12 novembre 2021

Coopération contre la cybercriminalité

Conférence Octopus 2021

16 -18 novembre 2021 - En ligne

Vue d'ensemble

Mar, 16 novembre (Veuillez noter que l'heure est en CET)	
13h00 - 19h00 CET	**Session plénière :** Evénement spécial organisé en coopération avec la Présidence hongroise du Comité des Ministres à l'occasion de la : **20eth anniversaire de la Convention de Budapest sur la cybercriminalité** **&** **2 ndProtocole additionnel sur le renforcement de la coopération et de la divulgation des preuves électroniques** ► Ouverture ► 20 ans de la Convention de Budapest - avantages et impact ► Le 2ème Protocole additionnel à la Convention sur la cybercriminalité ► Interventions de haut niveau

mer, 17 novembre		
7h00 - 8h50	WS 1 : Atelier régional pour l'Asie	
9h00 - 10h50	WS 2 : COVID-19 et la cybercriminalité	WS 3 : Atelier régional pour l'Afrique
11h00 - 12h50	WS 4 : Criminalité et crypto-monnaies	WS 5 : L'état mondial de la législation sur la cybercriminalité
13h00 - 14h00	Pause	
14h00 - 15h50	WS 6 : Détection automatisée des documents relatifs à l'exploitation sexuelle des enfants	WS 7 : Ransomware
16h00 - 17h50	WS 8 : Cybercriminalité et intelligence artificielle	Discussions éclair I
18h00 - 19h50	WS 9 : Atelier régional pour l'Amérique latine et les Caraïbes	

Jeu, 18 novembre		
7h00 - 8h50	Atelier 10 : Atelier régional pour le Pacifique	
9h00 - 10h50	Atelier 11 : Renforcement des capacités : formation judiciaire	Atelier 12 : Les victimes de la cybercriminalité
11h00 - 12h50	Atelier 13 : Renforcement des capacités : guides et outils	Atelier 14 : Cybercriminalité : Délinquants
13h00 - 13h45		Discussions éclair II
13h45 - 14h30	Pause	
14h30 - 15h30	Outlook 1 : Cybercriminalité - menaces et tendances	
15h30 - 16h15	Outlook 2 : Droits de l'homme et état de droit dans le cyberespace	
16h15 - 16h30	Pause	
16h30 - 17h15	Perspective 3 : Coopération contre la cybercriminalité en 2022	

17h15 - 18h00	Conclusions - Les points à retenir de la pieuvre
18h00	*Fin de la conférence*

Programme détaillé

MARS, 16 NOVEMBRE - EVÉNEMENT SPÉCIAL	
Plénière	Langues : Anglais / Français / Espagnol / Hongrois
13h00 - 19h00	**20e th anniversaire de la Convention de Budapest sur la cybercriminalité** **&** **2 ndProtocole additionnel sur le renforcement de la coopération et de la divulgation des preuves électroniques** Modérateur : Jan Kleijssen (Directeur de la société de l'information et de la lutte contre la criminalité, Conseil de l'Europe) ► **Ouverture** – Sándor Pintér (Ministre de l'Intérieur, Hongrie) – Marija Pejčinović Burić (Secrétaire Générale, Conseil de l'Europe) ► **Interventions I** – Interventions de ministres ou de hauts fonctionnaires ► **Panel : 20 ans de la Convention de Budapest - impact mondial** – Modérateurs : Cristina Schulman (Présidente du Comité de la Convention sur la cybercriminalité (T-CY), Ministère de la Justice, Roumanie) / Alexander Seger (Secrétaire exécutif, T-CY, Conseil de l'Europe) – Panélistes : Betty Shave (anciennement US Department of Justice, USA), Pedro Verdelho (Vice-président du T-CY, Procureur de la République, Portugal), Papa Assane Touré (Magistrat, Secrétaire Général Adjoint du Gouvernement, Sénégal), Claudio Peguero (Inspecteur Général de la Police Nationale, République Dominicaine), Jayantha Fernando (Avocat Général, ICT Agency of Sri Lanka et Directeur, Sri Lanka CERT), Gareth Sansom (Department of Justice, Canada)
14h45-15h15	*Pause*
	► **Interventions II** – Interventions de ministres ou de hauts fonctionnaires ► **Panel : Le 2ème Protocole additionnel à la Convention sur la cybercriminalité - attentes** – Modérateurs : Cristina Schulman (Présidente du Comité de la Convention sur la cybercriminalité, Roumanie) / Alexander Seger (Secrétaire exécutif, T-CY, Conseil de l'Europe) – Panélistes : Kenneth Harris (Conseiller principal pour les affaires pénales internationales, Département de la Justice, Mission des États-Unis auprès de l'Union européenne, États-Unis), Jacqueline Palumbo (Avocat général principal et chef des négociations de traités, Groupe d'assistance internationale, Justice Canada), Nathan Whiteman (Directeur, Département de l'Intérieur, Australie), Tjabbe Bos (Chef d'équipe, Unité "Sécurité à l'ère numérique", Direction générale de la migration et des affaires intérieures, Commission européenne) ► **Interventions III** – Interventions des ministres et hauts fonctionnaires

	► **Conclusions**
MERCREDI 17 NOVEMBRE - SESSIONS D'ATELIERS	
Mer, 17 Nov 7h00 - 8h50	**Atelier 1 - Atelier régional pour l'Asie : Renforcer la coopération internationale en matière de cybercriminalité et de preuves électroniques dans la région : Défis et solutions** Langue : EN Objectif : En Asie, la législation de fond pour lutter contre la cybercriminalité est largement ou partiellement en place, tandis qu'environ 60% des pays disposent de pouvoirs procéduraux à cet égard. L'atelier vise à fournir une plateforme de dialogue entre les décideurs et les praticiens de la région, afin d'identifier les défis particuliers et les bonnes pratiques pour la coopération internationale en matière de cybercriminalité et de preuves électroniques en Asie. L'atelier est structuré comme une table ronde entre les décideurs et les praticiens de la région, en mettant l'accent sur l'engagement des participants. L'atelier est co-organisé avec l'Office des Nations Unies contre la drogue et le crime (ONUDC). Modérateur/s : Vu Trung Hoang (Responsable des opérations de lutte contre la cybercriminalité, INTERPOL) Rapporteur: Betty Shave (Consultante, USA) Secrétariat : Martha Stickings / Cosmina Menghes (GLACY +, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Vu Trung Hoang (responsable des opérations de lutte contre la cybercriminalité, INTERPOL) ► **Principaux défis de la coopération internationale en matière de cybercriminalité et de preuves électroniques. Quels sont les problèmes spécifiques de la coopération internationale en matière de cybercriminalité et de preuves électroniques en Asie ? Comment les autorités de justice pénale en Asie obtiennent-elles des preuves d'autres États ?** – Alexandru Caciuloiu (Conseiller en matière de cybercriminalité et de crypto-monnaie et coordinateur de programme pour l'Asie du Sud-Est et le Pacifique, UNODC) – Yeongsu Jeong (Procureur principal, Directeur de la Division des enquêtes sur la cybercriminalité, Département des enquêtes scientifiques, Bureau des procureurs suprêmes, République de Corée) ► **Meilleures pratiques en matière de coopération internationale en Asie** – Jayantha Fernando (directeur, Sri Lanka CERT et avocat général, ICT Agency of Sri Lanka) – Norikazu Otaki (Chef adjoint pour les affaires internationales, Unité des procureurs japonais sur les crimes émergents (JPEC), Bureau des procureurs publics suprêmes, Japon) – Vu Trung Hoang (responsable des opérations de lutte contre la cybercriminalité, INTERPOL) ► **Recommandations sur l'amélioration de la coopération internationale dans la région et au-delà**

