Conférence Octopus 2023

13-15 décembre 2023 - Bucarest, Roumanie

Programme de la conférence - Aperçu

Version 8 décembre 2023

MER, 13 DECEMBRE 2023			
8h30-9h30	*Café de bienvenue et inscription*		
9h30-13h00 Pause café *10h30-11h00*	**Session plénière d'ouverture – Salle Rosetti** EN/FR/ES ► Cybercriminalité et preuves électroniques : perspectives mondiales ► Cybercriminalité et preuves électroniques des crimes de guerre : Leçons tirées de l'agression russe contre l'Ukraine ► Cybercriminalité contre liberté d'expression ► Le cadre de la Convention sur la cybercriminalité : Mise à jour		
13h00-14h30	*Photo de groupe et pause déjeuner*		
14h30-16h00	**Atelier 1:** EN/FR/ES/RO ► État de la législation sur la cybercriminalité dans le monde Salle Iorga	**Atelier 2:** EN/FR/ES/RO ► Partage spontané d'informations Salle Brătianu	**Atelier 3:** EN/FR/ES ► Détection automatique des matériels d'exploitation et d'abus sexuels concernant des enfants Salle Bălcescu
16h00-16h30	Pause-café		
16h30-18h00	**Atelier 4:** EN/FR/ES/RO ► Synergies entre les conventions de Budapest, de Lanzarote, d'Istanbul et sur la traite des êtres humains Salle Iorga	**Atelier 5:** EN/FR/ES/RO ► L'interaction entre la cybercriminalité et les enquêtes financières Salle Bălcescu	**Atelier 6:** EN/FR/ES ► Cybercriminalité et intelligence artificielle Salle Brătianu
18h00-20h00	Evénement social – Salle Take Ionescu		

JEU, 14 DECEMBRE				
9h30-13h00 *[pause-café 11h00-11h30]*	**Événement du projet :** EN ► De CyberEAST à CyberEast+ Salle Iorga		**Événement du projet :** EN ► De iPROCEEDS-2 à CyberSEE Salle Bălcescu	**Événement du projet :** EN/FR/ES/PT (passif) ► De GLACY+ à GLACY-e Salle Brătianu
13h00-14h30 Pause déjeuner				
14h30-15h30			**Événement du projet :** EN/FR/ES ► De CyberSouth à CyberSouth+ Salle Bălcescu	
15h30-16h00 Pause-café				
16h00-18h00	**Discussions éclair** EN/FR/ES/RO Salle Iorga			
VENDREDI 15 DECEMBRE				
9h30-11h00	**Atelier 7:** EN ► Atelier régional pour l'Asie Salle des Droits Humains	**Atelier 8:** EN ► Atelier régional pour le Pacifique Salle Bălcescu	**Atelier 9:** EN/FR/ES/ PT (passif) ► Atelier régional pour l'Afrique Salle Brătianu	**Atelier 10:** EN/ES/RO ► Atelier régional pour l'Amérique latine et les Caraïbes Salle Iorga
11h00-11h30	*Pause-café*			

11h30-13h00	**Atelier 11:** EN/FR/ES/RO ► Le renforcement des capacités pour changer la donne : qu'est-ce qui fait la différence ? Salle Iorga	**Atelier 12:** EN/FR/ES/RO ► Xénophobie et racisme en ligne contre liberté d'expression Salle des Droits Humains	**Atelier 13:** EN/FR/ES ► Renforcer les points de contact 24/7 Salle Bălcescu	**Atelier 14:** EN/FR/ES/RO ► L'interaction entre la cybersécurité et la cybercriminalité Salle Brătianu
13h00-14h30	*Pause déjeuner*			
14h30-17h00	**Plénière de clôture et conclusions – Salle Rosetti** EN/FR/ES ► Points essentiels des ateliers ► Discours principaux ► Événement de la Convention ► Leçons tirées de 10 années de programme de lutte contre la cybercriminalité du Bureau du Conseil de l'Europe (C-PROC) ► Perspectives 2024 et conclusions			
18h00	*Fin de la conférence*			

Programme détaillé

MER, 13 DECEMBRE 2023

9h30-13h00

Session plénière d'ouverture *(diffusion en direct)*

Langues : EN/FR/ES

Modérateur: Alexander Seger, Chef de la division de la cybercriminalité, Conseil de l'Europe

Secrétariat : Nina Lichtner, Cheffe de projet Octopus, Conseil de l'Europe

► **Ouverture [9h30-9h45]**

- Benone-Marian Matei, inspecteur général de la police Roumaine
- Dmytro Verbytskyy, procureur général adjoint de l'Ukraine
- Patrick Penninckx, chef du service de la société de l'information, Conseil de l'Europe

► **Cybercriminalité et preuves électroniques : perspectives mondiales (9h45-10h30)**

- Erica O'Neil, Cheffe adjointe, Section de la criminalité informatique et de la propriété intellectuelle, Département de la justice des États-Unis
- Carlo Diaz, Procureur général, Costa Rica
- Linda S Folaumoetu'i, procureur général, Tonga
- Pedro Verdelho, Président du Comité de la Convention sur la cybercriminalité, Portugal
- Jamila Akaaga Ade, Counter Ransomware Initiative (CRI), chef de l'unité de lutte contre la cybercriminalité, Ministère fédéral de la justice, Nigeria
- Claudio Peguero, Cyber-ambassadeur, République dominicaine

Pause café
10h30-11h00

► **Cybercriminalité et preuves électroniques des crimes de guerre : Leçons tirées de l'agression russe contre l'Ukraine [11h00-11h45]**

- Dmytro Verbytskyy, Procureur général adjoint de l'Ukraine
- Aisling Kelly, avocate générale adjointe, application de la loi et sécurité nationale, Europe, Microsoft
- Commentaires : Zahid Jamil, Pakistan / Markko Künnapu, Estonie / Giorgi Jokhadze (Conseil de l'Europe)

► **Cybercriminalité contre liberté d'expression [11h45-12h30]**

- Modérateur : Patrick Penninckx, Chef du Service de la Société de l'Information, Conseil de l'Europe
- Introduction à la question : Krešimir Kamber, Avocat, Cour européenne des droits de l'homme, Strasbourg
- Panel : Jayantha Fernando, Sri Lanka / Gatembu Kairu, Kenya / Gareth Sansom, Canada

► **Le cadre de la Convention sur la cybercriminalité : Mise à jour [12h30-13h00]**

