



COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

## **Documents d'information**

**SG/Inf(2019)38**

Strasbourg, 19 novembre 2019

---

**Bureau de programme du Conseil de l'Europe sur la  
cybercriminalité à Bucarest**

**Rapport d'activité du C-PROC pour la période octobre  
2018 - septembre 2019**

---

## Table des matières

1.	Cadre et objet du présent rapport .....	3
2.	Cybercriminalité - l'approche du Conseil de l'Europe .....	4
3.	Résumé des projets et des résultats pour la période d'octobre 2018 à septembre 2019 .....	5
3.1	Aperçu des projets en cours.....	6
3.2	Cybercrime@Octopus .....	7
3.3	Cybercrime@EAP 2018 – Collaboration Internationale et publique/ privée .....	8
3.4	Projet CyberEast sur la lutte contre la Cybercriminalité pour la Cyber-Résilience dans la région du Partenariat oriental.....	9
3.5	Projet iPROCEEDS ciblant les produits du crime sur Internet en Europe du Sud-Est.....	10
3.6	Projet CyberSud sur la cybercriminalité et les preuves électroniques dans la région du voisinage sud.....	12
3.7	Élargissement du projet GLACY+ sur l'action mondiale contre la cybercriminalité 13	
3.8	EndOCSEA@Europe pour mettre fin à l'exploitation et aux abus sexuels des enfants en ligne en Europe .....	16
4.	Impact.....	18
5.	Conclusions et priorités .....	21
6.	Annexe : Inventaire des activités soutenues par le C-PROC (Octobre 2018 – Septembre 2019) .....	24

## 1. Cadre et objet du présent rapport

Le présent rapport a pour objet d'informer le Comité des Ministres des activités menées par le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) à Bucarest (Roumanie), pendant la période allant d'octobre 2018 à septembre 2019.<sup>1</sup>

En octobre 2013, le Comité des Ministres a décidé<sup>2</sup> de créer un Bureau de programme sur la cybercriminalité à Bucarest, en Roumanie, pour répondre à la nécessité de renforcer les capacités en matière de cybercriminalité et de preuves électroniques. Dans la même décision, il a demandé au/à la Secrétaire général(e) de faire rapport sur une base annuelle sur les activités de ce bureau, ainsi que sur son coût, y compris une proposition concernant la poursuite de son fonctionnement.

Cette décision faisait suite à une offre du Gouvernement roumain et à une proposition du Secrétaire Général au printemps 2013<sup>3</sup>. Le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) est devenu opérationnel en avril 2014.

L'objectif du Bureau est d'assurer la mise en œuvre des projets de renforcement des capacités du Conseil de l'Europe en matière de cybercriminalité dans toutes les régions du monde.<sup>4</sup> Cela inclut :

- L'identification des besoins en matière de renforcement des capacités dans le domaine de la cybercriminalité ;
- Des conseils, un soutien et une coordination dans la planification, la négociation et la mise en œuvre en temps utile d'activités ciblées du Conseil de l'Europe sur la cybercriminalité, y compris des programmes conjoints avec l'Union européenne et d'autres donateurs ;
- L'établissement de partenariats contre la cybercriminalité avec des organisations des secteurs public et privé ;
- La coopération avec les autorités roumaines en matière de cybercriminalité ;
- Des activités de collecte de fonds pour des projets et programmes spécifiques.

Les locaux du C-PROC sont situés dans la Maison de l'ONU à Bucarest. Les espaces de bureaux sont alloués gratuitement au Conseil de l'Europe par le Gouvernement de la Roumanie dans le cadre du Mémoire d'accord signé en octobre 2013.

<sup>1</sup> Pour le rapport couvrant la période d'avril 2014 à septembre 2015, voir <https://rm.coe.int/168047d1b8>

Pour la période d'octobre 2015 à septembre 2016, voir <https://rm.coe.int/16806b8a87>

Pour la période d'octobre 2016 à septembre 2017, voir [ce rapport](#).

Pour la période d'octobre 2017 à septembre 2018, voir [ce rapport](#).

<sup>2</sup> Le 9 octobre 2013, à leur 1180e séance.

<sup>3</sup> SG/Inf(2013)29

<sup>4</sup> Voir SG/Inf(2013)29 et MoU entre le Conseil de l'Europe et le Gouvernement de la Roumanie, signé le 15 octobre 2013.

Le Secrétariat du Comité de la Convention sur la cybercriminalité (T-CY) - et donc le volet intergouvernemental des travaux du Conseil de l'Europe sur la cybercriminalité - demeure à Strasbourg.

En septembre 2019, le C-PROC disposait de trente employés financés par les budgets des projets, à l'exception du chef du bureau qui est également le secrétaire exécutif du T-CY et partage son temps entre Strasbourg et Bucarest. Cet arrangement assure les liens étroits entre les activités du T-CY et du C-PROC.

Le 5<sup>ème</sup> anniversaire du C-PROC a été célébré à Bucarest du 25 au 27 février 2019, à l'occasion de la conférence internationale sur « [La justice pénale dans le cyberspace](#) », organisée conjointement par le Conseil de l'Europe et la Présidence Roumaine du Conseil de l'UE, et à laquelle la Secrétaire Générale adjointe a participé. Il a confirmé l'impact du Bureau en termes d'adhésion à la Convention de Budapest sur la Cybercriminalité et le niveau de mise en œuvre de celle-ci, le renforcement de la législation dans le monde entier sur la base de cet instrument, de programmes durables de formation des autorités judiciaires et répressives sur la cybercriminalité et les preuves électroniques, de renforcement de la coopération internationale, notamment par des points de contact 24/7, ainsi que de partenariats et synergies avec un grand nombre d'organisations.

## **2. Cybercriminalité - l'approche du Conseil de l'Europe**

La cybercriminalité - en tant que délit contre et au moyen de systèmes informatiques - est devenue une menace majeure pour les droits fondamentaux, la démocratie et l'État de droit, ainsi que pour la paix et la stabilité internationales et a un impact économique majeur. Parallèlement, la question de la preuve sur les systèmes informatiques (« preuve électronique ») a gagné en importance et en complexité.

Toute infraction - qu'il s'agisse de fraude, d'attaques contre les médias, les parlements, les systèmes électoraux ou les infrastructures publiques, de maltraitance des enfants ou d'autres formes d'exploitation sexuelle, de vol de données personnelles, de racisme et de xénophobie, de blanchiment d'argent ou de terrorisme - est susceptible d'impliquer la cybercriminalité ou des preuves électroniques.

Cette question est donc étroitement liée aux objectifs fondamentaux du Conseil de l'Europe, à savoir la promotion des droits de l'Homme, de la démocratie et de l'Etat de droit.

L'approche du Conseil de l'Europe face à ces défis consiste en un triangle « dynamique » composé de trois éléments interdépendants :

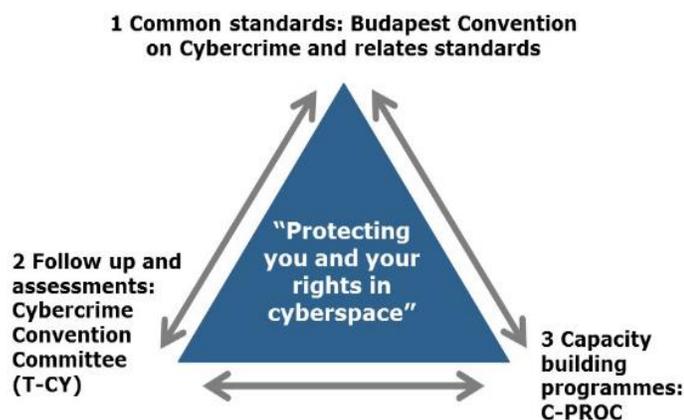
- La Convention de Budapest sur la cybercriminalité (STE 185), ouverte à la signature en 2001<sup>5</sup>, demeure l'accord international le plus pertinent en la matière. En septembre 2019, [64 États étaient Parties et huit autres](#) l'avaient signé ou avaient

---

<sup>5</sup> Complété par le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE 189) de 2003.

été invités à y adhérer. La Convention de Budapest est donc l'un des traités du Conseil de l'Europe les plus réussis en termes d'adhésion ;

- Le [Comité de la Convention sur la cybercriminalité](#) (T-CY) évalue la mise en œuvre de la Convention par les Parties, adopte des notes d'orientation et maintient des groupes de travail pour identifier les réponses aux nouveaux défis. Avec actuellement 73 États<sup>6</sup> membres et observateurs, ainsi que douze organisations observatrices, le T-CY est l'un des principaux organes intergouvernementaux sur la cybercriminalité au niveau international. Son objectif principal est actuellement la préparation d'un Protocole additionnel à la Convention sur la cybercriminalité sur le renforcement de la coopération internationale et l'accès aux preuves dans le nuage ;



- Le [renforcement des capacités en matière de cybercriminalité](#) est un élément essentiel de l'approche du Conseil de l'Europe depuis 2006. Les discussions qui ont eu lieu au niveau des Nations Unies au début de 2013<sup>7</sup> ont confirmé qu'un large accord international sur le renforcement des capacités était un moyen efficace d'aider les sociétés à relever le défi de la cybercriminalité et des preuves électroniques. Cet argument - qui a conduit à la création de C-PROC en 2013 - reste valable aujourd'hui. Cela a été confirmé dans un récent [rapport du Secrétaire général de l'ONU à la 74e session de l'Assemblée générale des Nations Unies](#).

### 3. Résumé des projets et des résultats pour la période d'octobre 2018 à septembre 2019

Depuis son établissement, le C-PROC a « pour principal objectif d'assurer la mise en œuvre des projets du Conseil de l'Europe relatifs au renforcement des capacités en matière de cybercriminalité »<sup>8</sup>. Il aide, au travers de projets, des pays du monde entier à renforcer leurs capacités de justice pénale en matière de cybercriminalité et de preuves électroniques sur la base de la Convention de Budapest sur la Cybercriminalité et des normes connexes<sup>9</sup>.

<sup>6</sup> 64 Parties, 8 signataires ou États invités à adhérer ainsi que la Fédération de Russie.

<sup>7</sup> Réunion du Groupe intergouvernemental d'experts des Nations Unies sur la cybercriminalité, Vienne, février 2013.

<sup>8</sup> SG/Inf(2013)29 et décision CM du 9 octobre 2013, à leur 1180e séance.

<sup>9</sup> Tels que le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE 189), la Convention pour la protection des personnes à l'égard du traitement automatisé des données personnelles (STE 108), Convention de Lanzarote relative à la protection des enfants contre l'exploitation et les abus sexuels (STCE 201), Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE 198) et autres.

### 3.1 Aperçu des projets en cours

Entre octobre 2018 et septembre 2019, le C-PROC a appuyé environ 240 activités<sup>10</sup> dans le cadre des projets énumérés ci-dessous.