	– Tous les panélistes (Session modérée par Vu Trung Hoang (Responsable des opérations de cybercriminalité, INTERPOL) ► **Conclusions**
Mer, 17 Nov 9h00 - 10h50	**Atelier 2 - COVID-19 et la cybercriminalité** Langues : EN/FR/ES Objectif : La pandémie de COVID-19 s'accompagne d'une augmentation sans précédent de la cybercriminalité, ce qui affaiblit encore la capacité des autorités publiques à répondre aux cyberattaques. Cet affaiblissement des défenses est susceptible d'être davantage exploité à des fins criminelles et éventuellement pour une utilisation terroriste des technologies de l'information et de la communication, comme les attaques par déni de service contre les hôpitaux ou l'interférence avec les systèmes et les données des établissements de recherche en santé, les ransomware, etc. Dans ce contexte, l'importance d'une réponse efficace à la cybercriminalité et aux autres délits impliquant des preuves électroniques est indéniable. Les autorités de justice pénale doivent entreprendre des enquêtes nationales et s'engager dans des formes de coopération internationales et autres pour détecter, enquêter, attribuer et poursuivre les infractions susmentionnées. L'objectif de l'atelier est d'identifier les défis rencontrés par les autorités de justice pénale et de rechercher des solutions pour d'éventuelles crises futures en tirant les leçons de la pandémie actuelle. Modérateur/s : Albert Rees (expert en cybercriminalité, USA) Rapporteur : Angela Marie de Gracia-Cruz (Conseiller d'Etat, Ministère de la Justice, République des Philippines) Secrétariat : Cristiana Mitea / Irina Drexler (Projet Octopus, C-PROC, Conseil de l'Europe) ► **Introduction et objectifs de l'atelier** – Albert Rees (expert en cybercriminalité, USA) ► **Le paysage des menaces et les principaux défis en matière d'enquêtes, de poursuites et de jugements concernant la cybercriminalité liée au COVID-19, y compris la collecte de preuves électroniques.** – Focus sur COVID-19, la tempête parfaite pour la cybercriminalité (Doug Witschi, Directeur adjoint de la lutte contre la cybercriminalité, INTERPOL) – Liens entre COVID-19 et le crime organisé (Simone Haysom, analyste principale, Initiative mondiale contre le crime organisé transnational #CovidCrimeWatch) ► **La réponse de la justice pénale, remodelée par COVID-19** – Covid 19 et la cybercriminalité - l'expérience roumaine (Daniel Marius Cuciurianu, chef du département de la cybercriminalité de Bucarest, police roumaine) – Khaled Youssef, chef de la division sécurité informatique, responsable du soutien international, ISF, Liban. – Bogdan Botezatu, directeur de la recherche et des rapports sur les menaces, Bitdefender – Discussions avec les participants et questions-réponses

	► **Dans quelle mesure sommes-nous préparés aux prochaines crises : recommandations** – Présentation des résultats intermédiaires de l'étude sur la cybercriminalité liée au COVID-19 pour l'Asie (Geronimo L Sy, Fondateur, Office of Cybercrime, Département de la Justice, République des Philippines) – Discussions ouvertes sur les défis et les solutions possibles ► **Conclusions**

Mer, 17 Nov 9h00 - 10h50	**Atelier 3 - Atelier régional pour l'Afrique : Renforcer la coopération en matière de cybercriminalité et de preuves électroniques dans la région - Défis et solutions** Langues : EN/FR/PT/AR Objectif : La pénétration de l'Internet et des services connexes, tels que les services financiers mobiles, connaît une croissance rapide en Afrique. Cette évolution s'accompagne d'une augmentation de la cybercriminalité. De nombreux pays d'Afrique ont fait de l'élaboration de cadres juridiques une priorité afin d'incriminer efficacement les infractions commises contre et au moyen d'ordinateurs, de permettre des enquêtes nationales et de permettre une coopération internationale efficace entre les autorités de justice pénale, conformément aux normes internationales, en particulier celles de la Convention de Budapest et de Malabo. Les avantages des approches coopératives ont été confirmés à l'occasion du premier Forum africain sur la cybercriminalité en 2018 et à nouveau lors du deuxième Forum africain en juin 2021. Cet atelier doit assurer le suivi de l'accord conclu dans ces forums pour renforcer davantage la coopération nationale et internationale en matière de cybercriminalité en Afrique, ainsi que de l'engagement des organisations régionales et internationales à soutenir ces efforts. L'objectif spécifique est d'identifier des initiatives concrètes à entreprendre dans un avenir proche. Cet atelier est co-organisé avec la Commission de l'Union Africaine (CUA) et avec le soutien du Global Forum for Cyber Expertise (GFCE) et de la Commission de la CEDEAO. Modérateur/s : Jean-Robert Hountomey (Groupe d'experts en cybersécurité de l'Union africaine) Rapporteur: Hein Dries (Projet OCWAR-C) Secrétariat: Martha Stickings (Projet GLACY+, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Jean-Robert Hountomey (Groupe d'experts en cybersécurité de l'Union africaine) ► **Le contexte** – Abdul Hakeem Ajijola (président du groupe d'experts en cybersécurité de l'Union africaine) ► **Coordination nationale et coopération internationale en matière de cybercriminalité en Afrique : besoins et défis**