- Alexander Seger, Conseil de l'Europe

14h30-16h00	**Atelier 1 - État mondial de la législation en matière de cybercriminalité** *(diffusion en direct)* Langues : EN/FR/ES/RO Objectif : La législation est 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, souvent en s'inspirant de la Convention de Budapest sur la cybercriminalité. Cependant, la législation sur la cybercriminalité doit également répondre aux exigences des droits humains 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 matière de législation sur la cybercriminalité et d'identifier les risques et les défis éventuels. Modérateur : Zahid Jamil, avocat, Jamil & Jamil, Pakistan Rapporteur : Fernanda Teixeira Domingos, Bureau du procureur, Brésil Secrétariat : Giorgi Jokhadze / Tatiana Bastrighin ► **Introduction et objectif de l'atelier [5 min]** – Remarques du modérateur – Secrétariat ► **De 2013 à 2023 : Dix ans de progrès dans la législation sur la cybercriminalité et la preuve électronique [10 min]** – Résultats d'une enquête menée par le Bureau du programme sur la cybercriminalité du Conseil de l'Europe (Giorgi Jokhadze, C-PROC) ► **Exemples de réformes récentes [30 min]** – Jamila Ade, Nigeria – Germán Ortega, Équateur – Glenys E. Andrews, Fidji ► **Défis et risques [40 min]** – Deuxième protocole additionnel : législation de mise en œuvre – Ioana Albani, Roumanie – Garanties des droits de l'homme/liberté d'expression – Jan Kralik, Conseil de l'Europe – Discussion : ce qu'il faut faire et ne pas faire en matière de législation sur la cybercriminalité et les preuves électroniques (discussion ouverte et exemples) ► **Conclusions [5 min]**

14h30-16h00	**Atelier 2 - Partage spontané d'informations** Langues : EN/FR/ES/RO Objectif : Les autorités de justice pénale possèdent souvent des informations précieuses qu'elles pensent pouvoir aider les autorités d'un autre pays dans le cadre d'une enquête criminelle, mais dont ces autres autorités n'ont pas connaissance. Les parties à la Convention de Budapest peuvent partager ce type d'informations en vertu de l'article 26 sur les "informations spontanées" : *"Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre...."* La pertinence de l'article 26 s'est accrue au fil du temps, notamment dans le cadre d'affaires liées au dark web ou au partage de données extraites de communications cryptées. L'objectif de l'atelier est d'identifier les pratiques actuelles d'utilisation de l'article 26 de la Convention sur la cybercriminalité. Modérateurs : Jan Kerkhofs, Magistrat fédéral, Chef de l'Unité Cyber, Parquet fédéral belge Antonio Segovia Arancibia, Professeur de droit pénal transnational, Université UAI, Chili Rapporteurs : Jorge Espina, Président de l'équipe de lutte contre la cybercriminalité, Membre national adjoint de l'Espagne, Eurojust Catalina Stroe, gestionnaire de programme, Bureau du programme sur la cybercriminalité du Conseil de l'Europe Secrétariat : Équipe GLACY ► **Introduction et objectif de l'atelier [5 min]** – Jan Kerkhofs, magistrat fédéral, chef de l'unité cybernétique, parquet fédéral belge ► **Application et interprétation du concept d'échange spontané d'informations entre les autorités judiciaires des États membres de l'UE et des pays ayant un procureur de liaison présent à Eurojust [10 min].** – Sofia Mirandola, conseillère en coopération judiciaire à l'unité de traitement des dossiers, département des opérations, Eurojust ► **Table ronde sur l'utilisation de l'article 26 de la Convention par les Parties fournissant des informations : quelles sont les procédures et les conditions ? [35 min]** – Benjamin Fitzpatrick, Senior Counsel, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice – Débats ouverts - modérés par Jan Kerkhofs

	► **Table ronde sur la réception d'informations spontanées : Comment l'utiliser comme preuve ? [35 min]** – Anastasiia Ponarina, Senior International Cooperation Officer, Department of Cybersecurity, State Security Service, Ukraine – Esteban Aquilar Vargas, procureur, coordinateur de l'unité de lutte contre la cybercriminalité, ministère public, Costa Rica – Philippines (à confirmer) – Débats ouverts - modérés par Antonio Segovia Arancibia ► **Conclusions des rapporteurs [10 min]** – Jorge Espina, président de l'équipe de lutte contre la cybercriminalité, membre national adjoint de l'Espagne, Eurojust – Catalina Stroe, gestionnaire de programme, Bureau du programme sur la cybercriminalité du Conseil de l'Europe
14h30-16h00	**Atelier 3 - Détection automatique des matériels d'exploitation et d'abus sexuels concernant des enfants** Langues : EN/FR/ES Objectif : Au cours de la dernière décennie, des fournisseurs de services multinationaux ont déployé une technologie de détection automatique des matériels d'abus sexuels sur enfants (CSAM) téléchargés ou diffusés par l'intermédiaire de leurs services. Des dizaines de millions de documents à caractère sexuel ont ainsi été identifiés et signalés, ce qui a souvent permis de sauver des victimes et d'identifier et de poursuivre des auteurs d'abus sexuels 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 humains, par exemple parce qu'elles portent atteinte à la confidentialité des communications, impliquent le transfert transfrontalier de données à caractère personnel ou violent les exigences d'une procédure régulière. L'objectif de l'atelier est de poursuivre la recherche de solutions permettant 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 CSAM avec les garanties nécessaires en matière de respect de la vie privée, de protection des données et d'État de droit. Modérateur : Maria José Castello-Branco, Présidente du Bureau du Comité de Lanzarote Rapporteur : Ana Elefterescu, Conseil de l'Europe Secrétariat : Naomi Trewinnard, Conseillère juridique, Secrétariat du Comité de Lanzarote Nina Lichtner, gestionnaire de programme, projet Octopus, Conseil de l'Europe ► **Introduction et objectif de l'atelier [5 min]** – Réflexion et progrès après l'atelier de la conférence Octopus 2021

	► **Progrès dans la détection automatisée et l'optimisation des rapports** – Christophe Boissier, INTERPOL – Susanna Pettersson, ECPAT Suède – Philip Attwood, Director of Impact, Child Rescue Coalition [online] ► **Renforcer les obligations et relever les défis** – Discussion avec le public ► **Solutions de collaboration et mise en œuvre des politiques** – Ms Soyoung Park, Korea Communications standards Commission [online] – Discussion avec le public ► **Conclusions [10 min]**
[13 déc, 16h30-18h00]	**Atelier 4 - Synergies entre les conventions de Budapest, de Lanzarote, d'Istanbul et sur la traite des êtres humains pour un cyberespace plus sûr** *(diffusion en direct)* Langues : EN/FR/ES/RO Objectif : Les normes des conventions maintenues par le Conseil de l'Europe dans les domaines de la cybercriminalité, de la protection des enfants contre les abus sexuels, de la traite des êtres humains et de la violence à l'égard des femmes ne sont pas simplement complémentaires, mais visent à encourager le travail entre les autorités de justice pénale, les responsables de la protection et les décideurs politiques afin d'assurer une meilleure justice pénale et des actions connexes dans ces domaines. Les infractions relevant du droit matériel, l'utilisation d'outils procéduraux pour les enquêtes et le travail de prévention/protection avec les victimes et les témoins ne sont que des exemples où l'harmonisation serait essentielle, tandis que des concepts tels que l'action contre la cyberviolence pourraient servir à indiquer où et comment de telles synergies devraient fonctionner. L'objectif de cet atelier est de renforcer les synergies entre quatre conventions différentes, mais interconnectées : - Convention sur la cybercriminalité (STE n° 185) - Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201) - Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE n° 210) - Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains (STCE n° 197) Modérateur : Miriam Bahamonde Blanco, Ministère de la Justice, Espagne Rapporteur : Ovidiu Majina, Division de l'enfance, Conseil de l'Europe Secrétariat: Giorgi Jokhadze / Ana Vlad