En septembre 2019, le budget combiné des projets en cours s'élevait à 32,3 millions d'euros. Cela représente une augmentation supplémentaire par rapport aux années précédentes.<sup>11</sup>

Les projets [Cybercrime@Octopus](#) et [EndOCSEA@EUROPE](#) sont entièrement financés par des contributions volontaires. Les projets conjoints avec l'Union européenne bénéficient d'un cofinancement de 10% du budget du Conseil de l'Europe (environ 2,7 millions EUR).

#### Liste des projets (octobre 2018 - septembre 2019)

Titre du Projet	Durée du projet	Budget	Financement
<a href="#">Cybercrime@Octopus</a>	Janvier 2014 - décembre 2020	4 millions EUR	Contributions volontaires (Estonie, Hongrie, Monaco, Pays-Bas, Roumanie, République slovaque, Royaume-Uni, Japon, États-Unis, Japon, Monaco et Microsoft)
<a href="#">Cybercrime@EAP 2018</a> sur la coopération internationale et la coopération publique/ privée dans la région du Partenariat oriental	Janvier 2018 - Déc 2018	0,98 million EUR	EU/CoE JP (Partenariat pour la bonne gouvernance)
Élargissement du projet <a href="#">GLACY+</a> sur l'action mondiale contre la cybercriminalité	mars 2016 - février 2021	13,35 millions EUR	EU/CoE JP
Projet <a href="#">iPROCEEDS</a> ciblant les produits du crime sur Internet en Europe du Sud-Est et en Turquie	Janvier 2016 - Déc 2019	5,56 millions EUR	EU/CoE JP
Projet <a href="#">EndOCSEA@EUROPE</a> contre l'exploitation et les abus sexuels des enfants sur Internet	Juillet 2018 - Déc 2020	0,85 million EUR	Fonds pour mettre fin à la violence contre les enfants
<a href="#">CyberSud</a> sur le renforcement des capacités dans le voisinage sud	Juillet 2017 - Juin 2020	3,33 millions EUR	EU/CoE JP

<sup>10</sup> Voir la liste des activités en annexe.

<sup>11</sup> Septembre 2015 : 6 millions EUR, septembre 2016 : 22 millions EUR, septembre 2017 : 24,4 millions EUR, septembre 2018: 26,7 millions d'euros.

Projet <a href="#">CyberEast</a> sur la lutte contre la cybercriminalité pour la résilience de la cybercriminalité dans la région du Partenariat oriental	Juin 2019 - Juin 2022	4,22 millions EUR	EU/CoE JP
---	-----------------------	-------------------	-----------

### 3.2 [Cybercrime@Octopus](#)

Le Cybercrime@Octopus est un projet mondial financé par des contributions volontaires. Il est conçu pour aider de manière pragmatique tout pays ayant besoin d'un appui, en particulier en ce qui concerne l'élaboration de la législation.

Les activités entre Octobre 2018 et Septembre 2019 comprenaient, par exemple :

- Ghana - une série d'ateliers à l'intention de hauts magistrats et de membres du Parlement en octobre 2018. Cela a facilité l'adhésion du Ghana à la Convention de Budapest en décembre 2018.
- Niger - Mission consultative sur la législation en décembre 2018. Cela s'est traduit par l'adoption d'une législation interne conforme à la Convention de Budapest et la décision d'adhérer à ce traité en 2019.
- Mauritanie - [Examen du cadre juridique et analyse des besoins en renforcement des capacités](#) en décembre 2018.
- Kazakhstan - Atelier (décembre 2018) suivi d'un examen de la législation nationale sur la cybercriminalité et les preuves électroniques.
- Guatemala - [Mission consultative sur la législation en](#) janvier 2019. Un projet de loi conforme à la Convention de Budapest a été soumis au Congrès en août 2019 ainsi qu'une décision d'adhésion à ce traité.
- Géorgie - Appui à une stratégie intégrée sur la cybercriminalité et la cybersécurité en février 2019.
- Côte d'Ivoire - [Visite du T-CY pour examiner la législation interne relative à la Convention de Budapest](#) en mars 2019. Il en a résulté une décision politique de demander l'adhésion à la Convention de Budapest.
- Guinée (Conakry) - [Examen de la législation interne contre la Convention de Budapest](#) en avril 2019. Cela a confirmé la nécessité de réformer la législation nationale.
- Bénin - [Visite du T-CY pour examiner la législation interne relative à la Convention de Budapest](#) en avril 2019. Il en a résulté une demande d'adhésion au cours de la visite et une invitation ultérieure à adhérer à la Convention de Budapest.
- La Gambie - Atelier sur la législation relative à la protection des données conformément à la Convention 108 en mai 2019.
- Qatar - Examen de la législation nationale (Doha, juin 2019). Il en est résulté une série de propositions de réforme de la législation conformément à la Convention de Budapest.
- La Formation judiciaire et formation des forces de l'ordre, notamment au Nigéria (Décembre 2018, février 2019), au Chili (Novembre 2018) ou au Costa Rica (Février 2019).

Ces exemples illustrent l'impact que les projets de renforcement des capacités peuvent avoir en termes de législation, de garanties en matière d'État de droit et de compétences des autorités de justice pénale.

Les objectifs de Cybercrime@Octopus comprennent le soutien au Cybercrime Convention Committee (T-CY).

Un événement majeur à cet égard a été la conférence internationale sur « [La justice pénale dans le cyberspace](#) », organisée conjointement par le Conseil de l'Europe et la Présidence Roumaine du Conseil de l'UE à Bucarest du 25 au 27 février 2019, qui a abouti à une [série de messages clés](#) et a permis de mieux comprendre les travaux sur le 2<sup>ème</sup> Protocole additionnel à la Convention de Budapest.

En outre, le projet a cofinancé des réunions du T-CY et en particulier des groupes de rédaction du Protocole (novembre 2018, février 2019, mars 2019, mai 2019, juillet 2019 et septembre 2019). Ainsi, les travaux sur le 2<sup>ème</sup> protocole additionnel ont pu se poursuivre sans délai malgré les difficultés financières de l'Organisation au cours de cette période.

Jusqu'à présent, le projet a été financé par l'Estonie, la Hongrie, Monaco, les Pays-Bas, la Roumanie (en nature), la République slovaque, le Royaume-Uni, le Japon, les États-Unis et Microsoft, les États-Unis étant le principal contributeur.

Dans l'ensemble, Cybercrime@Octopus est un outil flexible pour répondre aux besoins, renforcer la législation, promouvoir les partenariats multipartites et soutenir le T-CY d'une manière pragmatique. Il reste une ressource à laquelle les donateurs peuvent contribuer à la lutte contre la cybercriminalité et soutenir le T-CY à tout moment, sans longs délais pour la conception et l'approbation des projets.

### **3.3 [Cybercrime@EAP 2018](#) – Collaboration Internationale et publique/privée**

Le Cybercrime@EaP 2018 était un projet d'une année qui s'appuyait sur des activités antérieures dans la région du Partenariat oriental. Il a pris fin en décembre 2018.

Entre octobre et décembre 2018, le Cybercrime@EaP 2018 s'est concentré sur le développement de compétences pratiques pour les enquêteurs, les autorités d'entraide juridique et les points de contact 24h/24 et 7j/7. Des cours techniques sur les enquêtes sur les réseaux et la criminalistique des données en direct, organisés au niveau régional en coopération avec le [Groupe européen de formation et d'éducation en matière de cybercriminalité](#) (ECTEG), ont été les temps forts du mois d'octobre.

Une série d'[exercices pratiques sur table portant sur la coopération internationale](#), la mise à l'essai d'outils pratiques (comme l'Octopus Cybercrime Community) et des modèles (« article 29-31 ») pour la coopération dans des situations réelles ont également été mis en concurrence durant cette période.

Les exercices régionaux de cybercriminalité organisés à l'occasion de la [Semaine de la Cybersécurité République de Moldova 2018](#) ont permis d'améliorer les compétences pratiques en matière de coopération entre les agents des services de détection et de répression travaillant sur la cybercriminalité et les membres des CSIRT/CERT travaillant sur la cybersécurité dans un certain nombre de domaines, tels que le traitement des incidents, l'analyse des logiciels malveillants et la protection des infrastructures critiques.

La [Conférence de clôture](#) du projet a adopté deux rapports régionaux sur les [menaces et les défis de la cybercriminalité dans le Partenariat oriental](#) et une étude actualisée sur les [stratégies de cybercriminalité et de cybersécurité dans la région](#).

L'écart de six mois entre la fin du projet Cybercrime@EAP 2018 et le nouveau projet CyberEast a été partiellement comblé par le projet Cybercrime@Octopus.

### **3.4 Projet CyberEast sur la lutte contre la Cybercriminalité pour la Cyber-Résilience dans la région du Partenariat oriental**

Le projet joint UE/Conseil de l'Europe CyberEast (« Action on Cybercrime for Cyber Resilience in the Eastern Partnership region ») a officiellement débuté le 20 juin 2019 et la [Conférence de lancement](#) a eu lieu à Bruxelles en septembre 2019.

Le projet couvre l'Arménie, l'Azerbaïdjan, la Biélorussie, la Géorgie, la République de Moldova et l'Ukraine. L'objectif est « d'accroître et de renforcer la cyber-résilience et les capacités des pays du Partenariat oriental en matière de justice pénale afin de mieux relever les défis posés par les cybermenaces et d'améliorer leur sécurité globale ».

Ce projet d'une durée de trois ans renforce les réalisations antérieures, telles que la mise en place de cadres législatifs mettant en œuvre la Convention de Budapest sur la Cybercriminalité, permettant une coopération régionale et internationale efficace et améliorant la coopération public/privé en matière de cybercriminalité et de preuves électroniques dans la région du Partenariat oriental.

Il vise également à renforcer les capacités opérationnelles des unités de lutte contre la cybercriminalité, à accroître la responsabilité, le contrôle et la visibilité publique des mesures de répression de la cybercriminalité, ainsi qu'à renforcer la coopération interinstitutionnelle sur la cybercriminalité et les preuves électroniques, en particulier en améliorant le partage des informations entre les équipes de réponse aux incidents de sécurité informatique (CSIRT) et les autorités compétentes.

Au cours de la phase initiale de CyberEast, une série de visites d'évaluation dans chaque pays du Partenariat oriental sur la structure institutionnelle, les capacités, les compétences et les besoins de formation des unités chargées de la cybercriminalité ainsi que la coopération interinstitutionnelle ont débuté en septembre 2019.