	– Albert Antwi-Boasiako (Directeur général par intérim, Cyber Security Authority, Ghana) – Conférencier à confirmer ► **Quelles initiatives pour renforcer la coopération nationale et internationale ?** – Dean Watkinson (Officier spécialisé dans la cybercriminalité, INTERPOL) – Papa Assane Touré (Magistrat, Secrétaire général adjoint du gouvernement, Sénégal) – Adel Jomni (Enseignant chercheur, Centre de droit des affaires, Université de Montpellier) ► **Recommandations sur l'amélioration de la coopération internationale dans la région et au-delà** – Panel de discussions ouvertes modéré par Moctar Yedaly, Global Forum on Cyber Expertise (GFCE) ► **Conclusions**

Mer, 17 Nov 11h00 - 12h50	**Atelier 4 - Criminalité et crypto-monnaies** Langues : EN/FR/ES Objectif : Compte tenu de la difficulté de suivre une piste d'argent dans la blockchain et de l'anonymat qui entoure en quelque sorte les transactions utilisant des crypto-monnaies, cet actif virtuel est préféré par les cybercriminels lorsqu'ils mènent leurs activités illicites et blanchissent les produits qui en découlent. Les ransomwares, le piratage et d'autres types de cybercriminalité sont sans aucun doute fortement liés aux crypto-monnaies et la réponse des autorités judiciaires est parfois entravée par la complexité de ce mélange de crimes. L'absence de législation sur les actifs virtuels et, plus encore, sur leur saisie, contribue également à ce vide que les cybercriminels exploitent. La pandémie COVID-19 n'a fait qu'accroître l'utilisation des actifs virtuels à des fins légitimes et illégitimes. L'objectif de cet atelier est de fournir aux participants des informations sur la façon dont les criminels utilisent les crypto-monnaies pour dissimuler les gains illicites résultant d'activités criminelles et de souligner l'importance de définir une législation au niveau national en ce qui concerne le traitement et la saisie de ce type de monnaie. Modérateurs : Jan Kerkhofs (magistrat fédéral, Unité cybernétique du parquet fédéral belge) / Paul Darcy (enquêteur principal, ministère de la Justice irlandais) Rapporteur: Hania Elhelweh (Juge, Présidente du tribunal de première instance au nord du Liban) Secrétariat : Alexandru Cristea / Liliana Trofim (Projet iPROCEEDS-2, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Jan Kerkhofs et Paul Darcy ► **Criminalité et crypto-monnaies : études de cas et typologies** – Toc-toc : qui est là dans la Blockchain ? (Bart De Vlaminck, détective ICT Crime, Federal Computer Crime Unit of Belgium)

	– Comment coordonner l'atténuation des infractions facilitées par les actifs virtuels (Jung Kee You, Officier de renseignement criminel, Service de lutte contre la criminalité financière d'INTERPOL) – The 69,370 BTC Seizure from Silk Road (Claudia Quiroz, Assistant Attorney, Department of Justice, United States of America) ► **Enquêter sur l'utilisation criminelle des crypto-monnaies : outils, réglementations et bonnes pratiques** – Drapeaux rouges liés à l'utilisation des crypto-monnaies (Janet Ho, analyste politique, Groupe d'action financière (GAFI)) – Regulating Virtual Asset Service Providers (VASP's), discussion (Irina Talianu, Chef d'Unité, Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment d'argent et le financement du terrorisme (MONEYVAL), Conseil de l'Europe) – Réglementer les crypto-monnaies, l'exemple du Salvador (Ana Virginia Samayoa Baron, Directrice, Financial Intelligence Unit, El Salvador) – Suivre l'argent, introduction au traçage des crypto-monnaies (Brian Carter, spécialiste principal en cybercriminalité, Chainalysis ► **Conclusions**
Mer, 17 Nov 11h00 - 12h50	**Atelier 5 - L'état mondial de la législation en matière de cybercriminalité : progrès, défis et leçons apprises** Langues : EN/FR/ES Objet : Une législation spécifique constitue la base de l'action de la justice pénale en matière de cybercriminalité et de preuves électroniques. De nombreux gouvernements dans le monde ont entrepris des réformes juridiques, en utilisant souvent la Convention de Budapest sur la cybercriminalité comme ligne directrice. Cependant, la législation sur la cybercriminalité doit également répondre aux exigences des droits de l'homme et de l'État de droit afin d'éviter les abus. L'objectif de cet atelier est d'examiner les progrès réalisés dans le monde en termes de législation sur la cybercriminalité et d'identifier les risques et les défis éventuels. Modérateurs : Zahid Jamil (Avocat, Jamil & Jamil, Pakistan) Rapporteur : Pedro Verdelho (Procureur général, Bureau du Procureur général de Lisbonne, Procuradoria General da Republica, Portugal) Secrétariat : Giorgi Jokhadze / Natalia Mardari (projet CyberEast, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** ► **De 2013 à 2021 : aperçu des progrès accomplis dans l'adoption de la législation sur la cybercriminalité et les preuves électroniques** – Résultats d'une enquête du Bureau du Programme sur la cybercriminalité du Conseil de l'Europe (Giorgi Jokhadze, C-PROC) – Discussion ► **Exemples de réformes récentes** – Exemples de bonnes pratiques et de réformes récentes : - James Lutui (Directeur des poursuites publiques, Tonga)