	► **Introduction et objectif de l'atelier [5 min]** – Remarques du modérateur – Secrétariat ► **Action en matière de justice pénale : nécessité de combler les lacunes avant de rechercher des synergies [40 min]** Interventions de : – Étude du Conseil de l'Europe sur les aspects de droit matériel des trois conventions : Budapest, Istanbul, Lanzarote (Betty Shave, consultante T-CY) – Perspective américaine : faire fonctionner les normes ensemble (Nate Brooks, ICHIP Zagreb, USDOJ) Avis de la commission : – Judith Herrnfeld, Bureau T-CY – Naomi Trewinnard, Comité de la Convention de Lanzarote – María Rún Bjarnadóttir, GREVIO (*en ligne*) – Mesut Bedirhanoglu, DGII : Direction générale de la démocratie et de la dignité humaine, Traite des êtres humains (GRETA) ► **Travail sur la prévention et la protection : une perspective différente [30 min]** Exemples de bonnes (et mauvaises) pratiques/interventions des panels : – Judith Herrnfeld, Bureau T-CY – Naomi Trewinnard, Comité de la Convention de Lanzarote – María Rún Bjarnadóttir, GREVIO (*en ligne*) – Mesut Bedirhanoglu, DGII : Direction générale de la démocratie et de la dignité humaine, Traite des êtres humains (GRETA) – Exemples tirés de la salle ► **Lutte contre la cyberviolence : potentiel de synergies [10 min]** – Le concept de cyberviolence : un "pont" entre ces traités ? – Discussion et exemples : points de vue des comités présents ► **Conclusions [5 min]**
[13 déc, 16h30-18h00]	**Atelier 5 - L'interaction entre la cybercriminalité et les enquêtes financières** Langues : EN/FR/ES/RO Objectif : L'établissement d'une collaboration efficace entre les autorités de justice pénale qui enquêtent sur la cybercriminalité et les institutions responsables des enquêtes financières est essentiel pour protéger les sociétés contre les activités criminelles. L'objectif de l'atelier est d'identifier les pratiques de collaboration, de favoriser la coopération nationale et internationale, les modèles efficaces de travail en équipe inter-agences et les principes régissant l'échange d'informations et de

	preuves entre les experts de la criminalité financière et de la cybercriminalité. Modérateur : Robert Golobinek, Ministère de la Justice Slovénie Rapporteur : Goran Jankoski, Banque nationale de la République de Macédoine du Nord Secrétariat : Daniel Cuciurianu, gestionnaire de programme, Conseil de l'Europe / équipe iPROCEEDS-2 ► **Introduction et objectif de l'atelier [5 min]** – Remarques du modérateur – Secrétariat ► **Flux de capitaux criminels en ligne et typologies de blanchiment d'argent [20 min]** – Camelia Lopez, conseillère juridique, Global ICHIP, Dark Web et Cryptocurrency, Ministère de la justice des États-Unis – Max Braun, Directeur, Bureau du Procureur Général, CRF Luxembourg ► **Coopération en matière de recherche, de saisie et de confiscation des produits de la criminalité en ligne [20 min]** – Max Braun, Directeur, Bureau du Procureur Général, CRF Luxembourg – Camelia Lopez, conseillère juridique, Global ICHIP, Dark Web et Cryptocurrency, ministère de la justice des États-Unis ► **Nouveaux outils et techniques d'investigation financière dans les affaires de cybercriminalité [35 min]** – Kārlis Pūce, analyste principal, CRF Lettonie – Horacio J. Azzolin, Procureur, Unité spécialisée dans la cybercriminalité UFECI, Argentine ► **Conclusions du rapporteur [10 min]** – Goran Jankoski, Banque nationale de la République de Macédoine du Nord
[13 déc, 16h30-18h00]	**Atelier 6 - Intelligence artificielle générative : menaces et avantages pour la justice pénale** Langues : EN/FR/ES Objectif : L'intelligence artificielle dans le secteur de la justice pénale peut à la fois représenter une menace sérieuse et renforcer la lutte contre la cybercriminalité. L'IA générative peut fournir des moyens efficaces de détecter les délits ou d'apporter une aide aux enquêtes en analysant de grandes quantités de données, mais elle peut aussi être détournée à des fins criminelles. Des données falsifiées (telles que les deep fakes) peuvent même être présentées comme preuves devant les tribunaux. L'objectif de cet atelier est d'examiner (a) les menaces criminelles que

	l'IA générative peut représenter pour le secteur de la justice pénale, (b) son rôle dans la lutte contre la cybercriminalité, et (c) les questions clés qui doivent être prises en compte dans l'évaluation des preuves électroniques générées par l'IA. Modérateur : Patrick Penninckx, Chef du Service de la Société de l'Information, Conseil de l'Europe Rapporteur : Hon. Hania EL HELWEH, Juge, Présidente du Tribunal de Première Instance, Nord du Liban Secrétariat : CyberSud et Secrétariat T-CY ► **Introduction et objectif de l'atelier [5 min]** – Patrick Penninckx, Chef du service Société de l'information, Conseil de l'Europe ► **Cybercriminalité et IA générative : menaces et opportunités [40 min]** – Emmanuel Kessler, Chef d'équipe - prévention/sensibilisation, Europol – Antonio Farelo, Responsable du laboratoire d'IA responsable (IRAIL), Centre d'innovation d'INTERPOL – Discussion ► **Aborder l'IA générative comme preuve électronique : questions clés, menaces et avantages [35 min]** – Sabine Gless, rapporteur du CDPC sur l'IA et le droit pénal, professeur de droit pénal et de procédure pénale, Université de Bâle, Suisse – Krešimir Kamber, Conseiller du Président et du Greffier, Cour européenne des droits de l'homme – Mario Lara Orellana, Directeur du département du développement institutionnel au sein de la branche administrative du Pouvoir judiciaire du Chili – Discussion ► **Conclusions [10 min]**
JEU, 14 DECEMBRE	
9h30-15h30 Pause café *11h00-11h30* *Pause déjeuner* *13h00-14h30*	**Événement du projet : De CyberEast à CyberEast+** Langues : EN Objectif : Cet événement est la conférence de clôture du projet CyberEast et ouvre la voie au projet de suivi CyberEast+. Il suivra les thèmes du projet, à savoir la législation et les politiques, le renforcement des capacités et la coopération. Il racontera l'histoire de CyberEast du point de vue des partenaires nationaux en démontrant l'impact et la pertinence du projet pour améliorer leurs capacités en matière de cybercriminalité et de preuves électroniques. La Commission européenne et le Conseil de l'Europe évalueront et achèveront officiellement le projet et lanceront une nouvelle action régionale sur la cybercriminalité et les preuves électroniques dans la région par le biais