### 3.5 **Projet [iPROCEEDS](#) ciblant les produits du crime sur Internet en Europe du Sud-Est**

Le projet joint iPROCEEDS du Conseil de l'Europe et de l'Union européenne couvre l'Albanie, la Bosnie-Herzégovine, le Monténégro, la Serbie, la Macédoine du Nord, la Turquie et le Kosovo\*<sup>12</sup> et vise à renforcer la capacité à rechercher, saisir et confisquer les produits de la cybercriminalité et prévenir le blanchiment de capitaux sur Internet. Il dispose d'un budget de 5,56 millions d'euros et s'étend de janvier 2016 à décembre 2019. Les composants comprennent :

- Les systèmes de rapports publics ;
- La législation ;
- La coopération entre les unités chargées de la cybercriminalité, des enquêtes financières et du renseignement financier ;
- Les lignes directrices et indicateurs pour la détection de la fraude en ligne et du blanchiment d'argent sur Internet ;
- Le partage d'informations public/privé ;
- La formation judiciaire ;
- La coopération internationale.

L'iPROCEEDS fait ainsi suite aux recommandations d'une [étude typologique](#) conjointe MONEYVAL/Global Project sur la Cybercriminalité de 2012.

Entre octobre 2018 et septembre 2019, iPROCEEDS a renforcé davantage les compétences et capacités des enquêteurs en matière de cybercriminalité et de criminalité financière, des spécialistes de la criminalistique numérique, des procureurs et des représentants des cellules de renseignement financier (FIUS) en matière de recherche, de saisie et de confiscation des produits du crime en ligne. Le projet a financé des séances de formation et d'ateliers spécialisés, tels que le [Network Investigations](#), l'[Online Financial Fraud and Credit Card Fraud](#), l'[Online Undercover Investigations](#). En outre, pour donner aux agents des services de détection et de répression les moyens d'enquêter sur les infractions liées à la cybercriminalité, l'accès à [FREETOOL \(Free Forensic Tools for the Law Enforcement Community\)](#) a été facilité. Sur la base d'un accord entre le Conseil de l'Europe et le Collège Universitaire de Dublin (UCD), les outils ont été mis à la disposition des Parties à la Convention sur la Cybercriminalité pour permettre la diffusion et l'utilisation au sein de leurs organismes respectifs.

Le projet a soutenu la formation d'agents de services de détection et de répression, dans le cadre d'un [programme de Master à distance sur l'informatique légale et les enquêtes sur la cybercriminalité](#), proposé par le Collège Universitaire de Dublin (Irlande). Dix étudiants ont terminé le programme avec succès. Il a été fonctionné pendant 24 mois et couvert des modules comme l'informatique criminalistique, les techniques d'investigation financière (« suivre l'argent »), les enquêtes sur les réseaux, les enquêtes sur les appareils mobiles,

---

<sup>12</sup> \*Toutes les références au Kosovo, qu'il s'agisse du territoire, des institutions ou de la population, dans le présent texte s'entendent dans le plein respect de la résolution 1244 du Conseil de sécurité des Nations unies et sans préjudice du statut du Kosovo.

la criminalistique des données en temps réel, VoIP et les enquêtes sur les communications sans fil, et autres.

Le renforcement des capacités des autorités de justice pénale en matière de coopération interinstitutionnelle et internationale pour la perquisition, la saisie et la confiscation des produits du crime en ligne demeure le principal objectif du projet. Trois exercices de simulation sur la cybercriminalité et les enquêtes financières ont été organisés à [Tirana, Albanie](#) (4-7 mars 2019), [Belgrade, Serbie](#) (8-11 avril 2019) et [Ankara, Turquie](#) (6-9 mai 2019). Des enquêteurs en matière de cybercriminalité et de criminalité financière, des spécialistes de la criminalistique numérique, des procureurs et des analystes du blanchiment d'argent des FIUs ont mené des enquêtes sur le Darknet, les monnaies virtuelles et coopéré dans le cadre des équipes communes d'enquête (JITs). Les participants ont établi des liens plus étroits entre diverses communautés professionnelles dans un environnement en temps réel aux niveaux national et international pour l'enquête sur la cybercriminalité et ses gains financiers.

iPROCEEDS s'est employé à renforcer la coopération internationale entre les unités chargées de la cybercriminalité, ainsi qu'entre les autorités compétentes en matière de coopération judiciaire en [testant la coopération internationale dans le cadre d'un exercice sur table](#) et en acquérant une solide compréhension en matière d'[utilisation des canaux formels et informels de coopération dans les enquêtes sur la cybercriminalité](#). Il en est résulté une meilleure compréhension de la coopération judiciaire directe, la nécessité d'utiliser des modèles et des outils en ligne et une coordination accrue entre les processus de coopération judiciaire et de coopération entre services de police. Un résultat important de ces efforts a été la [traduction par les pays du projet des modèles standard](#) approuvés par le T-CY pour les demandes au titre des articles 29 (conservation des données) et 31 (accès aux données enregistrées) de la Convention de Budapest. Leur utilisation augmentera l'efficacité des points de contact 24/7 et des autorités d'entraide judiciaire dans leurs procédures correspondantes en vertu de ces dispositions.

L'iPROCEEDS a pris l'initiative d'organiser la [Conférence sur l'économie souterraine 2019](#), co-organisée en septembre 2019 par le Conseil de l'Europe dans ses locaux à Strasbourg (France). Cet événement international de premier plan sur la sécurité de l'information a rassemblé quelque 450 représentants d'organismes d'application de la loi, du milieu de la cybersécurité, du secteur privé et du milieu universitaire du monde entier. Il a été ouvert par la Secrétaire Générale adjointe.

En 2019, le Projet a continué d'appuyer des programmes de formation judiciaire sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne. Les cours nationaux d'introduction à la justice sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne ont eu lieu au [Kosovo\\*](#) (19-22 février 2019), au [Monténégro](#) (11-12 mars 2019 et 15-16 avril 2019), en [Bosnie-Herzégovine](#) (22-25 avril 2019), en Albanie (11-12 mars 2019 et 13-14 mai 2019 et 12-13 juin), en [Turquie](#) (14-17 mai 2019) et en Macédoine du Nord (17-18 et 28-29 octobre 2019). Quelque 150 juges, procureurs, juristes et candidats ont renforcé leurs compétences et leurs connaissances nécessaires pour s'acquitter de leurs rôles et fonctions respectifs dans les affaires de cybercriminalité, de preuves électroniques et de perquisition, de saisie et de confiscation

des produits du crime en ligne. Le module de formation a été dispensé par des formateurs nationaux et organisé en coopération avec des institutions nationales de formation. En outre, en coopération avec d'autres projets, la première [Conférence internationale des formateurs judiciaires nationaux sur la cybercriminalité et les preuves électroniques](#) a été organisée, qui a réuni des institutions de formation et des formateurs nationaux du monde entier pour déterminer les besoins et les priorités en matière de formation sur la cybercriminalité et les preuves électroniques et réfléchir aux avantages, à la faisabilité et aux mesures à prendre concernant la création d'un réseau national de formateurs judiciaires sur la cybercriminalité et les preuves électroniques.

### **3.6 Projet [CyberSud](#) sur la cybercriminalité et les preuves électroniques dans la région du voisinage sud**

Le projet joint CyberSud du Conseil de l'Europe et de l'Union européenne couvre la région du voisinage méridional avec l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie comme pays prioritaires initiaux. Il a une durée de 36 mois (juillet 2017 - juin 2020) avec un budget de 3,33 millions d'euros.

L'objectif est de renforcer la législation et les capacités institutionnelles en matière de cybercriminalité et de preuves électroniques dans la région du voisinage sud, conformément aux exigences des droits de l'homme et de l'état de droit. Il se concentre sur la législation relative à la cybercriminalité, les services de police spécialisés et la coopération interinstitutionnelle, la formation judiciaire, les points de contact 24/7 et la coopération internationale, ainsi que les politiques en matière de cybercriminalité. La conférence de lancement s'est tenue à Tunis en mars 2018.

Au cours de la deuxième année de sa mise en œuvre, CyberSud est devenu un partenaire majeur soutenant les cinq pays prioritaires dans la coopération sur la cybercriminalité et les preuves électroniques.

Les actions du projet allaient de la réflexion régionale sur l'élaboration de rapports de situation nationales sur la cybercriminalité et les preuves électroniques, à des ateliers de conseil législatif spécialisés, à la formation des magistrats et des services de détection et de répression et enfin à la participation des pays aux forums internationaux sur la cybercriminalité, ce qui a entraîné des changements ayant un impact durable sur la coopération internationale.

Le CyberSud a organisé 52 activités (nationales/régionales/internationales) ciblant les pays prioritaires entre octobre 2018 et septembre 2019. Le projet a démarré avec une phase de démarrage de huit mois, sans aucun antécédent de coopération avec quatre des pays (à l'exception du Maroc). Il s'agit là d'une réalisation importante : la confiance et l'engagement des pays à coopérer avec le Conseil de l'Europe non seulement pour tirer profit des activités, mais aussi pour contribuer et acquérir les mêmes normes et capacités que les autres Etats européens dans la coopération en matière de cybercriminalité et de preuves électroniques.

Une centaine de magistrats de référence ont été formés sur le sujet et des groupes de travail ont été créés pour élaborer des cours nationaux sur la cybercriminalité et les preuves électroniques pour la formation initiale et continue.

Les services de détection et de répression des pays prioritaires ont eu la possibilité de mettre à jour leurs procédures et pratiques de travail en participant à des ateliers et à des activités de formation, notamment sur la compromission des e-mails professionnels et la fraude par carte de crédit, le criminalistique informatique en direct, le darkweb et les cryptomonnaies, les enquêtes en ligne sous couverture, les enquêtes d'OSINT (Open Source Intelligence) et les analyses de logiciels malveillants.

Ces organismes ont contribué à l'adaptation du cours E-First (mis au point par le Groupe européen de formation et d'éducation en matière de cybercriminalité, ECTEG), un cours en arabe sur la cybercriminalité et les preuves en ligne destiné aux primo-intervenants. Cette action a été complétée par un appui à une approche stratégique du renforcement des capacités répressives en matière de cybercriminalité et de preuves électronique visant à rendre les compétences et les qualifications disponibles aux niveaux national et régional.

Bien que le Maroc soit déjà partie à la Convention et que la Tunisie ait été invitée à y adhérer, le Liban et la Jordanie ont également accompli des progrès importants dans l'alignement de leur législation sur les normes de la Convention de Budapest. Plus important encore, le Liban et la Jordanie ont compris l'importance de devenir parties à un tel accord international, qui fournit une base juridique pour l'échange accéléré d'informations essentielles aux enquêtes sur la cybercriminalité et les éléments de preuve électroniques.

### **3.7 Élargissement du projet [GLACY+](#) sur l'action mondiale contre la cybercriminalité**

Sur la base de l'expérience du GLACY, le Conseil de l'Europe et l'Union européenne sont convenus d'assurer le suivi du projet GLACY+ sur une « Action mondiale contre la cybercriminalité élargie ». Le projet a démarré techniquement en mars 2016 avec une durée initiale de quatre ans et un budget de 10 millions d'euros.