	- Jacqueline Fick (Avocat, Directeur Général, VizStrat Solutions, Afrique du Sud) - David Simmons (Président, Commission de réforme du droit, Barbade) ► **Défis et risques** – Les défis de la mise en œuvre du droit procédural du point de vue des sauvegardes et des garanties (Alexandros Ioannis Kargopoulos, chargé de programme, unité Recherche et données, Agence des droits fondamentaux de l'UE) – Discussion : répondre aux exigences en matière de droits de l'homme et d'État de droit - ce qu'il faut faire et ne pas faire (discussion ouverte et exemples) ► **Conclusions**
Mer, 17 Nov 14h00 - 15h50	**Atelier 6 - Détection automatisée de matériel pédopornographique** Langues : EN/FR Objectif : L'exploitation et l'abus sexuels d'enfants en ligne constituent une violation majeure des droits de l'enfant depuis de nombreuses années ; elle s'est encore accrue depuis le début de la pandémie de COVID-19. Au cours de la dernière décennie, les fournisseurs de services multinationaux ont déployé des technologies pour la détection automatique des matériels d'abus sexuels sur les enfants (CSAM) qui sont téléchargés ou diffusés via leurs services. Des dizaines de millions de CSAM ont ainsi été identifiés et signalés, ce qui a permis dans de nombreux cas de sauver des victimes et d'identifier et de poursuivre des délinquants dans le monde entier. Dans le même temps, l'utilisation de ces techniques a suscité des inquiétudes en matière d'État de droit et de droits de l'homme, par exemple parce qu'elles portent atteinte à la confidentialité des communications ou impliquent le transfert transfrontalier de données à caractère personnel ou violent les exigences d'une procédure régulière. Ces préoccupations sont apparues au premier plan avec l'entrée en vigueur du Code européen des communications électroniques de l'Union européenne, qui a soumis ces fournisseurs aux règles strictes de la directive "vie privée et communications électroniques" de l'UE. En juin 2021, le Conseil de l'Europe a publié un rapport d'experts indépendants sur cette question. L'objectif de l'atelier est de poursuivre la recherche de solutions qui permettent aux gouvernements de respecter leur obligation positive de protéger les enfants contre la violence sexuelle en ligne et aux fournisseurs de services d'utiliser des technologies automatisées pour identifier et signaler les MSC avec les garanties nécessaires en matière de vie privée, de protection des données et d'État de droit. Modérateur/s: Jean-Christophe Le Toquin (Président de Point de Contact (hotline française), et associé gérant de SOCOGI) Rapporteur: Katarzyna Staciwa (Expert indépendant, Institut national de recherche/Dyzurnet.pl, Pologne) Secrétariat : Gioia Scappucci (Secrétaire exécutif, Comité de Lanzarote, Conseil de l'Europe) / Cristiana Mitea & Irina Drexler (Projet Octopus, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Jean-Christophe Le Toquin ► **Détection automatisée des documents relatifs à l'exploitation sexuelle des enfants : Comment cela fonctionne-t-il ?**

	– John Shehan (Vice-président, Division des enfants exploités, National Centre for Missing and Exploited Children (NCMEC), USA) – Arda Gerkens (PDG, Expertisebureau Online Kindermisbruik (EOKM), Pays-Bas) – Discussion avec l'intervention d'Uri Sadeh (Coordinateur, Unité Crimes contre les enfants, VCO/Direction de la criminalité organisée et émergente, INTERPOL) ► **Le problème : le droit à la vie privée contre les obligations positives de protection contre la criminalité** – Liora Lazarus (professeur de droit, Peter A. Allard School of Law, Université de Colombie-Britannique, Canada et membre surnuméraire, St. Anne's College, Oxford, Royaume-Uni) – Ella Jakubowska (Conseillère politique, European Digital Rights - EDRi) – Discussion ► **Solutions** – Réglementation intérimaire et solutions à long terme par l'Union européenne (Cathrin Baur-Bulst, Chef d'unité Sécurité à l'ère numérique, DG Home, Commission européenne) – Propositions concernant la Convention de Lanzarote (Maria José Castello-Branco, Vice-Présidente Membre du Comité de Lanzarote, Portugal) – Le programme néerlandais de partenariat public-privé et le point de vue de l'industrie de l'Internet (Michiel Steltman, directeur général, Dutch Digital Infrastructure Association, Pays-Bas) – Discussion avec les interventions du Général Eric Freyssinet (Commandant adjoint du Commandement du cyberespace de la Gendarmerie nationale, France) et de Fred Langford (Directeur de la technologie en ligne, OFCOM, UK) ► **Conclusions**
Mer, 17 Nov 14h00 - 15h50	**Atelier 7 - Ransomware** Langues : EN/FR/ES Objectif : Pendant la pandémie de COVID-19 et en raison des restrictions imposées, de plus en plus d'entreprises ont transféré leurs activités vers l'environnement en ligne, leurs employés travaillant depuis leur domicile. Alors que dans la plupart des environnements professionnels, des méthodes de protection sont en place pour contrer les cybermenaces, les ordinateurs personnels peuvent ne pas avoir le même niveau de conformité aux règles de sécurité Internet, laissant ainsi leurs utilisateurs sans défense contre les attaques de ransomware. Ces deux dernières années, les attaques par ransomware ont frappé fort, ciblant à la fois les postes de travail personnels mais aussi les infrastructures critiques, exposant ainsi les hôpitaux et les établissements médicaux aux attaques concentrées des cybercriminels. La réponse des autorités judiciaires et du secteur privé doit être adéquate pour relever les défis posés par cette forme croissante d'activité criminelle. L'atelier vise à fournir des recommandations sur la manière de se protéger contre cette forme de cybercriminalité et à fournir les outils nécessaires pour atténuer cette menace. Un autre objectif est de déterminer comment la coopération sur les ransomwares peut être davantage soutenue au niveau du Conseil de l'Europe.

	Modérateurs : Hein Dries (PDG de Vigilo Consult et expert en cybercriminalité dans le projet OCWAR-C) / James Shank (Architecte en chef des services communautaires, Team CYMRU et membre de la Ransomware Task Force (RTF)) Rapporteur : Matteo Lucchetti (Directeur de CYBER 4.0, Centre italien de compétences en cybersécurité) Secrétariat : Alexandru Cristea / Liliana Trofim (Projet iPROCEEDS-2, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Hein Dries et James Shank ► **Ransomware : menaces et modi operandi** – Une perspective du secteur privé sur les ransomwares, leurs menaces et leur évolution dans le temps (Alexandru Catalin Cosoi, Chief Security Strategist, Bitdefender) – La lutte contre les ransomwares en tant que service, partenariat public-privé (Dominik Helble, ancien enquêteur du BKA sur la cybercriminalité et responsable de la cybersécurité de Festo, Allemagne) ► **Ransomware : outils, réglementations, bonnes pratiques** – Atténuation des attaques de ransomware de grande envergure, l'affaire Colonial Pipeline (Nikhil Bhagat, procureur fédéral au sein du ministère américain de la justice) – No More Ransom, une perspective européenne de prévention et de lutte contre les ransomwares (Emmanuel Kessler, chef de l'équipe Prévention et sensibilisation, EUROPOL) ► **Conclusions**

Mer, 17 Nov 16h00 - 17h50	**Atelier 8 - Cybercriminalité, preuves électroniques et intelligence artificielle** Langues : EN/FR/ES Objectif : Les progrès rapides de l'IA soulèvent : ▪ risques supplémentaires de cybercriminalité (délinquants utilisant l'IA comme arme, IA détectant des vulnérabilités pour commettre des cybercrimes ou automatiser des attaques. L'IA en tant que cible manipulée par les délinquants) ▪ les questions de responsabilité pénale (qui est responsable des décisions prises et des crimes commis grâce à la technologie de l'IA ?) ▪ les défis complexes liés aux preuves électroniques (comment sécuriser et utiliser dans les procédures pénales les preuves électroniques liées à des délits impliquant l'IA ?) D'autre part, l'IA peut apporter des avantages à la réponse de la justice pénale à la cybercriminalité (amélioration de la cybersécurité, détection des attaques, aide à l'identification, à l'enquête et à la poursuite des délinquants, ou automatisation de la coopération nationale et internationale). Toutefois, cela soulève à son tour des questions supplémentaires (comment garantir l'État de droit et les garanties d'une procédure régulière ; quelles sont les implications sur la territorialité et la juridiction lorsque les enquêtes menées par l'IA traversent les frontières ?)