	du nouveau projet CyberEast+. L'atelier discutera également, en vue de son adoption, d'une nouvelle déclaration sur les priorités stratégiques pour la région du partenariat oriental avec les principaux partenaires du projet, qui servira d'inspiration pour les politiques et le renforcement des capacités dans les pays de la région. Modérateur/s: Giorgi Jokhadze / équipe CyberEast Rapporteur : Équipe CyberEast Secrétariat : Giorgi Jokhadze / équipe CyberEast ► **Séance d'ouverture [20 min]** – Représentant de la Commission européenne – Représentant du Conseil de l'Europe – Présentation des équipes de pays chargées des projets – Introduction : ordre du jour de la réunion (Cybercrime Programme Office) ► **Clôture du projet CyberEast [70 min]** – Priorités et réalisations du pays en termes de législation et de politiques (représentant du pays du projet) – Renforcement des capacités : besoins et impact (représentant du projet dans le pays) – Coopération : mettre les normes en pratique (représentant de pays) Pause café [30 min] ► **Discussion sur le projet CyberEast+ [90 min]** – Nouvelles priorités et directions d'action (Commission européenne) – Équipes nationales (Bureau du programme sur la cybercriminalité) – Plan d'activités (Bureau du programme sur la cybercriminalité) Pause déjeuner [90 min] ► **Réunion des décideurs politiques sur les politiques de lutte contre la cybercriminalité dans la région du partenariat oriental [120 min] (en anglais)** – Présentation et analyse comparative de l'ancienne déclaration (2013) (expert invité) – Déclaration des priorités stratégiques pour le partenariat oriental 2023 (Secrétariat) – Intervention et évaluation de la Commission européenne – Interventions et évaluations dans chacun des pays du partenariat oriental – Synthèse et adoption de la déclaration des priorités stratégiques pour 2023
9h30-16h30	**Événement de projet : De iPROCEEDS-2 à CyberSEE** Langues : EN Objet : Cette conférence de clôture du projet iPROCEEDS-2 évaluera les principaux objectifs du projet, notamment la législation et les approches

	stratégiques, les mécanismes de signalement, le renforcement des capacités en matière de cybercriminalité, la formation des magistrats et la promotion de la collaboration entre les secteurs public et privé, ainsi que la coopération internationale. L'accent sera mis sur la présentation par les partenaires nationaux de l'impact du projet sur l'amélioration des compétences de leurs agences en matière de lutte contre la cybercriminalité et de preuves électroniques. Cet événement marquera l'évaluation formelle et la clôture du projet. Il préparera également le terrain pour une nouvelle action régionale ciblant la cybercriminalité et les preuves électroniques en Europe du Sud-Est et en Turquie : la nouvelle initiative "CyberSEE" sera entreprise conjointement par la Commission européenne et le Conseil de l'Europe de 2024 à 2027. Modérateur : Daniel Cuciurianu / équipe iPROCEEDS-2 Rapporteur : Daniel Cuciurianu / équipe iPROCEEDS-2 Secrétariat : Daniel Cuciurianu / équipe iPROCEEDS-2 ► **Séance d'ouverture [20 min]** – Représentant de la Commission européenne – Représentant du Conseil de l'Europe – Présentation de l'objectif et de l'ordre du jour de la réunion – Présentation des équipes nationales du projet ► **Événement de clôture du projet iPROCEEDS-2 [70 min]** – Réalisations des pays/régions en termes de législation, de politiques et de stratégies – Capacités des pays/régions en matière d'enquêtes sur la cybercriminalité, de recherche, de saisie et de confiscation des produits du crime en ligne et de sécurisation des preuves électroniques – Résultats de la formation judiciaire : l'objectif le plus important du projet – Progrès réalisés en matière de coopération publique-privée et internationale
Pause café 11h00-11h30	Pause café [30 min]
Pause déjeuner 13h00-14h30	► **Vers le projet CyberSEE : réunion régionale [90 min]** – Priorités stratégiques et nouvelles directions d'action (Commission européenne) – Plan d'activités (Bureau du programme sur la cybercriminalité) – Besoins actuels, priorités nationales et régionales (équipes nationales) Pause déjeuner [90 min] ► **L'essentiel du nouveau projet [120 min]** – Formation durable à la cybercriminalité et aux preuves électroniques dans les académies de justice, les académies de police et d'autres établissements de formation – Une attention accrue aux menaces d'attaques par ransomware et à l'OCSEA

	– Coopération entre les institutions chargées de la cybercriminalité et de la cybersécurité – Complémentarité des activités nationales et régionales
9h30-18h00 **Bilan des réalisations de GLACY** *9h00 - 13h00* Pause café *11h00-11h30* **Perspectives d'avenir : Les perspectives de GLACY-e** 14h30 - 18h00 Pause café *16h00-16h30*	**Événement du projet : De GLACY+ à GLACY-e** Langues : EN/FR/ES/PT (passif) Objectif : Cette session constitue l'événement de clôture du projet GLACY+. Elle sera l'occasion d'examiner l'impact du projet GLACY+ et de partager les enseignements tirés. S'appuyant sur les résultats positifs de GLACY+, le projet "Action Globale Renforcée sur la cybercriminalité" (GLACY-e), un nouveau projet conjoint de l'UE et des pays d'Europe centrale et orientale, s'inscrit dans la continuité, la consolidation et l'expansion du projet. GLACY-e étendra l'expérience du projet GLACY+ en soutenant de nouveaux pays sélectionnés en Afrique, en Asie-Pacifique et en Amérique latine. Il renforcera le rôle de premier plan des huit pays pivots dans le programme de renforcement des capacités dans leurs régions respectives. Modérateur : Catalina Stroe, Directrice des projets GLACY+/-e Secrétariat : Projet GLACY ► **Séance d'ouverture** *[30 min]* – Union européenne – INTERPOL – Conseil de l'Europe ► **Aperçu et impact de GLACY+** *[30 min]* – Catalina Stroe, Conseil de l'Europe et Dong Uk Kim, INTERPOL – présentation introductive ► **Enseignements tirés de GLACY+** *[150 min]* – Coordinateurs nationaux, réalisations nationales, impact au niveau national et améliorations potentielles *[5 minutes chacun].* ► **Quelles sont les prochaines étapes ?** *[30 min]* – Présentation du projet GLACY-e, Catalina Stroe ► **Présentation des pays sélectionnés** *[60 min]* – Représentants des pays, présentation des pays sélectionnés *[7 min chacun]* ► **Plan de travail GLACY-e pour le 1er trimestre 2024** *[30 min]* – Catalina Stroe et Dong Uk Kim, Présentation du plan de travail et débats ouverts ► **Durabilité par conception et par défaut - priorités stratégiques pour les pays pivots** *[45 min]*