Compte tenu de son impact et des besoins croissants suite aux demandes d'adhésion ou d'adhésion à la Convention de Budapest (Cap-Vert, Nigeria, Chili, Costa Rica), de l'intérêt pour l'adhésion et des besoins d'assistance des autres pays (Burkina Faso, Gambie, Népal, Samoa, Ouganda, Vanuatu et autres), le budget a été porté à 13,35 millions EUR en mars 2018 et sa durée prolongée jusqu'en février 2021. En septembre 2019, une nouvelle augmentation et extension était à l'étude.

Le GLACY+ comprend trois composantes :

1. La Promotion de l'adoption et de la mise en œuvre d'une législation, de politiques et de stratégies cohérentes en matière de cybercriminalité ;

2. Le Renforcement de la capacité des autorités policières à enquêter sur la cybercriminalité et à coopérer efficacement entre elles, ainsi qu'au niveau international avec les unités de cybercriminalité en Europe et dans d'autres régions;
3. L'aide aux autorités de justice pénale dans l'application de la législation, la poursuite et le jugement des affaires de cybercriminalité et de preuves électroniques et de s'engager dans la coopération internationale.

En vertu d'un accord de partenariat avec le Conseil de l'Europe, INTERPOL dirige la mise en œuvre de la composante police du projet. Parmi les autres partenaires du projet figurent l'Estonie (Ministère de la Justice), la France (Ministère de l'Intérieur), la Roumanie (Police Nationale, Ministère Public (DIICOT) et Ministère de la Justice), le Royaume-Uni (Agence nationale de lutte contre la criminalité) et les États-Unis (Département de la Justice) ainsi que Europol (Centre Européen de lutte contre la Cybercriminalité - EC3).

Entre octobre 2018 et septembre 2019, GLACY+ a soutenu quelque 96 activités impliquant plus de 80 pays dans le monde.

Au cours de cette période, l'accent a été mis sur le renforcement de la législation. Des missions consultatives sur la législation ont été effectuées au [Costa Rica](#), au [Guatemala](#), au Kenya, au [Mexique](#), en [Namibie](#), en [Sierra Leone](#) et en [Gambie](#).

L'une des caractéristiques de GLACY+ est la recherche de synergies avec d'autres organisations et programmes internationaux :

- Un événement majeur à cet effet a été le premier [Forum africain sur la cybercriminalité](#), auquel ont participé 300 délégués de 52 pays africains. Il a été organisé conjointement avec la Commission de l'Union africaine et plusieurs organisations régionales et internationales, dont l'ONUDC, INTERPOL, le Secrétariat du Commonwealth, la Banque mondiale, ainsi que l'Office du Foreign et Commonwealth du Royaume-Uni, le Département de la Justice des États-Unis et le Département d'État américain.
- La Co-organisation de la [3<sup>ème</sup> réunion du Groupe de travail sur la cybercriminalité du Pacific Island Law Officers Network \(PILON\)](#) à Vanuatu en mai 2019 en coopération avec le Secrétariat du PILON et l'Australie. Cela a contribué à la réforme de la législation interne dans six États insulaires du Pacifique.
- La coopération s'est développée avec le FOPREL (Forum des Présidents des pouvoirs législatifs d'Amérique centrale et du bassin des Caraïbes) à travers [un atelier régional et un échange de lettres](#). Cela a permis de s'adresser aux parlements nationaux de la région et de les sensibiliser à l'alignement des législations nationales sur la cybercriminalité et les preuves électroniques sur la Convention de Budapest.

- La Conférence internationale conjointe d'[Eurojust et du Conseil de l'Europe sur les enquêtes en ligne sur les abus envers les enfants dans le Darknet](#) fin septembre 2019.
- Les Synergies avec d'autres projets financés par l'UE et actifs dans des domaines complémentaires et des zones géographiques similaires (à savoir OCWAR-C, Cyber4D et EIPacCto), grâce à des réunions de coordination avec les unités de gestion de projets concernées et leurs homologues de la Commission européenne. La coordination avec le projet SIRIUS d'Europol a également été assurée.
- Parmi les autres activités menées dans ce cadre, citons la participation de tous les pays prioritaires du GLACY+ au [Cyber Forum de l'UE](#), l'élaboration d'un [manuel](#) conjoint Conseil de l'Europe – l'Agence des droits fondamentaux de l'UE [sur la cybercriminalité et les droits fondamentaux](#), les contributions au GFCE (Global Forum on Cybercrime Expertise) et le groupe de travail de l'ICANN sur la sécurité publique.

La coopération internationale et le partage des bonnes pratiques ont été encouragés par un certain nombre de réunions régionales et internationales. Par exemple, la République dominicaine a accueilli des [manifestations pour les pays des Caraïbes](#), le Cap-Vert pour les bureaux des procureurs de tous les [pays lusophones](#), le Chili a accueilli la réunion du [Réseau ibéro-américain de cyberprocureurs](#) (« CiberRede ») et le Nigeria a accueilli l'[Atelier régional africain](#) sur la cybercriminalité, la cybersécurité nationale et le piratage sur Internet.

En outre, des manifestations internationales ont été organisées pour renforcer les compétences techniques des enquêteurs de la cybercriminalité des pays du GLACY+ :

- l'[Atelier INTERPOL sur les voies et moyens de coopération internationale en matière de cybercriminalité](#) ;
- la [Formation de formateurs sur la cybercriminalité et les preuves électroniques](#) pour les premiers intervenants des gendarmeries africaines ;
- la formation INTERPOL à l'analyse des logiciels malveillants.

Les capacités de l'appareil judiciaire et du parquet ont été renforcées grâce à des cours d'initiation et de perfectionnement au [Cap-Vert](#), au [Chili](#), au [Costa Rica](#), en République dominicaine, au Ghana, en [Indonésie](#), à Maurice, au [Nigéria](#) et au Sri Lanka. Dans plusieurs cas, l'équipe de formateurs se composait en tout ou en partie de juges, de magistrats ou de procureurs précédemment formés dans le cadre des activités du GLACY et du GLACY+. Certains des formateurs ont également présenté le programme de formation du Conseil de l'Europe à leurs pairs des pays voisins, des formations judiciaires étant organisés aux Philippines pour la [région de l'ANASE](#) et au Sénégal pour les pays francophones et lusophones de la [CEDEAO](#).

Dans le but de créer un réseau de ces formateurs, une [réunion internationale de formateurs judiciaires nationaux et internationaux sur la cybercriminalité et les preuves électroniques](#), formés dans le cadre des programmes du Conseil de l'Europe, a été organisée à

Strasbourg. Les besoins de formation et les nouveaux cours, les programmes de certification et la faisabilité d'un réseau international de formateurs judiciaires ont été discutés.

En outre, l'intégration de modules de formation dans les programmes des établissements de formation judiciaire et l'intégration des procédures d'entraide judiciaire ont été facilitées au [Costa Rica](#), en République dominicaine et au [Ghana](#).

Enfin, les capacités des services chargés de l'application de la loi ont été renforcées avec l'appui d'INTERPOL, en tant que partenaire d'exécution du projet, grâce à des ateliers/formations sur les enquêtes en matière de cybercriminalité, les preuves électroniques et la coopération internationale à Singapour (avec la participation de tous les pays GLACY+), en République dominicaine, aux Philippines et à Tonga.

Des conseils opérationnels ont été fournis dans le cadre de missions techniques sur la mise en place d'unités d'enquête sur la cybercriminalité et d'unités de criminalistique des données au Nigéria et au Cap-Vert et sur l'intégration des matériels de formation ECTEG dans le plan de formation des services de répression aux Tonga. D'autres capacités de détection et de répression ont été renforcées par des formations et des cours techniques sur les outils et services INTERPOL au Cap-Vert, en Colombie, au Ghana, à Hong Kong, à Hong Kong, à l'Île Maurice, au Maroc, au Nigéria, au Sénégal et à Sri Lanka.

En conclusion, pendant cette période, le projet GLACY+ a eu un impact en termes de :

- Mise en œuvre des dispositions de la Convention de Budapest et de sensibilisation à ses avantages ;
- Coopération internationale et de synergies avec un large éventail d'organisations et de projets pertinents ;
- Renforcement des capacités dans des pays du monde entier grâce à une formation judiciaire et policière sur la cybercriminalité et les preuves électroniques.

### **3.8 [EndOCSEA@Europe](#) pour mettre fin à l'exploitation et aux abus sexuels des enfants en ligne en Europe**

Le projet End Online Child Sexual Exploitation and Abuse @ Europe (EndOCSEA@Europe) est mis en œuvre par la Division des droits de l'enfant du Conseil de l'Europe avec le soutien du bureau de programme C-PROC. Le projet bénéficie à l'ensemble des 47 Etats membres du Conseil de l'Europe, en particulier à l'Albanie, l'Arménie, l'Azerbaïdjan, la Bosnie-Herzégovine, la Géorgie, la République de Moldova, le Monténégro, la Serbie, la Turquie et l'Ukraine. Le projet est financé par le Fonds pour mettre fin à la violence contre les enfants (EVAC), a une durée de 30 mois (juillet 2018 - décembre 2020) et un budget de 849.041 euros.

Les objectifs du projet sont de :

- Renforcer la collaboration multidisciplinaire aux niveaux national et régional, par le biais de structures de gouvernance nationales et d'analyses de situation (risques/réponses en matière d'exploitation et d'abus sexuels des enfants en ligne);
- Soutenir les réformes législatives et procédurales, la formation et le renforcement des capacités des responsables de l'application des lois, des juges et des procureurs afin qu'ils puissent apporter un soutien de bout en bout aux victimes ;
- S'attaquer aux capacités sociétales par la sensibilisation, l'éducation des principaux groupes cibles et l'autonomisation des enfants.

Ce projet est mis en œuvre dans le cadre de la Stratégie du Conseil de l'Europe pour les droits de l'enfant (2016-2021) et contribue au travail dans deux domaines prioritaires : le droit de l'enfant à une vie sans violence et les droits de l'enfant dans un environnement numérique.

Au cours de la période d'octobre 2018 à septembre 2019, le projet a, entre autres choses :

- Appuyé les États signataires de la Convention de Lanzarote afin de faciliter leur participation à la réunion du Comité de Lanzarote, du 5 au 7 mars 2019.
- Confirmé<sup>13</sup> l'Arménie, l'Azerbaïdjan et l'Ukraine en tant que pays pilotes pour les activités de projet, y compris l'analyse des lacunes et l'élaboration de modules de formation.
- Analysé les réponses permettant de prévenir et de combattre l'exploitation et la maltraitance sexuelles des enfants en ligne aux niveaux national et régional, et a réalisé une cartographie de référence des réponses des Etats membres du Conseil de l'Europe et une étude comparative des mécanismes collectifs disponibles au niveau paneuropéen doivent être publiées en novembre 2019.
- Entrepris des recherches sur la législation, les politiques et les pratiques visant à prévenir et à combattre l'exploitation sexuelle des enfants en ligne en Arménie, en Azerbaïdjan et en Ukraine. Des visites in situ et des ateliers avec les ministères et autorités compétents ont eu lieu en Azerbaïdjan, en Arménie et en Ukraine entre juin et septembre. Les conclusions et recommandations de l'analyse des écarts seront publiées en novembre 2019.
- Dialogué avec des organisations de la société civile en vue de renforcer leurs capacités et leurs contributions au mécanisme de mise en œuvre et de suivi de la *Convention de Lanzarote*. 35 organisations de la société civile actives dans 20 Etats membres ont participé à une [conférence internationale](#) les 8 et 9 avril 2019 à Strasbourg (France).