	Des organisations du monde entier travaillent actuellement sur des questions liées à l'intelligence artificielle, notamment le Conseil de l'Europe. Dans ce contexte, l'objectif de l'atelier est d'identifier les questions clés qui devraient être prises en compte lors de la conception de la future réponse de la justice pénale à la cybercriminalité et aux preuves électroniques en relation avec l'IA. Modérateur/s: Jan Kleijssen (Directeur de la société de l'information et de la lutte contre la criminalité, Conseil de l'Europe) Rapporteur : Tania Schröter (Chef d'unité adjoint, Droit pénal procédural, Direction générale de la justice et des consommateurs, Commission de l'Union européenne) Secrétariat : Martha Stickings / Gratiela Dumitrescu (GLACY+, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Jan Kleijssen (Conseil de l'Europe) ► **Cybercriminalité et intelligence artificielle : quelles sont les menaces et les défis, quelles sont les opportunités ?** – Usages malveillants et abus de l'intelligence artificielle (Aglika Klayn, spécialiste en cybercriminalité/coordinateur J-CAT, EC3, EUROPOL / Maria Eira, responsable de l'information et de la technologie, Centre pour l'intelligence artificielle et la robotique, Institut interrégional de recherche des Nations unies sur la criminalité et la justice / David Sancho, TrendMicro) – Techniques de Provenance Tech (Origin et C2PA) et leçons tirées des contre-mesures de désinformation (Ashish Jaiman, directeur de la gestion des produits, Bing Multimedia, Microsoft) – Discussion ► **L'IA, la cybercriminalité et le droit : les fondamentaux** – IA, cybercriminalité et droit pénal : qu'est-ce qui est nouveau et qu'est-ce qui ne l'est pas ? (Dennis Baker, professeur, faculté de droit de l'université De Montfort, Leicester, Royaume-Uni) – IA, preuve électronique et responsabilité pénale (Sabine Gless, rapporteur du CDPC sur l'IA et le droit pénal, professeur de droit pénal et de droit de la procédure pénale, Université de Bâle, Suisse) – Discussion ► **Conclusions**
Mer, 17 Nov 16h00 - 17h50	**Lightning talks I - Brèves interventions pour présenter des idées ou des projets** Langues : EN/FR/ES/PT/AR Modérateur/s : Elvio Salomon (Projet GLACY+, C-PROC, Conseil de l'Europe) / Elliot Mayhew - Global Forum on Cyber Expertise (GFCE)
Mer, 17 Nov 18h00 - 19h50	**Atelier 9 - Atelier régional pour l'Amérique latine et les Caraïbes : Coopération avec les prestataires de services** Langues : EN/ES/PT

	Objet : L'obtention d'informations sur les abonnés permettant d'identifier l'utilisateur d'une adresse de protocole Internet (IP) utilisée dans le cadre d'une infraction pénale ou le propriétaire d'un compte de messagerie ou de médias sociaux utilisé à des fins criminelles est cruciale pour toute autorité de justice pénale enquêtant sur la criminalité en ligne. Il en va de même pour les informations relatives à l'enregistrement d'un nom de domaine concernant le propriétaire d'un domaine Internet utilisé à des fins frauduleuses. Dans les situations d'urgence où des vies sont en danger, un accès rapide au contenu d'un compte peut également être nécessaire. Souvent, ces informations sont détenues par des fournisseurs de services dans d'autres juridictions. L'objectif de cet atelier est d'identifier les bonnes pratiques actuelles des autorités d'Amérique latine et des Caraïbes pour obtenir les données nécessaires à une enquête criminelle auprès de fournisseurs de services multinationaux et d'expliquer les nouvelles solutions qui pourraient bientôt être disponibles dans le cadre du nouveau protocole de la Convention de Budapest. Modérateur/s : Anthony Teelucksingh (Président du groupe de travail OEA/REMJA sur la cybercriminalité, Département de la Justice des Etats-Unis) Rapporteur : Dale Joseph (Spécialiste de la politique en matière de cybercriminalité, CARICOM IMPACS) Secrétariat: Catalina Stroe / Oana Tarus (GLACY+, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Anthony Teelucksingh (Président du groupe de travail OEA/REMJA sur la cybercriminalité, Département de la Justice des Etats-Unis) ► **Coopération avec des prestataires de services multinationaux** – La perspective chilienne (Mauricio Fernandez Montalban, directeur de l'unité spécialisée dans le blanchiment d'argent et le crime organisé du parquet national, Chili) – L'expérience brésilienne (Fernanda Teixeira Souza Domingos, procureur fédéral, coordinateur du groupe consultatif sur la cybercriminalité à la chambre pénale du parquet fédéral, Brésil) ► **Le 2ème protocole additionnel : vers une coopération renforcée avec les prestataires de services transfrontaliers** – Erica O'Neil (Computer Crime and Intellectual Property Section, United States Department of Justice) – Claudio Peguero (Inspecteur général de la police nationale, République dominicaine) ► **Comment améliorer la coopération entre les LEA et les prestataires de services dans les enquêtes criminelles dans la région ?** – Panel de discussions ouvertes modéré par Dale Joseph (spécialiste de la politique en matière de cybercriminalité, CARICOM IMPACS) ► **Conclusions**
JEU, 18 NOVEMBRE, AM : SESSIONS D'ATELIER	
Jeu, 18 Nov 7h00 - 8h50	**Atelier 10 - Atelier régional pour le Pacifique**

