et Evidencia Digital.Lat, Allemagne) – Hania Helweh (juge, correspondant cybercriminalité, ministère de la Justice, Liban) – Henry Bryers (directeur principal – Réponse aux menaces, Service national sur la cybercriminalité, Agence nationale de lutte contre la criminalité (NCA), Royaume-Uni) – Karuna Devi-Gunesh (conseillère parlementaire, Bureau du procureur général, île Maurice) – Albert Antwi-Boasiako (conseiller sur la politique et la stratégie nationales de cybersécurité, ministère des Communications, Ghana) – Le problème du lien fortuit : comment savoir si l'impact est lié aux actions du projet ? – Introduction (Panagiota-Nayia Barmpaliou) – Discussion ► **Impact des projets : études de cas** [16h00 – 17h00] – Comment évalue-t-on l'impact dans des projets concrets ? Exposés introductifs suivis de discussions : – Exemple d'un projet de l'ONUDC (Neil J. Walsh, chef de la Section cybercriminalité et lutte contre le blanchiment, ONUDC) – Exemple de GLACY+ (Manuel de Almeida Pereira, Conseil de l'Europe) – Quels sont les principaux risques pouvant réduire l'impact ? – Introduction (Panagiota-Nayia Barmpaliou) – Discussion ► **Enseignements tirés : garantir l'impact lors de la conception et de la mise en œuvre des projets** [17h00 – 18h00] Séance de brainstorming (modérée par Panagiota-Nayia Barmpaliou) et observations préliminaires du rapporteur (George-Maria Tyendezwa) : – Les enseignements sont-ils positifs ou négatifs ? – Enseignements pour améliorer les futurs projets et leur impact ?
18h00	*Fin de la journée 2*

VENDREDI 13 JUILLET	
Ateliers	*Hémicycle (E/F/S/R)*
9h00 *Pause-café* *10h45 – 11h00*	**Atelier 4 – WHOIS : Et maintenant ?** Depuis de nombreuses années, l'accès public aux données WHOIS est un outil important, permettant à la justice pénale d'identifier les personnes inscrites sur les sites web utilisés à des fins criminelles. De même, certains s'interrogent de longue date sur la compatibilité de ce registre WHOIS public avec les exigences de la protection des données. Eu égard au Règlement général sur la protection des données (RGPD) de l'Union européenne, l'ICANN – l'organisation chargée d'allouer l'espace des adresses de protocole Internet (IP) et de gérer le système des noms de domaine – a mis en place la Spécification temporaire relative aux données d'enregistrement des gTLD, entrée en vigueur le 25 mai 2018, qui restreint l'accès à la partie des informations WHOIS considérée comme des données à caractère personnel. Des consultations sont menées depuis un certain temps en vue de trouver des solutions permettant aux forces de l'ordre et autres acteurs légitimes d'avoir accès aux données WHOIS tout en respectant les exigences en matière de protection des données. Cet atelier a pour but d'aider les acteurs à mieux comprendre les enjeux, afin qu'ils contribuent de manière éclairée à la recherche de solutions. Modérateurs : Jayantha Fernando (directeur/conseiller juridique, Agence des TIC, Sri Lanka) Rapporteur : Tjabbe Bos (chargé de mission, cybercriminalité, Commission européenne) Secrétariat : Matteo Lucchetti (chargé de projet, C-PROC, Conseil de l'Europe) ► **WHOIS – de quoi s'agit-il et pourquoi est-ce important ?** [9h00 – 10h00] – Présentation générale, qu'est-ce que WHOIS ? – Tjabbe Bos (chargé de mission, cybercriminalité, Commission européenne) – L'entrée en vigueur du RGPD : WHOIS avant et après le 25 mai 2018 – Peter Kimpian (Unité protection des données, Conseil de l'Europe) – Elena Plexida (directrice principale, Participation des gouvernements et des organisations intergouvernementales, ICANN) – La situation actuelle – Caroline Greer (Politique publique européenne, Cloudflare) – WHOIS dans les enquêtes sur la cybercriminalité – exemple d'utilisation – Gregory Mounier (chef de l'Unité sensibilisation et prévention – European Cybercrime Center EC3, Europol) – Q&R (15 min) ► **Problèmes** [10h00 – 11h30] – Protection des données et société civile : protection des données à caractère personnel et respect des normes applicables – Peter Kimpian (Unité protection des données, Conseil de l'Europe)