---

<sup>13</sup> par le groupe de pilotage du projet, comprenant des représentants de chacun des 10 pays concernés.

- Adopté des [priorités stratégiques pour renforcer la coopération multisectorielle afin de prévenir et de combattre l'exploitation et la maltraitance sexuelle des enfants en ligne](#) lors d'une conférence internationale qui s'est tenue les 16 et 17 mai 2019 à Strasbourg et qui a réuni plus de 70 participants de 22 pays.
- Octroyé des subventions à des organisations de la société civile en République de Moldova, Serbie et Ukraine, ainsi qu'au Bureau des défenseurs des droits de l'Homme au Monténégro, pour développer des outils et des activités de sensibilisation. Plus de 5 000 enfants et 42 écoles participeront aux ateliers et aux campagnes, 5 outils d'information et de plaidoyer seront développés d'ici juillet 2020.
- Elaboré une version adaptée aux enfants de la *Convention de Lanzarote*, avec la participation d'enfants, qui doit être publiée en novembre 2019.
- Sensibilisé de manière accrue aux activités du projet et fait participer nombre d'experts des pays cibles à d'autres événements pertinents, tels que la Conférence de l'OCDE sur la protection des enfants dans un monde connecté (Zurich, Octobre 2018), la Conférence régionale sur les stratégies de Cybercriminalité (Tbilissi, Décembre 2018), la Conférence conjointe Eurojust sur les enquêtes en ligne : Darkweb et abus d'enfants en ligne (La Haye, Septembre 2019), 23ème Conférence annuelle de l'ENOC sur les droits des enfants dans l'environnement numérique (Belfast, Septembre 2019).

#### 4. Impact

Le C-PROC a soutenu quelque 850 activités au cours des cinq années et demie écoulées depuis avril 2014, date à laquelle il est devenu opérationnel, et quelque 240 entre octobre 2018 et septembre 2019.

Une quarantaine de pays prioritaires ont bénéficié d'un large éventail de soutiens. Une centaine d'autres pays ont participé à des activités régionales ou internationales ou ont bénéficié d'une assistance spécifique, telle que des conseils sur la législation.

L'analyse de l'impact de toutes ces activités, par exemple en termes d'enquêtes, de poursuites, d'adjudications ou de coopération internationale, dépasserait le cadre du présent rapport.

Cependant, les éléments suivants peuvent illustrer l'impact du C-PROC :

- L'augmentation du nombre de membres de la Convention de Budapest : depuis 2014, 23 autres États sont devenus parties à ce traité (Andorre, Argentine, Cap-Vert, Canada, Chili, Costa Rica, Ghana, Grèce, Israël, Liechtenstein, Île Maurice, Monaco, Maroc, Panama, Paraguay, Pérou, Philippines, Pologne, Saint-Marin, Sénégal, Sri Lanka, Tonga, Turquie), d'autres ont été invités à y adhérer (Bénin, Nigeria, Tunisie) et des consultations étaient en cours avant septembre 2019. Alors que les États européens auraient adhéré tôt ou tard de toute façon, le renforcement

des capacités du C-PROC a été l'un des principaux facteurs d'adhésion de la plupart des pays non européens.

- L'impact sur la législation : le C-PROC, dans le cadre de plusieurs projets, suit de près l'évolution de la législation sur la cybercriminalité et les preuves électroniques dans le monde depuis 2013. La [dernière mise à jour a été préparée en juin 2019](#). Les résultats indiquent qu'en juin 2019, plus de la moitié des États membres de l'ONU avaient un droit pénal matériel largement conforme à la Convention de Budapest. Des progrès satisfaisants ont également été accomplis en ce qui concerne les pouvoirs procéduraux. En juin 2019, 152 États (79 % des membres de l'ONU) semblaient avoir utilisé la Convention de Budapest comme ligne directrice ou au moins comme source pour élaborer leur législation nationale. En Afrique, en Asie-Pacifique et en Amérique latine, cela est dû en grande partie aux activités de renforcement des capacités.

#### Dispositions de droit pénal matériel conformes à la Convention de Budapest

	États	Largement en place jusque janvier 2013		Largement en place jusque juin 2019	
L'ensemble de l'Afrique	54	6	11%	18	33%
L'ensemble de l'Amérique	35	10	29%	15	43%
L'ensemble de l'Asie	42	13	31%	18	43%
L'ensemble de l'Europe	48	38	79%	45	94%
L'ensemble de l'Océanie	14	3	21%	4	29%
<b>Total</b>	<b>193</b>	<b>70</b>	<b>36%</b>	<b>100</b>	<b>52%</b>

#### Pouvoirs procéduraux spécifiques pour obtenir des preuves électroniques

	États	Largement en place jusque janvier 2013		Largement en place jusque juin 2019	
L'ensemble de l'Afrique	54	5	9%	15	28%
L'ensemble de l'Amérique	35	5	14%	12	34%
L'ensemble de l'Asie	42	8	19%	13	31%
L'ensemble de l'Europe	48	31	65%	40	83%
L'ensemble de l'Océanie	14	1	7%	3	21%
<b>Total</b>	<b>193</b>	<b>50</b>	<b>26%</b>	<b>82</b>	<b>43%</b>

- Le renforcement des garanties : compte tenu de la nécessité de concilier l'efficacité de la justice pénale et les garanties de l'État de droit, le C-PROC soutient non seulement les réformes du droit pénal, mais aussi la législation sur la protection

des données avec la Convention 108 sur la protection des données et ses protocoles. A cet effet, le C-PROC s'appuie sur l'expertise de l'Unité de protection des données du Conseil de l'Europe. Le Kenya, le Nigéria, le Sri Lanka et la République dominicaine en sont des exemples. Ce n'est donc pas un hasard si 49 des 64 Parties à la Convention de Budapest sont actuellement Parties à la Convention 108.

- Les synergies se sont accrues : le manque de coordination et de cohérence des organisations chargées du renforcement des capacités ou le fait qu'elles soient en concurrence les unes avec les autres a été une préoccupation majeure pendant des années.<sup>14</sup> La recherche de partenariats et de synergies guide donc le C-PROC et se traduit par des projets communs avec l'Union européenne, une coopération avec Eurojust et Europol, des accords avec INTERPOL, la Commission de l'Union africaine, l'ECOWAS ou FOPREL, mais aussi avec des institutions des Parties à la Convention de Budapest comme l'Estonie, la France, la Roumanie, le Royaume-Uni ou les Etats-Unis, la participation à ICANN ou au Forum Mondial sur la Cyber-expertise, et à de nombreux autres. Le Forum pour l'Afrique (Éthiopie, octobre 2018), la réunion PILON pour les États insulaires du Pacifique (mai 2019) ou la Conférence Eurojust/Conseil de l'Europe sur la maltraitance des enfants dans le Darknet (septembre 2019) sont des exemples de l'utilité de cette coopération avec les autorités judiciaires pénales sur place.
- La formation durable : le C-PROC soutient des programmes de formations durables qui peuvent avoir un impact à long terme. En ce qui concerne la formation judiciaire, dans de nombreux pays prioritaires, le séquençage a consisté en :
  1. Formation des formateurs des académies nationales de formation ;
  2. Adaptation des modules de formation aux besoins nationaux ;
  3. Assistance aux formateurs formés dans la conduite des cours pilotes ;
  4. Insertion de modules dans les programmes réguliers des écoles de formation ;

En juillet 2019, un élément supplémentaire a été lancé, à savoir la création d'un [réseau de formateurs judiciaires formés à la cybercriminalité et aux preuves électroniques](#).

En résumé, l'expérience des cinq ans et demi écoulés depuis la création du C-PROC confirme que le renforcement des capacités est un moyen efficace d'aider les sociétés de toutes les régions du monde à relever le défi majeur de la cybercriminalité. Le renforcement des capacités en matière de cybercriminalité et de preuves électroniques :

- fonctionne, répond aux besoins et a un impact en termes d'action de la justice pénale sur la cybercriminalité et les preuves électroniques avec des garanties en matière d'État de droit ;
- facilite la coopération multipartite ;

---

<sup>14</sup> Cette question a été soulevée, entre autres, lors de plusieurs conférences Octopus (voir par exemple [Octopus 2011](#)).

- présente des avantages sur le plan du développement humain et contribue à la réalisation des objectifs des Nations Unies en matière de développement durable ;
- contribue à réduire la fracture numérique ;
- repose sur un large soutien international et peut contribuer à surmonter les divisions politiques.

## 5. Conclusions et priorités

Les conclusions suivantes peuvent être tirées :

- Entre octobre 2018 et septembre 2019, le Bureau a appuyé environ 240 activités dans le cadre de sept projets couvrant des régions prioritaires en Europe ainsi que des pays d'autres régions du monde, qui se sont engagés à appliquer la Convention de Budapest. Des fonctionnaires de plus de 120 pays ont participé aux activités du projet au cours de cette période.
- Au cours de ces douze mois, le Bureau a encore amélioré ses performances en termes de qualité, d'efficacité, de résultats et d'impact. Les activités soutenues par le C-PROC ont eu un impact en termes d'adhésion à la Convention de Budapest et de niveau de mise en œuvre, de renforcement de la législation dans le monde entier sur la base de ce traité, de programmes durables de formation judiciaire et répressive sur la cybercriminalité et les preuves électroniques, de renforcement de la coopération internationale, notamment par des contacts permanents et permanents, ainsi que des partenariats et synergies avec un grand nombre d'organisations.
- Par l'intermédiaire du Bureau de programme de lutte contre la cybercriminalité, le Conseil de l'Europe demeure un chef de file mondial en matière de renforcement des capacités dans le domaine de la cybercriminalité et des preuves électroniques. Le C-PROC confirme que le renforcement des capacités a un impact et constitue un moyen efficace d'aider les sociétés du monde entier à relever le défi majeur de la cybercriminalité.
- Le « triangle dynamique » combinant des normes convenues (Convention de Budapest), avec un suivi par le T-CY et le renforcement des capacités par le C-PROC est une caractéristique distinctive du Conseil de l'Europe qui demeure très efficace. Les projets C-PROC soutiennent la mise en œuvre de la Convention de Budapest et assurent le suivi ou contribuent aux travaux du Comité de la Convention sur la cybercriminalité. Etant donné les récents défis budgétaires du Conseil de l'Europe, il est très précieux que le T-CY puisse compter sur des contributions volontaires par le biais du projet Cybercrime@Octopus. Le T-CY et la préparation du 2<sup>nd</sup> Protocole additionnel à la Convention de Budapest n'ont donc pas été affectés par les difficultés financières auxquelles le Conseil de l'Europe a été confronté pendant cette période.
- La Convention de Budapest est l'un des traités du Conseil de l'Europe qui compte le plus grand nombre de parties et il a une portée mondiale. Avec chaque nouvelle

partie, la Convention de Budapest et la coopération internationale en matière de cybercriminalité deviendront plus efficaces. Etant donné que tous les Etats membres sauf un sont parties ou signataires, les parties supplémentaires seront des Etats non membres du Conseil de l'Europe. Entre octobre 2018 et septembre 2019, l'Argentine, le Cap-Vert, le Ghana, le Maroc, le Paraguay et le Pérou sont devenus parties. Le Bureau contribue à faire en sorte que les parties potentielles et effectives aient la capacité d'appliquer la Convention de Budapest.