	Langue : EN Objectif : L'exploitation et les abus sexuels des enfants en ligne (OCSEA) constituent depuis de nombreuses années une violation majeure des droits des enfants. La pandémie de COVID-19, et l'augmentation du temps passé devant l'écran par chacun, a exacerbé la prévalence et les risques d'OCSEA, y compris dans la région Pacifique. Si des approches globales sont nécessaires pour prévenir l'OCSEA, et identifier, protéger et aider les victimes, une justice pénale efficace est un élément important de la réponse pour protéger les enfants contre l'OCSEA et traduire les délinquants en justice. L'objectif de cet atelier est de partager des informations sur la menace de l'OCSEA ainsi que les bonnes pratiques en termes de politiques, de législation, de capacités institutionnelles et de coopération nationale et internationale sur l'OCSEA. Modérateur/s : James Lutui (Directeur des poursuites publiques, Tonga) et Patricia Femia (Assistant State Counsel State Solicitor's Office Western Australia) Rapporteur : Ana Guerreiro (Conseillère de programme, Division des droits de l'enfant/Comité de Lanzarote, Conseil de l'Europe) Secrétariat : Catalina Stroe/ Sinziana Hanganu (GLACY+, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – James Lutui (Directeur des poursuites publiques, Tonga) ► **Etat des lieux : Menaces et tendances de l'OCSEA pendant la pandémie de COVID-19** – Matthew DOMPIER (Officier de renseignement criminel, Unité des crimes contre les enfants, INTERPOL) – Alexandru Caciuloiu (Conseiller en matière de cybercriminalité et de crypto-monnaies et coordinateur régional pour l'Asie du Sud-Est et le Pacifique, UNODC) ► **Réponses politiques dans la zone Pacifique pour protéger les enfants de l'OCSEA** – Haya Snobar (Directrice adjointe, Partenariats internationaux pour la protection de l'enfance, Ministère de l'Intérieur, Australie) – Sophie Harding (Directrice adjointe, Partenariats internationaux pour la protection de l'enfance, Département des affaires intérieures, Australie) – Tupou Kafa Vainikolo (Procureur de la Couronne, Bureau du procureur général, Tonga) ► **Comment assurer des réponses efficaces de la justice pénale à l'OCSEA** – Discussions ouvertes modérées par Alexandru Caciuloiu (conseiller en matière de cybercriminalité et de crypto-monnaies et coordinateur régional pour l'Asie du Sud-Est et le Pacifique, UNODC). ► **Conclusions**

Jeu, 18 Nov 9h00 - 10h50	**Atelier 11 - Renforcement des capacités : formation judiciaire durable sur la cybercriminalité et les preuves électroniques** Langues : EN/FR/ES/PT/AR

Objectif :	Étant donné que non seulement la cybercriminalité mais aussi tout type de crime peut impliquer des preuves sur un système informatique (preuves électroniques), tout juge ou procureur doit avoir les compétences nécessaires pour poursuivre ou juger des affaires impliquant de telles preuves. En 2009, le Conseil de l'Europe a développé un concept de formation à la cybercriminalité pour les juges et les procureurs. La mise en œuvre de ce concept a depuis été soutenue dans de nombreux pays, généralement en coopération avec les institutions nationales de formation judiciaire. Plus récemment, la mise en réseau des juges et procureurs formés dans le cadre de différents programmes a été encouragée. Afin de garantir qu'au fil du temps, tout juge ou procureur ait accès et puisse participer à une formation pertinente, la durabilité de ces programmes et les approches stratégiques de la formation sont essentielles. Un autre défi est qu'en raison de la pandémie de COVID, une grande partie de la formation n'est désormais disponible qu'en ligne. Pour cette raison, C-PROC développe actuellement une plateforme de formation en ligne qui sera mise à la disposition des pays du projet. L'objectif de cet atelier est d'examiner comment la durabilité de la formation judiciaire sur la cybercriminalité et les preuves électroniques peut être assurée par des approches stratégiques de la formation, la mise en réseau des formateurs et des outils tels que la plateforme en ligne pour la formation judiciaire.
Modérateur/s :	Marcos Salt (professeur de droit pénal, directeur des études de troisième cycle sur la cybercriminalité et les preuves électroniques, Université de Buenos Aires, Argentine)
Rapporteur :	Angela Marques Rodrigues (Juge, Conseil Supérieur de la Magistrature, Cabo Verde)
Secrétariat:	Catalina Stroe / Elena Floroiu (Projet GLACY+, C-PROC, Conseil de l'Europe)

► **Introduction et objectif de l'atelier**

- Marcos Salt (professeur de droit pénal, directeur des études de troisième cycle sur la cybercriminalité et les preuves électroniques, Université de Buenos Aires, Argentine)

► **Stratégies de formation en matière de cybercriminalité : une enquête**

- Hania Helweh (Présidente du Tribunal de Première Instance du Nord Liban)
- Discussions ouvertes sur les résultats de l'enquête

► **Façonner l'avenir**

- Rapport d'activité du Réseau international de formateurs judiciaires sur la cybercriminalité et les preuves électroniques (Sharon Segura Rodriguez, Procureur, Unité de renforcement des capacités et de supervision, point focal du Costa Rica pour le Réseau international de formateurs judiciaires)
- Rapport d'étape sur la plateforme de formation e-learning sur la cybercriminalité du Conseil de l'Europe (Victor Voelzow, consultant du Conseil de l'Europe)