	– Introduction des priorités et agendas régionaux par les pays pivots ► **Remarques finales** *[10 min]* – Union européenne – INTERPOL – Conseil de l'Europe
14h30-18h00 Pause café *15h30-16h00*	**Événement du projet : De CyberSouth à CyberSouth+** Langues : EN/FR/ES Objectif : L'objectif de la conférence finale est d'examiner et de valider conjointement les progrès réalisés dans la lutte contre la cybercriminalité dans la région MENA au cours de la période 2018 - 2023 ; d'évaluer l'impact du projet CyberSouth dans cinq domaines principaux liés aux résultats du projet (législation, travail de la police, travail de la justice, coopération internationale, stratégies nationales) et d'évaluer ensemble ce qui a bien fonctionné (meilleures pratiques) et ce qui peut être amélioré au cours de la prochaine phase. Modérateur : Denise Mazzolani, Responsable de programme, Conseil de l'Europe Secrétariat : L'équipe CyberSouth ► **Séance d'ouverture (10 min)** – Denise Mazzolani, responsable du programme CyberSouth, Conseil de l'Europe ► **Évaluation de CyberSouth : évaluation des cinq résultats du projet (50 min)** – Résumé du rapport d'évaluation final – Contributions des pays prioritaires – Discussion ► **Meilleures pratiques et examen des modalités de mise en œuvre des projets (60 min)** – Présentation de l'équipe du projet CyberSouth – Contributions des pays prioritaires – Discussion ► **Priorités de la région MENA dans la coopération sur la cybercriminalité 2024-2026 (50 min)** – Présentation des pays prioritaires – Politique européenne de voisinage : priorités pour la région MENA – Introduction au projet CyberSouth+ : principales composantes et phase de démarrage ► **Remarques finales (10 min)**
16h00-18h00	**Discussions éclair** *(diffusion en direct)*

Langues : EN/FR/ES/RO

Objectif : Pour la troisième fois, le Conseil de l'Europe proposera des sessions de discussions éclair, au cours desquelles les orateurs présenteront brièvement des idées innovantes dans le domaine de la cybercriminalité. Une discussion éclair est une présentation très courte qui ne dure que quelques minutes. Plusieurs discussions éclair seront généralement présentés par différents orateurs au cours d'une même session.

Nous vous invitons à soumettre votre proposition d'idée innovante majeure que vous souhaitez partager avec plus de 500 participants du monde entier, qui se réuniront lors de la conférence Octopus à Bucarest. 10 propositions seront sélectionnées en fonction de la diversité des sujets et des présentateurs.

Modérateur : Jacqueline Fick, CEO, VizStrat Solutions

Secrétariat : Équipe du projet Octopus

► **Introduction et objectif de la session**

► **Discussions éclair**

- Abdullah Al Noman, avocat, Cour suprême du Bangladesh
- Adriana Freitas, directrice responsable des projets de recherche, APWG.EU, Espagne
- Antonio Piña Alonso, Magistrat, Conseil général du pouvoir judiciaire, Espagne
- Cherie Adhiambo Oyier, Chargée de programme - Droits numériques des femmes, Réseau d'action TIC du Kenya (KICTANet) et Association for Progressive Communications (APC), Kenya
- Contanza Mateuzzi, avocate experte en cyberdroit, cybercriminalité et protection des données, Women4Cyber, Italie
- Daniela Rodriguez, Responsable des technologies de l'information, Ministère de la Justice, Luxembourg
- Ekaterina Dorodnych, spécialiste de l'évaluation, ONU Femmes, Italie
- Ilvana Dedja, chercheuse, Sense Cyber Research Center, Albanie
- Ioana Lekea, professeur adjoint, Académie hellénique de l'armée de l'air - Département des sciences aéronautiques - Laboratoire des jeux de guerre, Grèce
- Matteo Lucchetti, directeur, CYBER 4.0, Italie
- Pavlos Topalnakos, avocat à la Cour suprême, Laboratoire des jeux de guerre de l'Académie de l'armée de l'air hellénique, Grèce
- Roberto Contreras (en ligne), avocat, ministère public du Chili / université du Chili
- Ryan Lim Yi Hern, procureur général adjoint, chambre du procureur général, Singapour
- Tuomas Tammilehto, spécialiste en R&D, Université des sciences appliquées de Laurea, Finlande
- Yi Hon, directeur principal, chambre des procureurs généraux, Singapour
- Yuko Yokoyama, directeur de programme, ICANN

► **Conclusions**

VENDREDI 15 DECEMBRE	
9h30-11h00	**Atelier 7 - Atelier régional pour l'Asie : La protection des données en tant que facteur facilitant les enquêtes et les jugements en matière de cybercriminalité et d'affaires impliquant des preuves électroniques** Langues : EN Objet : Avec la dépendance croissante à l'égard des technologies de l'information et la croissance exponentielle de la quantité de données créées et échangées chaque jour par les utilisateurs et les organisations, le droit à la protection des données à caractère personnel est confronté à des défis majeurs. Cela vaut également pour les autorités de justice pénale qui doivent concilier des mesures efficaces pour obtenir, traiter et partager les données à caractère personnel nécessaires aux enquêtes et procédures pénales avec les exigences en matière de protection des données. Lorsque ces exigences sont respectées, elles facilitent le partage des données à caractère personnel, y compris au-delà des frontières et avec des fournisseurs de services et d'autres entités du secteur privé. C'est la raison pour laquelle l'article 14 sur la protection des données à caractère personnel a été inclus dans le deuxième protocole à la Convention de Budapest. L'objectif de cet atelier est de partager l'expérience - et de discuter des défis - des pays d'Asie en matière de mise en place de cadres de protection des données afin de permettre une réponse plus efficace de la justice pénale à la cybercriminalité. Modérateur : Peter Kimpian, Directeur de programme, Unité de protection des données du Conseil de l'Europe Rapporteur : Keongmin Yoon, conseiller, Banque mondiale Secrétariat : projet GLACY ► **Introduction et objectif de l'atelier [5 min]** – Peter Kimpian, Directeur de programme, Unité de protection des données du Conseil de l'Europe ► **Les garanties en matière de protection des données dans le deuxième protocole additionnel - pourquoi en avions-nous besoin ? [10 min]** – Ethel Mercado-Gutay, juge exécutif, tribunal régional de première instance de Makati, Cour suprême des Philippines ► **La protection des données, pierre angulaire de la coopération policière internationale [10 min]** – Marko Juric, Professeur associé, Département de droit, Université de Zagreb, Croatie – Caroline Goemans-Dorny, Déléguée à la protection des données, INTERPOL ► **Protection des données - témoignages de pays [10 min]** – Dilan Ratnayake, solliciteur général adjoint principal, ministère du Procureur général, Sri Lanka