- Le C-PROC reste l'un des bureaux extérieurs du Conseil de l'Europe les plus performants en matière de mobilisation des ressources. Un grand nombre d'activités sont menées par le C-PROC et ont un impact efficace et rentable. C'est ce qui rend le Bureau attrayant pour les donateurs. En septembre 2019, des projets d'un volume de plus de 32 millions d'euros étaient en cours.
- L'Union européenne reste le principal bailleur de fonds par le biais de projets joints cofinancés par le Conseil de l'Europe. Entre octobre 2018 et septembre 2019, des contributions volontaires ont également été reçues des Pays-Bas, du Royaume-Uni, du Japon et des États-Unis pour le projet Cybercrime@Octopus.
- Non seulement le Gouvernement roumain met gratuitement à disposition des locaux à usage de bureaux, mais il y apporte également son soutien par le biais de son expertise. Le Ministère de la justice, la Police nationale, le ministère public (DIICOT), l'Institut national de la magistrature et l'Équipe d'intervention d'urgence informatique contribuent en substance aux activités du projet.
- Plusieurs autres États (Allemagne, Estonie, États-Unis, France, Royaume-Uni et Espagne) ainsi que le Centre européen de la cybercriminalité d'Europol (EC3) et INTERPOL sont également partenaires d'un ou plusieurs projets. De nombreuses activités de projet sont menées en partenariat avec un large éventail d'organisations des secteurs public et privé ou avec leur participation.

Tout en suivant la voie qui s'est jusqu'ici révélée fructueuse et efficace en partenariat avec d'autres organisations, les priorités spécifiques du Bureau pour les douze mois à venir seront :

- Nourrir le triangle dynamique de la Convention de Budapest, du T-CY et du renforcement des capacités : le C-PROC oeuvrera à faciliter l'adhésion d'États supplémentaires à la Convention de Budapest et soutiendra le T-CY dans la préparation du 2<sup>nd</sup> Protocole additionnel. Une fois le Protocole adopté, il faudra appuyer sa mise en œuvre par les parties à la Convention.
- Mettre l'accent sur les droits de l'homme et les garanties de l'État de droit : les Projets C-PROC visent à soutenir l'élaboration d'une législation spécifique assortie de garanties, de procédures normalisées et mettant fortement l'accent sur la formation des juges. Il conviendra de continuer à soutenir l'élaboration d'une législation sur la protection des données conforme à la Convention 108 modernisée

sur la protection des données, en coopération avec l'Unité Protection des données du Conseil de l'Europe.

- Renforcer l'expertise du Bureau : le rôle du C-PROC en tant que centre de connaissances spécialisées doit être encore renforcé grâce à des matériels de formation, des outils et des ressources en ligne ainsi qu'au suivi de l'évolution de la législation dans le monde.
- Mobiliser des ressources : le portefeuille actuel de projets couvre des régions prioritaires en Europe (région du partenariat oriental, Europe du Sud-Est et Turquie) ainsi que des pays d'autres parties du monde engagés dans la mise en œuvre de la Convention de Budapest. Certains de ces projets prendront fin d'ici quelques mois et un suivi sera nécessaire :
  - le suivi d'iPROCEEDS sur les flux d'argent criminels en ligne en Europe du Sud-Est, le projet actuel devant s'achever en décembre 2019 ;
  - le projet de suivi de Cybercrime@Octopus (se terminant en décembre 2020) sera financé par des contributions volontaires. Il s'agit notamment d'appuyer les travaux du Comité de la Convention sur la cybercriminalité ;
  - l'élargissement du GLACY+ en termes de budget et de durée pour répondre aux demandes croissantes d'assistance et d'adhésions à la Convention de Budapest ;
  - l'extension de CyberSud pour le voisinage sud, le projet en cours devant s'achever en juin 2020 ;
  - le nouveau projet sur la xénophobie et le racisme (CybercrimeXR) pour soutenir la mise en œuvre du Protocole à la Convention de Budapest sur la cybercriminalité ;
  - assurer le suivi d'EndOCSEA@Europe afin de prévoir un éventail plus large de mesures de renforcement des capacités pour la protection des enfants contre la violence sexuelle en ligne (le projet actuel prend fin en décembre 2020).
- Les synergies et partenariats : ces caractéristiques seront encore renforcées par la coopération avec des organisations extérieures (par exemple en ajoutant une composante à GLACY+ pour soutenir les institutions régionales de formation) mais aussi au sein du Conseil de l'Europe (par exemple par des activités liées aux Conventions de Lanzarote, d'Istanbul ou sur la traite).

En résumé, le C-PROC devrait continuer d'évoluer en termes de qualité, d'expertise, d'impacts et de synergies pour la coopération mondiale en matière de cybercriminalité et de preuves électroniques.

## 6. Annexe : Inventaire des activités soutenues par le C-PROC (Octobre 2018 – Septembre 2019)

### Octobre 2018

iPROCEEDS	<a href="#">Deuxième prestation nationale du module de formation d'introduction sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne</a> , Bihać, Bosnie-Herzégovine, 1-4 octobre 2018.
CyberCrime@EAP 2018	Cours ECTEG sur l'investigation des réseaux, Erevan, Arménie, 1-5 octobre 2018
CyberSud	<a href="#">Formation des magistrats sur la cybercriminalité et la preuve électronique niveau Avancé</a> , Rabat, Maroc, 1-5 octobre 2018
GLACY+ Cybercrime@Octopus	Atelier sur la législation relative à la protection des données, Nairobi, Kenya, 2-5 octobre 2018
iPROCEEDS Cybercrime@Octopus	<a href="#">Forum régional sur la fraude en ligne</a> , Zagreb, Croatie, 4-5 octobre 2018
GLACY+	<a href="#">Mission consultative sur la législation en matière de cybercriminalité et mission consultative sur les politiques et stratégies nationales en matière de cybercriminalité</a> , San José, Costa Rica, 8-11 octobre 2018
CyberSud	<a href="#">Atelier sur la Convention de Budapest en Jordanie</a> , Amman, Jordanie, 8-9 octobre 2018
CyberCrime@EAP 2018	Conférence de l'OSCE sur la prévention et la lutte contre le terrorisme à l'ère numérique, Minsk, Bélarus, 9-10 octobre 2018
CyberCrimeCyberSud@EAP 2018	Exercice sur table sur la coopération internationale en matière de cybercriminalité, Minsk, Bélarus, 11-12 octobre 2018
CyberCrime@EAP 2018	Réunion sur la poursuite du renforcement des capacités en matière de cybercriminalité dans la région du Partenariat oriental, Bucarest, Roumanie, 12 octobre 2018
CyberCrime@EAP 2018	Exercice sur table sur la coopération internationale en matière de cybercriminalité, Tbilissi (Géorgie), 15-16 octobre 2018
GLACY+	Formation INTERPOL aux enquêtes en matière de cybercriminalité pour la région Afrique, Nairobi (Kenya), 15-19 octobre 2018
iPROCEEDS	<a href="#">Formation régionale ECTEG sur les enquêtes sur les logiciels malveillants en</a> coopération avec le Département de la cybercriminalité, Police nationale turque, Ankara, Turquie, 15-19 octobre 2018
GLACY+ CyberSud Cybercrime@Octopus	<a href="#">Forum africain sur la cybercriminalité : Politiques et législation, Coopération internationale et renforcement des capacités</a> , Addis-Abeba, Éthiopie, 16-18 octobre 2018
iPROCEEDS	Réunion du groupe de travail chargé d'élaborer/améliorer les lignes directrices et les indicateurs pour les entités du secteur financier afin de prévenir le blanchiment d'argent dans l'environnement en ligne, Sarajevo, Bosnie-Herzégovine 18 octobre 2018
CyberCrime@EAP 2018	Exercice sur table sur la coopération internationale en matière de cybercriminalité, Kiev, Ukraine, 18-19 octobre 2018
CyberCrime@EAP 2018	Cours ECTEG sur la criminalistique des données en direct, Bakou, Azerbaïdjan, 22-26 octobre 2018

GLACY+ Cybercrime@Octopus	Atelier sur la cybercriminalité et les preuves électroniques à l'intention des juges de la Cour suprême, Accra, Ghana, 23 octobre 2018
GLACY+	Atelier sur la cybercriminalité et la preuve électronique à l'intention des juges de la Cour d'appel, Accra, Ghana, 24 octobre 2018
GLACY+ Cybercrime@Octopus	<a href="#">Atelier sur la cybercriminalité et la cybersécurité à l'intention de certains parlementaires</a> , Accra (Ghana), 25 octobre 2018
GLACY+ Cybercrime@Octopus	Participation au Forum du secteur de la justice pénale sur la cybercriminalité, Accra, Ghana, 23 octobre 2018
GLACY+	Conférence internationale sur la cybercriminalité organisée par l'École de la magistrature de la République dominicaine, Saint-Domingue, République dominicaine, 25-26 octobre 2018
CyberCrime@EAP 2018	Soutien à la Semaine régionale du cyberespace et à l'Expo 2018 en Moldova, Kishinev, République de la Moldova, 29 octobre - 2 novembre 2018
GLACY+	Cours ECTEG sur la cybercriminalité et la criminalistique numérique à l'intention des agents de la force publique, Colombo (Sri Lanka), 29 octobre - 2 novembre 2018
EndOCSEA@Europe	Atelier de l'OCDE sur la protection des enfants dans l'environnement numérique, Zurich, Suisse, 15-16 octobre 2018.
EndOCSEA@Europe	Conférence de l'ERA sur la cyberintimidation, le sexting et le sextortion - réponses juridiques aux risques et dangers pour les enfants dans le cyberespace, Barcelone, Espagne, 29-30 octobre 2018.