► **Comment élaborer et dispenser une formation judiciaire durable**

- Discussions ouvertes modérées par Marcos Salt et Catalina Stroe

► **Conclusions**

Jeu, 18 Nov 9h00-10h50	**Atelier 12 - Cybercriminalité : Victimes** Langues : EN/FR/ES Objectif : La cybercriminalité est un type de criminalité de plus en plus avancé sur le plan technologique et qui connaît une croissance rapide. Elle est extrêmement coûteuse, touche prétendument un très grand nombre de victimes et a un impact psychologique, ce qui rend les effets de la victimisation dans le cyberespace difficiles à quantifier. On comprend mal qui sont les victimes (individus et organisations) et comment la cybercriminalité affecte les différentes catégories de victimes. Par rapport à la criminalité traditionnelle, la cyber-victimisation comporte des éléments d'*accessibilité (les* auteurs peuvent atteindre un nombre important de victimes), d'*anonymat*, et donc de *détectabilité limitée* (parfois, les victimes ne sont même pas conscientes d'avoir été victimisées), et est également *difficile à contraindre*, en raison de la vitesse étonnante avec laquelle les données sont partagées et de la volatilité des preuves possibles. Cet atelier examinera qui sont les victimes de la cybercriminalité (individus et organisations) et se penchera sur la réponse de la justice pénale mais aussi sur les remèdes alternatifs (tels que la justice réparatrice) qui leur sont disponibles. Modérateur : Jeffrey DeMarco (Directeur adjoint de la connaissance et des idées, Victim Support, Royaume-Uni) Rapporteur : Miriam Bahamonde Blanco (Procureur principal, Ministère de la Justice d'Espagne) Secrétariat : Cecilia Popa (CyberEast, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Jeffrey DeMarco ► **Qui sont les victimes de la cybercriminalité ?** – Une analyse des données d'enquête sur les victimes (Jan Van Dijk, membre de l'Institut néerlandais pour l'étude de la criminalité et de l'application de la loi) – Les victimes de la cybercriminalité : qui sont-elles et quels sont les problèmes (Marianne Junger, Université de Twente) – Discussion ► **Vers une typologie des victimes de la cybercriminalité ?** – Manuels de soutien aux victimes de la cybercriminalité (Ricardo Salgueiro Dos Santos Fernandes Estrela, Association portugaise d'aide aux victimes) – Les entreprises victimes de la cybercriminalité : Rapport de l'ENISA sur la cybersécurité pour les PME - Défis et recommandations (Anna Sarri, Cybersecurity Officer, ENISA) – Discussion ► **Obtenir justice pour les victimes de la cybercriminalité** – La justice pénale pour les victimes de la cybercriminalité - Exemple de la cyberviolence (Gareth Sansom, Ministère de la Justice, Canada)

	– La justice réparatrice peut-elle s'adresser aux victimes de la cybercriminalité ? (Emanuela Biffi, Chargée de projet et d'événements, Forum européen pour la justice réparatrice) – Discussion ► **Conclusions**
Jeu, 18 Nov 11h00 - 12h50	**Atelier 13 - Renforcement des capacités : Guides et outils** Langues : EN/FR/ES Objectif : Le renforcement des capacités en matière de cybercriminalité et de preuves électroniques est un processus complexe qui demande beaucoup de temps et de ressources et qui implique un grand nombre d'organisations et de praticiens. Étant donné la croissance de la cybercriminalité et le fait que tout crime peut impliquer des preuves électroniques, tout enquêteur, procureur ou juge sera confronté à de tels cas et doit être équipé des compétences nécessaires pour les traiter. Un certain nombre de guides et d'autres outils ont été élaborés par le Conseil de l'Europe et d'autres organisations ces dernières années, afin d'aider les praticiens de la justice pénale à acquérir ces compétences. Ces guides et outils peuvent compléter les programmes de formation ou servir à l'auto-apprentissage. L'objectif de cet atelier est d'accroître la connaissance des participants sur ces guides et outils et de promouvoir leur adaptation pour répondre aux besoins nationaux. Modérateur/s: Michele Socco (Chargé de mission, Commission européenne, Direction générale de la migration et des affaires intérieures, Unité "Sécurité à l'ère numérique") Rapporteur : Nayia Barmpaliou (Directrice, Cyber Lab International, Institut d'études de sécurité de l'Union européenne (IESUE)) Secrétariat: Virgil Spiridon (Chef des opérations, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** – Michele Socco (Chargé de mission, Commission européenne, Direction générale de la migration et des affaires intérieures, Unité "Sécurité à l'ère numérique") ► **Éléments clés du renforcement des capacités en matière de cybercriminalité** – Craig Jones (Directeur de la cybercriminalité, INTERPOL) – Renata Delgado-Schenk (Responsable du programme de lutte contre la cybercriminalité, UNODC) ► **Guides et outils : élaboration, mise en œuvre et avantages** – Projet SIRIUS - Robert Laid (Chef de projet, EUROJUST) - Juan De Dios Toledo Martinez (Chef de projet, EUROPOL) – Wouter Veenstra (responsable de la sensibilisation et des partenariats mondiaux, Forum mondial sur la cyber-expertise) – Conseil de l'Europe : Guides C-PROC - Victor Voelzow (consultant du CoE)

	- Safia El Moutaouakil (Chef du laboratoire numérique régional, Maroc) – Terry Wilson (Directeur du partenariat mondial, Global Cyber Alliance) ► **Conclusions**

Jeu, 18 Nov 11h00 - 12h50	**Atelier 14 - Cybercriminalité : Délinquants** Langues : EN/FR/ES Objectif : Les auteurs de cybercrimes sont aussi divers et complexes que les cybercrimes qu'ils commettent. Par exemple, ils viennent d'horizons différents et ont des motivations différentes (égoïstes, techniques, monétaires, idéologiques, politiques, professionnelles, vengeresses, sexuelles ou autres). Il peut s'agir de criminels professionnels ou non, d'individus ou de membres de groupes ou de réseaux organisés (exemple des menaces persistantes avancées). Certains peuvent commettre des crimes pour leur propre compte ou mettre leurs services à la disposition d'autres personnes, et d'autres peuvent être soutenus par des acteurs étatiques ou être des acteurs étatiques. Une meilleure compréhension des types d'auteurs, de leurs motivations et de leurs techniques peut contribuer à la prévention de la cybercriminalité et à une réponse plus efficace de la justice pénale. L'objectif de cet atelier est de contribuer à cette meilleure compréhension et d'initier les étapes vers une typologie des délinquants. Modérateur/s : Dong Uk Kim (Officier spécialisé, INTERPOL Cybercriminalité, Projet GLACY+) Rapporteur : Silvia Portesi (Expert en cybersécurité, Agence de l'Union européenne pour la cybersécurité, ENISA) Secrétariat: Ana Vlad / Giorgi Jokhadze (Projet CyberEast, C-PROC, Conseil de l'Europe) ► **Introduction et objectif de l'atelier** ► **Qui sont les auteurs de violences ? Vers une typologie** – Réseaux cybercriminels à motivation financière (Enregistrement : Rutger Leukfeldt, chercheur principal, Institut néerlandais pour l'étude du crime et de l'application de la loi (NSCR), et directeur du Centre d'expertise en cybersécurité, Université des sciences appliquées de La Haye) – Typologies des délinquants de la cybercriminalité dans les études de cas (Youngjin Song, professeur, Centre international de recherche sur la cybercriminalité, Université de la police nationale de Corée) – Conclusions d'EUROPOL (Emmanuel Kessler, chef de l'équipe Prévention et sensibilisation, EC3, le centre de lutte contre la cybercriminalité d'Europol) – Délinquants : Principales menaces pour l'Europe en 2021 (Georgios Chatzichristos, Officier en cybersécurité, Unité de coopération opérationnelle, ENISA) – Le point de vue du secteur privé (Aisling Kelly, Senior Counsel, Law Enforcement & National Security, Microsoft) – Questions et réponses et discussion ► **Réponse de la justice pénale aux auteurs de crimes soutenus par l'État ?**