	► **L'obligation de l'Etat de protéger contre les crimes et le droit à la vie privée : comment trouver le bon équilibre ? [50 min]** – Discussion animée par Jayantha Fernando, directeur de l'Autorité de protection des données et directeur du conseil d'administration du CERT du Sri Lanka. ► **Conclusions [5 min] du rapporteur**

9h30-11h00	**Atelier 8 - Atelier régional pour le Pacifique : Les défis de la mise en œuvre des lois sur la cybercriminalité dans les petites juridictions du Pacifique** Langues : EN Objectif : Des cadres juridiques solides en matière de cybercriminalité et de preuves électroniques sont la pierre angulaire d'enquêtes et de procédures pénales fructueuses. Les normes internationales, telles que la Convention de Budapest, fournissent un cadre pour des définitions et des incriminations cohérentes, des pouvoirs procéduraux normalisés et des mécanismes de coopération internationale. L'absence de transposition de ces mesures dans les législations nationales compromet la capacité d'un pays à enquêter, poursuivre et juger les affaires impliquant des preuves électroniques et à s'engager dans les efforts mondiaux visant à répondre efficacement aux nouveaux défis posés par la cybercriminalité. Les petites juridictions, telles que les États insulaires du Pacifique, peuvent rencontrer des difficultés supplémentaires pour adopter et adapter des lois appropriées, compte tenu de leurs contextes juridiques, administratifs et techniques spécifiques. L'atelier vise à recenser ces difficultés et les solutions possibles sur la base des pratiques réussies dans la région. Modérateur : Linda Folaumoetu'i, procureur général de Tonga et présidente du groupe de travail PILON sur la cybercriminalité Rapporteur: Jamie Crawford, Senior Crown Counsel, Crown Law Office of the Cook Islands, en représentation de PILON Secrétariat : projet GLACY ► **Introduction et objectif de l'atelier [10 min]** – Linda Folaumoetu'i, procureur général des Tonga et présidente du groupe de travail PILON sur la cybercriminalité

	► **Qu'est-ce qui fait un cadre juridique efficace en matière de cybercriminalité, adapté aux besoins des Etats insulaires du Pacifique, et quels sont les défis qu'ils rencontrent lorsqu'ils travaillent sur leur réforme législative ? [35 min]** – Glenys Andrews, directrice juridique et responsable de la rédaction, Bureau du procureur général, Fidji – Andrew Ega Kelesi, Directeur des poursuites publiques, Bureau du Directeur des poursuites publiques, Îles Salomon – Discussions modérées par Noumea Loretta Afamasaga-Teueli, Chef de la rédaction législative, Département de la justice et du contrôle des frontières, Nauru ► **Perspectives du Pacifique sur la mise en œuvre : quels sont les ingrédients clés d'une mise en œuvre efficace ? [40 min]** – Domingo Kabunare, Bureau de la transformation numérique, ministère de l'information, des communications et des transports, Kiribati – John Graham Jack, CIO Office of Government, Prime Minister's Office Vanuatu – Discussions modérées par Matthew Blackwood, ICHIP, Département américain de la Justice ► **Conclusions du rapporteur** – Jamie Crawford, Senior Crown Counsel, Crown Law Office of Cook Islands, en représentation de PILON
9h30-11h00	**Atelier 9 - Atelier régional pour l'Afrique : La Convention sur la cybercriminalité et le deuxième protocole - la clé de la coopération internationale en matière de preuves électroniques** Langues : EN/FR/ES/PT (passif) Objet : Alors que les preuves électroniques revêtent une importance croissante dans les enquêtes et procédures pénales, y compris en Afrique, les procédures d'obtention de ces preuves auprès d'autres juridictions sont souvent longues et peu efficaces. Le deuxième protocole à la convention de Budapest (ouvert à la signature en 2022) fournit des outils pour améliorer la coopération et la divulgation des preuves électroniques - comme la coopération directe avec les fournisseurs de services et les bureaux d'enregistrement, des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic, une coopération immédiate en cas d'urgence ou d'enquêtes conjointes, tout en assurant un système solide de garanties en matière de droits de l'homme et d'État de droit, en particulier lorsqu'il s'agit de protéger les données à caractère personnel. Près d'un quart des pays africains sont parties à la Convention de Budapest ou ont été invités à y adhérer. L'utilisation des outils du deuxième protocole est donc une option pour l'Afrique. Le Cap Vert, le Ghana, l'île Maurice et le Maroc figurent parmi les signataires à ce jour. L'atelier vise à démontrer la pertinence et l'opportunité des outils de coopération prévus par le protocole, ainsi qu'à discuter des défis éventuels liés à leur mise en œuvre dans la région africaine. Modérateurs : Rabiyatou Bah, gestionnaire de programme, projet OCWAR-C