	– Représentant d'une APD de l'UE [à confirmer] – L'ICANN et les obligations contractuelles des fournisseurs de services – Elena Plexida (directrice principale, Participation des gouvernements et des organisations intergouvernementales, ICANN) – *Registrars* et registres – Caroline Greer (Politique publique européenne, Cloudflare) – Spencer Payton (analyste principal des ressources en ligne, Centre de coordination des RIPE) – Justice pénale et organisations de cybersécurité : WHOIS est-il devenu « secret » ? – Erica O'Neil (chef adjointe pour la criminalité informatique, Section criminalité informatique et propriété intellectuelle, ministère de la Justice des États-Unis) – Jaap Van Oss (Expert principal sur la cybercriminalité, Police, Pays-Bas) – Peter Cassidy/ Pat Cain (Secrétaire général/ chercheur invité, Groupe de travail anti-phishing) – Q & R ► **Solutions envisagées** [11h30 – 12h00] – Système de niveaux d'accès et d'autorisation pour les utilisateurs légitimes – Elena Plexida (directrice principale, Participation des gouvernements et des organisations intergouvernementales, ICANN) – Sûreté publique et forces de l'ordre – Tjabbe Bos (chargé de mission, cybercriminalité, Commission européenne) – Gregory Mounier (chef de l'Unité sensibilisation et prévention – European Cybercrime Center EC3, Europol) – Erica O'Neil (chef adjointe pour la criminalité informatique, Section criminalité informatique et propriété intellectuelle, ministère de la Justice des États-Unis) – Secteur privé – Peter Cassidy/ Pat Cain (Secrétaire général/ chercheur invité, Groupe de travail anti-phishing) ► **Perspectives** [12h00 – 12h30] – Discussion ouverte
	Pause-déjeuner

VENDREDI 13 JUILLET	
Ateliers	*Salle 11 (E/F/S)*
9h00 *Pause-café* *10h45 – 11h00*	**Atelier 5 – Cyberviolence : problèmes et solutions** Les actes de violence contre les personnes physique commis ou facilités au moyen des technologies de l'information et de la communication (la « cyberviolence ») sont devenus un problème majeur pour les sociétés et les individus. Bien que la cyberviolence existe déjà depuis plusieurs années, il n'y a semble-t-il que peu de temps qu'on a commencé à identifier et comprendre ses formes spécifiques. La plupart des pays s'efforcent d'identifier les différentes composantes du problème et d'y apporter une réponse dans leur législation interne. Le but de l'atelier est d'examiner ces problèmes du point de vue de la justice pénale et de réfléchir à des solutions nationales et internationales, notamment une meilleure coopération et d'éventuelles synergies. Ces solutions incluent notamment une meilleure utilisation des outils proposés par les Conventions de Budapest, Lanzarote et Istanbul du Conseil de l'Europe, ainsi que par le Protocole à la Convention de Budapest sur la xénophobie et le racisme. Modératrice/s : Betty Shave, États-Unis Rapporteur: Briony Daley Whitworth (Department of Home Affairs, Australie) Secrétariat : Nina Lichtner et Mariana Chicu (Division de la cybercriminalité, Conseil de l'Europe) ► **Concepts de la cyberviolence :** – Définir la cyberviolence : Gareth Sansom (membre du Bureau du T-CY, Directeur de la technologie et de l'analyse, Section de la police criminelle, ministère de la Justice, Canada) – Discussion ► **Expériences et réponses nationales et internationales à la cyberviolence :** – Menace et impact de la cyberviolence : brèves présentations suivies de discussions – Aura Freeman (responsable de campagne, Équipe des campagnes mondiales, Amnesty International) – Maria José Castello Branco (Membre du Bureau de la Convention de Lanzarote) – Daniela Pichler (directrice Politiques et campagnes, Lobby européen des femmes) – Discussion sur les thèmes suivants Quels incidents observez-vous dans votre pays ? Quelles sont les évolutions ? Qui sont les victimes ? – Études de cas sur la législation, les politiques, les stratégies et autres réponses nationales : – Canada : approche législative du cyberharcèlement (Gareth Sansom, ministère de la Justice, Canada) – Serbie : étude de cas sur les matériels pornographiques mettant en scène des enfants et la coercition (Tatjana Vasiljevic, Bureau spécial de lutte contre la cybercriminalité, Serbie) – Sénégal (Papa Assane Touré, magistrat, Secrétaire général adjoint du