	– La cybercriminalité soutenue par l'État et la réponse de la justice pénale américaine (Sean Newell, chef adjoint (cyber), section du contre-espionnage et du contrôle des exportations, division de la sécurité nationale, ministère de la Justice des États-Unis) – Point de vue du secteur privé (Aisling Kelly, Senior Counsel, Law Enforcement & National Security, Microsoft) – Discussion ► **Un autre regard : la prévention** – Prévention de la cybercriminalité et travail avec les délinquants (Floor Jansen, National High Tech Crime Unit, Dutch Police) – Discussion ► **Conclusions**
Jeu, 18 Nov 13h00 - 13h45	**Lightning talks II - Brèves interventions pour présenter des idées ou des projets** Langues : EN/FR/ES/PT/AR Modérateur/s : Elvio Salomon (Projet GLACY+, C-PROC, Conseil de l'Europe) / Elliot Mayhew - Global Forum on Cyber Expertise (GFCE)
13h45 - 14h30	*Pause*
JEUDI 18 NOVEMBRE APRES-MIDI : SEANCES PLENIERES	
Jeu, 18 Nov 14h30 - 15h30	**Outlook 1 : Cybercriminalité - menaces et tendances** Langues : EN/FR/ES Objectif : Les rapports publiés par les organisations des secteurs public et privé montrent une image en évolution rapide - et parfois contradictoire - de la cybercriminalité et des cyberattaques. L'objectif de cette session est d'arriver à des prédictions concernant les menaces et tendances cybernétiques en 2022/2023 et les défis auxquels les autorités de justice pénale doivent se préparer. Modérateur/s : Martha Stickings (GLACY+, C-PROC, Conseil de l'Europe) Secrétariat : Gratiela Dumitrescu / Floriane Spielman (Projet GLACY+/Octopus, C-PROC, Conseil de l'Europe) ► **Introduction** – Martha Stickings (GLACY+, C-PROC, Conseil de l'Europe) ► **Panel sur les menaces actuelles, les prévisions pour 2022/2023 et le rôle de la réponse de la justice pénale** – IOCTA (Emmanuel Kessler, Chef d'équipe Prévention et Sensibilisation, EC3, EUROPOL) – La cybercriminalité au Japon (Ko Ikai, Directeur du Bureau d'enquête sur la cybercriminalité, Agence nationale de police du Japon) – Groupe de travail anti-hameçonnage (Peter Cassidy, Secrétaire général, APWG) – Rapport Microsoft Digital Defense : l'état de la cybercriminalité (Uwe Rasmussen, avocat principal de Microsoft sur les logiciels malveillants, EMEA)

	– BITKOM (Sebastian Artz, responsable de la cybersécurité et de la sécurité de l'information, BITKOM) ► **Conclusions**
Jeu, 18 Nov 15h30-16h15	**Outlook 2 : Droits de l'homme et état de droit dans le cyberespace** Langues : EN/FR/ES Objectif : La cybercriminalité étant une menace pour les droits de l'homme, les gouvernements ont non seulement l'obligation "négative" de s'abstenir d'interférer avec ces droits (sauf si certaines conditions sont remplies), mais il est de plus en plus considéré que les gouvernements ont une obligation "positive" de protéger les individus contre l'interférence de tiers dans leurs droits. Cela inclut, par exemple, l'obligation de mettre en place des moyens efficaces pour protéger les individus contre la cybercriminalité par le biais du droit pénal. Cependant, ces moyens sont également soumis à des conditions. Cette session discutera de ce qu'il faut faire pour que la réponse de la justice pénale soit efficace et qu'elle réponde en même temps aux exigences des droits de l'homme et de l'état de droit. Modérateur: Isabelle Servoz-Gallucci (Secrétaire du Comité de la Convention 108 (T-PD), Chef de l'Unité de la protection des données, Conseil de l'Europe) Secrétariat : Martha Stickings (GLACY+, C-PROC, Conseil de l'Europe) ► **Introduction** – Isabelle Servoz-Gallucci ► **Panneau** – Keynote : Robert Spano (Président de la Cour européenne des droits de l'homme) – Nnenna Ifeanyi-Ajufo (vice-présidente du groupe d'experts en cybersécurité de l'Union africaine / maître de conférences en droit et technologie, faculté de droit, université de Swansea, Royaume-Uni) – Liora Lazarus (professeur de droit, Peter A. Allard School of Law, The University of British Columbia, Canada et membre surnuméraire, St. Anne's College, Oxford, Royaume-Uni) ► **Conclusions**
16h15-16h30	*Pause santé*
Jeu, 18 Nov 16h30-17h30	**Perspective 3 : Coopération contre la cybercriminalité en 2022** Langues : EN/FR/ES Objectif : Après avoir discuté des problèmes et des défis, mais aussi partagé des expériences et des bonnes pratiques tout au long de cette conférence, l'objectif de cette session est de permettre aux organisations impliquées dans les politiques, l'établissement de normes et le renforcement des capacités en matière de cybercriminalité de présenter leurs intentions sur la façon de renforcer la coopération internationale en matière de cybercriminalité et de preuves électroniques en 2022.

	Modérateur/s : Alexander Seger (Chef de la Division de la cybercriminalité, Conseil de l'Europe) Secrétariat : Celine Dewaele (Division de la cybercriminalité, Conseil de l'Europe) ► **Introduction** ► **Panneau** – UNODC (Neil Walsh, chef de la section cybercriminalité et lutte contre le blanchiment d'argent, Office des Nations unies contre la drogue et le crime) – Commission de l'Union africaine (Abdul-Hakeem Ajijola, président du groupe d'experts en cybersécurité de l'Union africaine) – [TBC : Fédération de Russie (Ernest Chernukhin, Chef de section, Département de la sécurité de l'information internationale, Ministère des affaires étrangères de la Fédération de Russie)]. – Organisation des États américains (Anthony Teelucksingh, président du groupe de travail OEA/REMJA sur la cybercriminalité, ministère américain de la Justice) – Union européenne (Cathrin Baur-Bulst, Chef d'unité Sécurité à l'ère numérique, DG Home, Commission européenne) ► **Conclusions**
Jeu, 18 Nov 17h30-18h00	**Conclusions de la conférence**