	Hein Dries, expert en cybercriminalité, projet OCWAR-C Rapporteur : Abdul-Hakeem Ajijola, président du groupe d'experts en cybersécurité de l'Union africaine Secrétariat : projet GLACY ► **Introduction et objectif de l'atelier - pourquoi les pays africains devraient-ils prendre en compte la Convention sur la cybercriminalité et ses protocoles ? [15 min]** – Erica O'Neil, Cheffe adjointe, Section de la criminalité informatique et de la propriété intellectuelle, Département de la justice des États-Unis – Albert Antwi-Boasiako, Directeur général de l'Autorité de la cybersécurité, Ghana – Alassane Ndiaye, Magistrat, Directeur adjoint de la Direction des affaires criminelles et des grâces, Sénégal ► **Des outils renforcés pour la coopération internationale - quels sont les changements apportés par le deuxième protocole additionnel ? [25 min]** – Daniel Monteiro, Procureur Général, Ministère de la Justice, Cabo Verde [5 min] – Rajeshsharma Ramloll, Solliciteur général, Bureau du Procureur général, Maurice [5 min] – Discussions modérées [15 min] ► **Mettre la théorie en pratique : pistes pour une coopération internationale plus efficace - bonnes histoires et défis dans la région [45 min]** – Jamila Akaaga Ade, Directrice adjointe, Cheffe de l'unité de lutte contre la cybercriminalité, Département des poursuites publiques, ministère fédéral de la justice, Nigeria – Jacqueline De Lange, Chef de section : Criminalité commerciale, financière et cybercriminalité, B.C.N. INTERPOL de Pretoria, Afrique du Sud – Discussions modérées ► **Conclusions [5 min]**
9h30-11h00	**Atelier 10 - Atelier régional pour l'Amérique latine et les Caraïbes : coopération inter-agences en matière de criminalistique numérique** Langues : EN/ES/RO Objectif : Ces dernières années, de nombreux pays d'Amérique latine et des Caraïbes se sont efforcés de mettre en place des unités spécialisées dans la cybercriminalité au niveau de la police et du ministère public, ainsi que des unités chargées de la criminalistique numérique. Toutefois, la structure organisationnelle et les fonctions de ces unités ne cessent d'évoluer et ne sont pas toujours fondées sur les bonnes pratiques internationales. En outre, la coopération entre les unités spécialisées dans la cybercriminalité et d'autres services pour garantir la recevabilité des preuves électroniques devant les tribunaux reste un défi. L'atelier vise à identifier les bonnes pratiques en matière de création d'unités de criminalistique au sein de la police ou du ministère public, les moyens d'assurer la coopération interinstitutionnelle et

	d'éviter les conflits de compétences dans le domaine de la criminalistique numérique. Modérateur : Fabio Bruno, Directeur adjoint, pro tempore, Innovation Appliquée, INTERPOL Rapporteur : Michael Stawasz, chef adjoint de la lutte contre la criminalité informatique, Département de la justice des Etats Unis (US DoJ) Secrétariat : équipe GLACY+, INTERPOL ► **Introduction et objectif de l'atelier [10 min]** – Fabio Bruno, Directeur adjoint, pro tempore, Innovation Appliquée, INTERPOL ► **Unités de criminalistique numérique : quelles sont les pratiques d'enquête et les capacités organisationnelles actuelles et quelles sont leurs limites ? [35 min]** – Luciano Kuppens, Conseil national fédéral de la justice, Brésil – Mauricio Fernandez Montalban, Directeur de l'Unité de lutte contre la cybercriminalité, Ministère public, Chili – Armando Jose Diaz, Chef du département de cybersécurité et membre de l'Unité de point de contact 24/7, République dominicaine – Débats ouverts ► **Pistes de coopération inter-agences en matière de criminalistique numérique [40 min]** – Discussions modérées par Fabio Bruno, Directeur adjoint, pro tempore, Innovation Appliquée, INTERPOL ► **Conclusions [5 min]**
11h30-13h00	**Atelier 11 - Le renforcement des capacités pour changer la donne : qu'est-ce qui fait la différence ?** (*diffusion en direct*) Langues : EN/FR/ES/RO Objectif : L'objectif de l'atelier est d'identifier conjointement des exemples d'efforts de renforcement des capacités qui ont fait la différence en termes d'introduction de changements durables dans les systèmes de justice pénale et d'amélioration de l'efficacité dans la lutte contre la cybercriminalité. Au cours de la dernière décennie, les gouvernements, les organisations internationales, le secteur privé et les organisations de la société civile ont mis en œuvre de nombreux projets pour lutter contre la cybercriminalité aux niveaux national, régional et international. Certaines actions ont été plus fructueuses que d'autres. Il est important de capitaliser sur les expériences qui ont eu un impact et qui ont aidé les autorités de justice pénale et les sociétés à lutter plus efficacement contre la cybercriminalité.

	Modérateur : Jayanta Fernando, Data Protection Authority & Board Director, Sri Lanka Rapporteur : Daniela Andrović, Autorité de régulation des communications électroniques et des postes, Serbie Secrétariat : L'équipe CyberSouth ► **Introduction et objectif de l'atelier [5 min]** ► **Débat d'experts : ce qui a bien fonctionné et ce qui a moins bien fonctionné** Des exemples d'efforts nationaux et internationaux de renforcement des capacités qui ont abouti à des changements systématiques, ainsi que des actions qui n'ont pas produit les résultats escomptés. Le modérateur posera des questions aux membres du panel et ouvrira la voie à des interventions sur les pratiques et les cas partagés : **L'expérience nationale (40 min)** – **Chili** (Mauricio Fernandez Montalban, Directeur de l'Unité de lutte contre la cybercriminalité, Ministère public) – **Ghana** (Albert Antwi-Boasiako, directeur général, Autorité de la cybersécurité) – **Corée du Sud** (Sunhwa LEE, procureur et Seonhyeon KIM, enquêteur) – **Maroc** (Ahmed Tahiri Alaoui, chef de l'unité de lutte contre la cybercriminalité, ministère public) – **Sri-Lanka** (Wasantha Perera, Secrétaire, Ministère de la Justice) **L'expérience internationale (40 min)** – **GFCE** (Wouter Veenstra, responsable de la sensibilisation et des partenariats au niveau mondial) – **INTERPOL** (Dong Uk Kim, Officier spécialisé en cybercriminalité) – **ICHIP** (Anand Ramaswamy, International Computer Hacking and Intellectual Property, Addis-Abeba, USDOJ) – **OAS** (Michael Stawasz, USDOJ) – **OSCE** (Martha Stickings, chef adjoint et conseillère en matière de cybercriminalité, Unité des questions stratégiques de police) – **ONUDC** (Mustafa Erten, Centre régional pour la cybercriminalité) – **Banque mondiale** (Keongmin Yoon, conseiller) – **Conseil de l'Europe** (Denise Mazzolani, Cheffe de projet CyberSouth) ► **Q&R** ► **Conclusions (10 minutes)**
11h30-13h00	**Atelier 12 - Xénophobie et racisme en ligne contre liberté d'expression** Langues : EN/FR/ES/RO Objet : Face à la montée du discours de haine en ligne, notamment du racisme et de la xénophobie, les sociétés s'efforcent de trouver une réponse