	Gouvernement, Primature) [à confirmer] – Réponses internationales : – Jurisprudence de la Cour de Strasbourg sur la cyberviolence (Robert Spano, juge, Président de la Section II, Cour européenne des droits de l'homme) – Rôle de la Convention de Lanzarote (Christel De Craim, Vice-Présidente, Comité de la Convention de Lanzarote ; Maria José Castello Branco, Membre du Bureau de la Convention de Lanzarote) – Rôle de la Convention d'Istanbul (représentant du GREVIO [à confirmer]) – Rôle de la Convention de Budapest et de son Protocole sur la xénophobie et le racisme (Gareth Sansom, membre du Bureau du T-CY) ► **Rôle des fournisseurs de services** – Maximilian Schubert (Vice-Président, EuroISPA) – Acadia Senese (juriste en entreprise, Application de la loi et sécurité de l'information, Google) ► **Enseignements tirés : bonnes pratiques et défis** – Conseils de participants à d'autres pays – Objectifs des participants pour leur propre pays – Conseils des participants pour les victimes ► **Conclusions : Quelles synergies ?**
12h30 – 14h00	*Pause-déjeuner*

VENDREDI 13 JUILLET	
Séance plénière	*Hémicycle (E/F/S/R)*
14h00	**Plénière** ► **Résultats des ateliers** [14h00-14h30] – Le rapporteur de chaque atelier présente ses résultats. ► **Regard sur l'avenir : intelligence artificielle et cybercriminalité** [14h30-15h45] Les progrès rapides de l'intelligence artificielle et de l'apprentissage automatique posent des questions fondamentales sur l'avenir de l'humanité, mais aussi des questions spécifiques quant à leur utilité et aux risques qu'ils représentent concernant la cybercriminalité et la justice pénale. L'objectif de ces interventions est de réfléchir à ce que nous devons faire aujourd'hui pour nous préparer à l'avenir de l'IA : ▪ IA et apprentissage automatique : de quoi s'agit-il ? ▪ Quelles sont les implications pour la cybercriminalité et la justice pénale ? ▪ L'IA peut-elle améliorer la cybersécurité et faciliter la détection et l'investigation des actes de cybercriminalité et l'identification de leurs auteurs ? ▪ L'IA peut-elle automatiser la cybercriminalité (systèmes de dépistage pour exploiter les failles, ingénierie sociale/usurpation d'identité, cybercriminalité autonome par des machines) ? ▪ L'IA, la cybercriminalité et la loi : qui est responsable des décisions prises et des infractions commises par des machines et des réseaux neuronaux ? ▪ Quelles normes éthiques pour l'utilisation de l'IA dans la justice pénale ? ▪ IA et cybercriminalité : comment se préparer à l'avenir ? Modérateur : – Jan Kleijssen (Directeur, Direction de la Société de l'information et de la lutte contre la criminalité, DG 1, Conseil de l'Europe) Intervenants : – Rebekah Overdorf (Département d'électrotechnique, KU Leuven, Belgique) – Claudia Peersman (Groupe Cybersécurité de Bristol, Université de Bristol, Royaume-Uni) – Pavel Gladyshev (Université de Dublin, Irlande) ► **Allocutions de clôture** [16h00 – 17h00] – Estela Bernabe (juge, Cour suprême des Philippines) à confirmer – Mamadú Iaia Djalo (ministre de la Justice, Guinée-Bissau) – Mohamed R. Swaray (ministre de l'Information et de la Communication, Sierra Leone) à confirmer – Gabriel Juarez Lucas (vice-ministre des Technologies de l'information et de la communication, Guatemala) à confirmer – Agni Prasad Kharel (Procureur général, Népal)
17h00	*Fin de la conférence*