### Novembre 2018

CyberCrime@EAP 2018	Mission consultative sur la coopération internationale par l'intermédiaire de points de contact et d'entraide judiciaire 24/7, Kiev (Ukraine), 1er et 2 novembre 2018
iPROCEEDS	<a href="#">Cours de formation sur les cryptocurrencies</a> , Budapest, Hongrie, 5-7 novembre 2018
GLACY+ Cybercrime@Octopus	<a href="#">Formation judiciaire de base sur la cybercriminalité à l'intention des formateurs/juges, procureurs et avocats et adaptation des matériels au contexte local</a> , Santiago du Chili, Chili, 5-9 novembre 2018
CyberCrime@EAP 2018	Mission consultative sur la coopération internationale par l'intermédiaire de points de contact et d'entraide judiciaire 24 heures sur 24/7, Kiev (Ukraine), 6-8 novembre 2018
CyberSud	<a href="#">Visite d'étude de la Gendarmerie - Centre de prévention et de lutte contre la criminalité informatique et la cybercriminalité (CPLCIC)</a> , Algiers, Algérie, 7-8 novembre 2018
CyberCrime@EAP 2018	Appui au Forum géorgien sur la cybersécurité 2018, Kvareli (Géorgie), 9 novembre 2018
CyberSud	<a href="#">Atelier sur la fraude en ligne et les fraudes aux paiements électroniques, Bucarest</a> , Roumanie, 12-14 novembre 2018
CyberSud	<a href="#">Formation initiale des magistrats en matière de cybercriminalité et preuve numérique</a> , Tunis, Tunisie, 12-14 novembre 2018
iPROCEEDS	<a href="#">Exercice régional de simulation de cas sur la cybercriminalité et les enquêtes financières</a> , Bucarest, Roumanie, 12 - 15 novembre 2018

GLACY+	<a href="#">Formation judiciaire avancée sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et autres membres du personnel judiciaire des pays francophones et lusophones de la CEDEAO + la Mauritanie</a> , Dakar, Senegal 12-15 novembre 2018
GLACY+	Conférence sur la cybercriminalité organisée par FIIAP, P, gestion du projet conjoint UE-FIIAPP El PaCcto, San Salvador, El Salvador, 13-14 novembre 2018
GLACY+	Présentation sur la Convention de Budapest et ses protocoles additionnels à l'atelier de l'ENISA-EC3 sur le CSIRT et la coopération policière internationale, Pays-Bas, 13 novembre 2018
GLACY+	Participation au séminaire « Enquêter sur le Web 2.0 - La collecte de données probantes et les défis de l'accès transfrontalier aux données », organisé par ERA et NIM (Institut National de la Magistrature), Bucarest, Roumanie, 13-14 novembre 2018
GLACY+	Atelier national sur la protection des données et les outils et services INTERPOL, ainsi que sur la mise en place et le renforcement des points de contact 24 heures sur 24 et 7 jours sur 7 pour la cybercriminalité et les preuves électroniques, Sri Lanka 14-16 novembre 2018
CyberSud	<a href="#">Table ronde sur la Cybersécurité</a> , Beyrouth, Liban, 15 novembre 2018
GLACY+	<a href="#">Cybercriminalité et droits fondamentaux - Réunion d'experts, Bucarest, Roumanie</a> , 15-16 novembre 2018
CyberSud	<a href="#">Atelier sur la Convention de Budapest</a> , Beyrouth, Liban, 16 novembre 2018
CyberSud	<a href="#">Sensibilisation et analyse des GAP sur la Convention de Budapest</a> , Amman, Jordanie, 18 novembre 2018
CyberSud	<a href="#">Formation initiale sur la cybercriminalité et les preuves électroniques pour les magistrats</a> , Amman, Jordanie, 19-22 novembre 2018
GLACY+	Atelier national sur la protection des données et les outils et services INTERPOL, ainsi que sur la mise en place et le renforcement des points de contact 24/7 pour la cybercriminalité et les preuves électroniques, Port Louis (Maurice), 19-21 novembre 2018
GLACY+	<a href="#">Cours d'introduction à la formation des formateurs sur la cybercriminalité et les preuves électroniques à l'intention des procureurs et des procureurs de la région de l'ANASE</a> , Manille (Philippines), 20-23 novembre 2018
CyberSud	<a href="#">Visite d'étude de la Garde Nationale</a> , Tunis, Tunisie, 19 et 21 novembre 2018
iPROCEEDS	<a href="#">Deuxième présentation nationale du module d'introduction sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne</a> , Ankara, Turquie 21-24 novembre 2018
CyberCrime@EAP 2018	Réunion sur le Modèle de maturité des capacités de cybersécurité pour les nations (CMM), Tbilissi, Géorgie, 22 novembre 2018

CyberSud	<a href="#">2e Comité directeur</a> , Strasbourg, France, 26 novembre 2018
CyberCrime@EAP 2018 GLACY+ iPROCEEDS CyberSud	20e réunion plénière du Comité de la Convention sur la cybercriminalité et 3ème réunion plénière de rédaction du Protocole, Strasbourg, France, 27-30 novembre 2018
CyberSud	Le 4ème Forum sur la cybercriminalité et le régime de cybersécurité - Risques et opportunités, Beyrouth, Liban, 29 novembre 2018
EndOCSEA@Europe	Réunion de planification avec WePROTECT Global Alliance et d'autres acteurs, Londres, Royaume-Uni, 8-9 novembre 2018.

### Décembre 2018

iPROCEEDS	<a href="#">Atelier sur la fraude financière et la fraude par carte de crédit en ligne</a> , Skopje, 3 décembre 2018
CyberSud	<a href="#">Formation judiciaire avancée</a> , Alger, Algérie, 2-6 décembre 2018
GLACY+	5ème réunion du Groupe de travail africain sur la cybercriminalité à l'intention des chefs des unités chargées de la cybercriminalité, Accra, GHANA, 4-6 décembre 2018
GLACY+	Réunion de la Commission interparlementaire sur la sécurité des citoyens et l'administration de la justice (CISCAJ), Guatemala, 6 décembre 2018
iPROCEEDS	<a href="#">Maîtrise en informatique légale et enquête sur la cybercriminalité Collège universitaire de Dublin - 4ème semestre</a> , Dublin, Irlande, 8-12 décembre 2018
CyberSud	<a href="#">Visite d'étude de la Direction Générale de la Sécurité Nationale (DGSN)</a> , Rabat, Maroc, 10-11 décembre 2018
iPROCEEDS	<a href="#">Atelier international sur la cybercriminalité</a> , Ankara (Turquie), 10 décembre 2018
GLACY+ Cybercrime@Octopus	Formation de formateurs de premiers intervenants à l'intention des responsables de l'application des lois, Abuja, Nigéria, 10-13 décembre 2018
Cybercrime@Octopus	<a href="#">Mission consultative pour l'élaboration de la législation en matière de la cybercriminalité et de preuve électronique</a> , Niamey, Niger, 10-13 décembre 2018
GLACY+	<a href="#">Mission consultative sur l'harmonisation de la législation sur la cybercriminalité et les preuves électroniques</a> , Freetown, Sierra Leone, 11-14 décembre 2018
CyberCrime@EAP 2018	Réunion régionale : Conférence sur les stratégies en matière de cybercriminalité et manifestation de clôture des projets Cybercrime@EaP (2015-2018), Tbilissi (Géorgie), 11-13 décembre 2018
CyberSud	<a href="#">Formation sur la preuve électronique à l'intention des magistrats libanais</a> , Beyrouth, Liban, 14 décembre 2018
GLACY+	<a href="#">Cours ECTEG, Formation spécialisée en cybercriminalité et criminalistique numérique à l'intention des agents de la force publique</a> , Dakar (Sénégal), 17-21 décembre 2018
Cybercrime@Octopus	<a href="#">Mission consultative sur le cadre législatif relatif à la cybercriminalité et aux preuves électroniques et sur l'évaluation des besoins en matière de renforcement des capacités</a> , Nouakchott, Mauritanie, 17-19 décembre 2018

Cybercrime@Octopus	Atelier sur la législation relative à la cybercriminalité et aux preuves électroniques, Astana, Kazakhstan, 20-21 décembre 2018
--------------------	---

### Janvier 2019

CyberSud	<a href="#">E- PREMIER COURS, European Cybercrime Training Education Group (ECTEG)</a> , Bucarest, Roumanie, 14-18 janvier 2019
GLACY+	Réunion de coordination avec d'autres projets financés par l'UE ayant des composantes sur la cybernétique, Bruxelles, Belgique, 16 janvier 2019
CyberSud	<a href="#">Formation judiciaire avancée sur la cybercriminalité et les preuves électroniques</a> , Beyrouth, Liban, 16-19 janvier 2019
Cybercrime@Octopus	Première réunion de travail sur la stratégie nationale de cybersécurité 2019-2020 et son plan d'action, Tbilissi, Géorgie, 17 janvier 2019
GLACY+ Cybercrime@Octopus	<a href="#">Mission consultative sur la législation relative à la cybercriminalité et aux preuves électroniques</a> , Guatemala City, Guatemala, 21-24 janvier 2019
GLACY+	<a href="#">Atelier sur la cybercriminalité et les preuves électroniques à l'intention des juges, magistrats et procureurs d'Indonésie</a> , Jakarta (Indonésie), 21-25 janvier 2019
CyberSud	Le Forum International de la Cybersécurité et Les Réunions intergouvernementales en cybersécurité, Paris- Lille, France, 22-25 janvier 2019
CyberSud	<a href="#">Atelier régional sur la stratégie de formation judiciaire</a> , Beyrouth, Liban, 23-25 janvier 2019
GLACY+ Cybercrime@Octopus	<a href="#">Introduction à la formation judiciaire des formateurs sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et avocats et adaptation des matériels au contexte local</a> , Abuja, Nigeria, 28 janvier - 01 février 2019
iPROCEEDS	<a href="#">Réunion sur la coopération public-privé pour lutter contre la cybercriminalité et les produits de la criminalité en ligne</a> , Tirana (Albanie), 29 janvier 2019