	efficace qui respecte également le droit fondamental à la liberté d'expression. Un large éventail de mesures peut être pris pour lutter contre le discours de haine en ligne (voir la recommandation du Conseil de l'Europe sur le discours de haine adoptée en 2022). Dans cet éventail de mesures, le droit pénal est un dernier recours important. En 2003, le premier Protocole à la Convention sur la cybercriminalité a été ouvert à la signature, portant sur "l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques" (STE n° 189). A l'occasion du vingtième anniversaire de ce protocole, une étude des bonnes pratiques a été entreprise sur l'expérience de ce traité. L'atelier vise à présenter les résultats de cette étude, à fournir des orientations supplémentaires et à discuter des défis à relever pour lutter contre la xénophobie et le racisme en ligne tout en respectant le droit à la liberté d'expression. Modérateur : Jamila Akaaga Ade, directeur adjoint, chef de l'unité de lutte contre la cybercriminalité, département des poursuites publiques, ministère fédéral de la justice, Nigeria Rapporteur : Marko Juric, Professeur associé, Département de droit, Université de Zagreb, Croatie Secrétariat : Octopus + Secrétariat T-CY ► **Introduction et objectif de l'atelier** – Jamila Akaaga Ade ► **Résultats de l'étude sur les bonnes pratiques** – Jan Kralik, Division de la cybercriminalité, Conseil de l'Europe ► **Défis à relever pour lutter contre la xénophobie et le racisme en ligne** – Fernanda Teixeira Souza, procureur fédéral itinérant à Brasilia, coordinatrice du groupe consultatif sur la cybercriminalité au sein du service fédéral des poursuites, Brésil – Antonio Piña Alonso, Magistrat, Conseil général du pouvoir judiciaire, Espagne ► **Déterminer les limites entre le discours d'incitation à la haine et la liberté d'expression** – Steven Gatembu Kairu, Juge d'appel, Cour d'appel, Pouvoir judiciaire, Kenya – Esther Agelan, Membre du Conseil d'administration, Association internationale des femmes juges ► **Conclusions**
11h30-13h00	**Atelier 13 - Renforcer les points de contact 24/7** Langues : EN/FR/ES Objectif : L'atelier a pour but d'explorer plus avant les modalités de renforcement du fonctionnement du Réseau 24/7 de points de contact dans le cadre

	de la Convention de Budapest : partager les bonnes pratiques pour un traitement efficace des demandes reçues ; identifier d'autres moyens d'accroître l'opérabilité du Réseau ; comprendre les rôles et les responsabilités du Réseau en ce qui concerne les nouveaux outils du Deuxième Protocole à la Convention de Budapest. Modérateur : Virgil Spiridon, chef adjoint de la police nationale Roumaine Rapporteur : Catalin Zetu, chef de l'unité de lutte contre la cybercriminalité de la police nationale roumaine Secrétariat : Daniel Cuciurianu / équipe iPROCEEDS-2 ► **Introduction et objectif de l'atelier [5 min]** – Remarques du modérateur – Secrétariat ► **Exemples de coopération internationale facilitée par le réseau [35 min]** – Erica O'Neil, Cheffe adjointe, Section de la criminalité informatique et de la propriété intellectuelle, Département de la justice des États-Unis – Nenad Bogunović, Service de lutte contre la cybercriminalité, Serbie ► **Mise en œuvre au niveau national des nouvelles responsabilités des points de contact 24/7 [25 min]** – Antonio Segovia Arancibia, Professeur de droit pénal transnational, Université UAI, Chili ► **Promouvoir le réseau au niveau national et international [15 min]** – Daniela Matei, Unité de lutte contre la cybercriminalité de la police nationale roumaine, 24/7 PoC – Theophilus Botchway, Autorité de la cybersécurité, 24/7 PoC du Ghana ► **Conclusions du rapporteur [10 min]**
11h30-13h00	**Atelier 14 - Interaction entre cybersécurité et cybercriminalité** Langues : EN/FR/ES/RO Objectif : Cet atelier explore les liens entre la cybersécurité et la prévention et le contrôle de la cybercriminalité. Il examinera en particulier la coopération entre les autorités de justice pénale et les équipes d'intervention en cas d'incident de sécurité informatique (Computer Security Incident Response Teams - CSIRT). L'objectif de cette session est d'identifier les moyens d'améliorer la coopération entre les autorités de justice pénale et les acteurs de la cybersécurité, notamment par une action conjointe contre les menaces communes, la protection des infrastructures critiques et le renforcement des capacités. Modérateur : Matteo Lucchetti, Directeur, Cyber 4.0, Italie Rapporteur : Cecilia Popa, EU CyberNet

	Secrétariat: Giorgi Jokhadze / Andrei Enachi ► **Introduction et objectif de l'atelier [5 min]** – Remarques du modérateur – Secrétariat ► **Risques et menaces communs : comprendre le paysage de la coopération [15 min]** – Le point de vue du secteur privé (Aisling Kelly, Microsoft) – Discussion ► **Protection des infrastructures critiques : une responsabilité commune [30 min]** – Ukraine (Anatasiia Ponarina, Service de sécurité de l'État) – Afrique du Sud : réformes en cours (Jacqueline Fick) – Discussion ► **Renforcement des capacités pour améliorer la sécurité et la résilience [20 min]** – César Moliné Rodríguez, Directeur regional, EU CyberNet – Centre de compétence en cybernétique pour l'Amérique latine et les Caraïbes (LAC4) ► **Options pour améliorer la coopération entre les services répressifs et les CSIRT [15 min]** – Discussion : exemples opérationnels et suggestions des pays et organisations participants ► **Conclusions [5 min]**
14h30-17h00	**Plénière de clôture et conclusions** *(diffusion en direct)* Langues : EN/FR/ES ► **Principaux enseignements des ateliers [14h45-15h15]** – Résumé de chaque atelier ► **Leçons tirées de 10 ans de programme de lutte contre la cybercriminalité du Bureau du Conseil de l'Europe (C-PROC) [15h15-16h15]** – Modérateur : Virgil Spiridon, Chef adjoint de la Police nationale roumaine ► **Discours d'ouverture :** – Traian Hristea, secrétaire d'État, ministère des affaires étrangères, Roumanie – Bjørn Berge, Secrétaire général adjoint, Conseil de l'Europe

	– Sabin Pop, S.E. Ambassadeur, Représentant permanent de la Roumanie auprès du Conseil de l'Europe (1995-2001) – Gheorghe Magheru, S.E. Ambassadeur, Représentant permanent de la Roumanie auprès du Conseil de l'Europe (2001-2006) – Stelian Stoian, S.E. Ambassadeur, Représentant permanent de la Roumanie auprès du Conseil de l'Europe (2006-2013) ► **Événement de la Convention** ► **Panel de gestionnaires de projets C-PROC sur l'impact du C-PROC à ce jour, la voie à suivre et les résultats des événements parallèles :** – Catalina Stroe, Cheffe de projet GLACY – Giorgi Jokhadze, Chef de projet CyberEast – Nina Lichtner, Cheffe de projet Octopus – Dan Cuciurianu, Chef de projet iPROCEEDS-2 – Denise Mazzolani, Cheffe de projet CyberSouth ► **Perspectives 2024 et conclusions [16h15-17h00]** – Panel de clôture – Messages clés de la conférence Octopus