### Février 2019

GLACY+	Mission consultative et atelier sur la collecte et la surveillance des statistiques de la justice pénale sur la cybercriminalité et la preuve électronique, Rabat, Maroc, 4–6 février 2019
GLACY+	Participation à la mission consultative sur la législation relative à la cybercriminalité dans le cadre du Programme de cybersécurité du Secrétariat du Commonwealth, Nairobi, Kenya, 4-8 février 2019
CyberSud	<a href="#">Formation judiciaire avancée sur la cybercriminalité et les preuves électroniques</a> , Tunis, Tunisie, 4-8 février 2019
Cybercrime@Octopus	Contribuer à la 2 <sup>ème</sup> réunion relative à l'élaboration de la nouvelle stratégie intégrée (cybercriminalité et cybersécurité) pour la Géorgie 2019-2020, Tbilissi, Géorgie, 5-7 février 2019
CyberSud	Appui à la réunion de l'ONU DC « Défis et meilleures pratiques en matière de traitement et d'utilisation des preuves numériques dans les affaires de terrorisme », Vienne, 5-7 février 2019

iPROCEEDS	<a href="#">Cours de formation ECTEG sur l'investigation des réseaux</a> , Bucarest, Roumanie, 11-15 février 2019
Cybercrime@Octopus	Réunion du Groupe de rédaction du Protocole T-CY, Strasbourg, France, 11-13 février 2019
GLACY+ Cybercrime@Octopus	<a href="#">Formation judiciaire préliminaire des formateurs sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et avocats</a> , San Jose (Costa Rica), 11-15 février 2019
GLACY+	Cours ECTEG sur la cybercriminalité et la criminalistique numérique à l'intention des forces de l'ordre, Rabat, Maroc, 11-15 février 2019
CyberSud	<a href="#">Réunion d'information avec les ambassades sur la cybercriminalité et les preuves électroniques</a> , Bucarest (Roumanie), 15 février 2019
CyberSud	<a href="#">ECTEG Live Data Forensics Training</a> , Bucarest, Roumanie, 18-22 février 2019
CyberSud	<a href="#">Intégration du matériel de formation judiciaire au Maroc</a> , Rabat, Maroc, 18-22 février 2019
Cybercrime@Octopus	Participation au 22ème Congrès européen de la police, 19 - 20 février 2019
iPROCEEDS	<a href="#">Deuxième exécution du module de formation d'introduction à la cybercriminalité, aux preuves électroniques et aux produits de la criminalité en ligne</a> , Pristina, Kosovo*, 19-22 février 2019
GLACY+ iPROCEEDS Cybercrime@Octopus	<a href="#">Conférence sur la justice pénale dans le cyberspace</a> , Bucarest (Roumanie), 25-27 février 2019
CyberSud	Appui à la réunion de l'ONU DC sur l'élaboration d'une loi sur la recevabilité des preuves numériques devant les tribunaux du terrorisme, Égypte, 24-28 février 2019
GLACY+	Cours de formation d'instructeurs INTERPOL pour les pays hispanophones et lusophones, Bogota (Colombie), 25 février - 1er mars 2019
GLACY+	Conférence sur la Convention de Budapest pour le programme de Master en cybersécurité, LUISS, Rome, Italie, 28 février 2019
Cybercrime@Octopus	Rédaction du 2 <sup>nd</sup> Protocole additionnel à la Convention de Budapest, février-décembre 2019

### Mars 2019

GLACY+	Réunion de coordination à Europol avec l'PMU du projet SIRIUS pour évaluer les possibilités de coopération GLACY+, La Haye, Pays-Bas, 1er mars 2019
GLACY+	<a href="#">Atelier sur la cybercriminalité et les preuves électroniques pour l'accueil de nouveaux juges</a> , Colombo, Sri Lanka, 2-3 mars 2019
EndOCSEA@Europe	Première réunion du Comité directeur du projet EndOCSEA@Europe, Strasbourg, France, 4 mars 2019
iPROCEEDS	<a href="#">Exercice de simulation de cas sur la cybercriminalité et les enquêtes financières</a> , Tirana, Albanie, 4-7 mars 2019
CyberSud	<a href="#">Cours ECTEG sur les devises en toile noire et les devises cryptographiques</a> , Bucarest, Roumanie, 4-8 mars 2019

GLACY+	Réunion de coordination avec les projets sur la cybercriminalité financés par l'UE (OCWAR-C, GLACY+, Cyber4Dev), Bruxelles, Belgique, 5 mars 2019
GLACY+	Réunion de coordination avec Eurojust pour la préparation d'une conférence internationale conjointe, La Haye, Pays-Bas, 8 mars 2019
iPROCEEDS	<a href="#">Mission d'évaluation sur l'harmonisation de la législation de la Serbie sur la cybercriminalité et les preuves électroniques avec les normes de l'UE et du Conseil de l'Europe</a> , Belgrade, Serbie, 11-12 mars 2019
iPROCEEDS	Troisième présentation du module d'introduction à la formation judiciaire sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne, Podgorica (Monténégro), 11-12 mars 2019
Cybercrime@Octopus	<a href="#">L'Atelier d'information sur la Convention de Budapest sur la Cybercriminalité</a> , Abidjan, Côte d'Ivoire, 12 mars 2019
iPROCEEDS	<a href="#">Réunion sur la mise à jour de la formation ECTEG sur les enquêtes relatives à la toile noire et aux monnaies virtuelles</a> , Bucarest, Roumanie, 11-13 mars 2019
GLACY+	Participation au programme Empact OA 3.6, 11-13 mars 2019
GLACY+	Formation judiciaire avancée des formateurs sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et défenseurs publics, Saint-Domingue, République dominicaine, 11-14 mars 2019
CyberSud	<a href="#">Formation avancée sur la cybercriminalité et les preuves électroniques à l'intention des magistrats</a> , Amman, Jordanie, 17-19 et 20-23 mars 2019
GLACY+	<a href="#">Conférence nationale sur l'application technique de la Convention de Budapest</a> , Accra, Ghana, 18-19 mars 2019
GLACY+	Participation au cours de cybercommandement organisé par la police de Hong Kong, Hong Kong, 18-22 mars 2019
GLACY+ Cybercrime@Octopus	<a href="#">Mission consultative sur l'intégration des modules de formation dans les programmes des institutions de formation judiciaire</a> , Accra, Ghana, 20-22 mars 2019
iPROCEEDS	6ème réunion du Groupe de rédaction du Protocole T-CY (T-CY PDG), Vienne, Autriche, 25-26 mars 2019
CyberSud	<a href="#">Formation des forces de l'ordre dans le domaine des opérations d'infiltration en ligne pour lutter contre la cybercriminalité</a> , Bucarest (Roumanie), 25-29 mars 2019
GLACY+	<a href="#">Législation sur la cybercriminalité et les preuves électroniques en Gambie - Exercice de rédaction</a> , Banjul, Gambie, 25-27 mars 2019
iPROCEEDS	4ème édition du Forum sur la protection des infrastructures critiques, Bucarest, Roumanie, 25-29 mars 2019
CyberSud GLACY+ iPROCEEDS Cybercrime@Octopus	Cinquième réunion du Groupe intergouvernemental d'experts des Nations Unies sur la cybercriminalité (UNIEG), Vienne (Autriche), 27-30 mars 2019
iPROCEEDS	<a href="#">6ème réunion du Comité de pilotage du projet, Bucarest, Roumanie</a> , 29 mars 2019

## Avril 2019

Cybercrime@Octopus	<a href="#">Atelier de sensibilisation sur la Convention de Budapest</a> , Conakry, Guinée, 1-2 avril 2019
CyberSud	ECTEG en ligne, Première intervention, Réunion de cours, Bucarest, Roumanie, 2-4 avril 2019
GLACY+	Mission consultative sur la rationalisation des procédures d'entraide judiciaire en matière de cybercriminalité et de preuves électroniques, Saint-Domingue, République dominicaine, 2-5 avril 2019
iPROCEEDS	<a href="#">Formation de formateurs au module de formation de base sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne à l'intention des juges et procureurs de</a> Macédoine du Nord et de Turquie, Skopje, Macédoine du Nord, 2-6 avril 2019
GLACY+	Réunions des groupes de travail du GFCE 2019, La Haye, Pays-Bas, 3-4 avril 2019
GLACY+	Atelier national sur la protection des données et les outils et services d'INTERPOL, ainsi que sur la mise en place et le renforcement des points de contact 24 heures sur 24 et 7 jours sur 7 pour la cybercriminalité et les preuves électroniques, Manille (Philippines), 3-5 avril 2019
iPROCEEDS	<a href="#">Atelier sur la fraude financière et la fraude par carte de crédit en ligne</a> , Ankara, Turquie, 4 avril 2019
Cybercrime@Octopus	<a href="#">Atelier de sensibilisation sur la Convention de Budapest</a> , Cotonou, Bénin, 4-5 avril 2019
GLACY+	Mission consultative sur l'intégration de la cybercriminalité et des preuves électroniques dans les programmes de formation des établissements de formation judiciaire, Saint-Domingue, République dominicaine, 4-5 avril 2019
EndOCSEA@Europe	Conférence de la société civile : Renforcer la participation de la société civile à la mise en œuvre et au suivi de la Convention de Lanzarote, Strasbourg, France, 8-9 avril 2019
CyberSud	<a href="#">Atelier régional en vue de l'élaboration de rapports nationaux sur l'évaluation des cybermenaces</a> , Rabat, Maroc, 8-10 avril 2019
GLACY+	<a href="#">Cours de formation judiciaire avancée sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et autres magistrats</a> , Santiago du Chili, 8-11 avril 2019
iPROCEEDS	<a href="#">Exercice de simulation de cas sur la cybercriminalité et les enquêtes financières</a> pour la Bosnie-Herzégovine, le Monténégro et la Serbie, Belgrade, Serbie, 8-11 avril 2019
CyberSud	Atelier sur la cybersécurité CEPOL, Beyrouth, Liban, 9-11 avril 2019
GLACY+	<a href="#">Conférence internationale sur la cybercriminalité et les preuves électroniques et 2e réunion du Forum sur la cybercriminalité pour les pays de la CPLP</a> , Praia, Cap-Vert, 11-12 avril 2019

iPROCEEDS	<a href="#">Réflexions juridiques sur les points de contact 24/7 et les demandes de préservation</a> , Istanbul, Turquie, 15-16 avril 2019
iPROCEEDS	<a href="#">Module d'introduction à la formation judiciaire sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne à l'intention des juges et des procureurs</a> (2e partie), Podgorica, Monténégro, 15-16 avril 2019
GLACY+	<a href="#">Participation au Cyber Forum de l'UE</a> , Bruxelles, Belgique, 15-16 avril 2019
CyberSud	Visite d'étude à l'unité spécialisée en cybercriminalité de la Police Nationale Française, Nanterre, France, 15-16 avril 2019
GLACY+	Comité de pilotage du GLACY+, Bruxelles, Belgique, 16 avril 2019
iPROCEEDS	<a href="#">Module d'introduction à la formation judiciaire sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne</a> , Vlasic, Bosnie-Herzégovine, 22-25 avril 2019
GLACY+	4ème réunion du Groupe mondial d'experts INTERPOL sur la cybercriminalité, Lyon (France), 24-26 avril 2019
iPROCEEDS	Soutien la participation à la Conférence internationale sur la criminalistique numérique et les preuves numériques - DataFocus 2019, Zagreb, Croatie, 30 avril 2019
iPROCEEDS	Soutien de la participation au programme de master longue distance à l'UCD (examen d'été), Dublin, Irlande, 30 avril - 2 mai 2019
EndOCSEA@Europe	Recherche documentaire pour la cartographie de référence sur l'OCSEA dans les États membres du Conseil de l'Europe, avril-octobre 2019
EndOCSEA@Europe	Recherche documentaire pour l'examen comparatif des mécanismes internationaux de prévention et de lutte contre l'OCSEA, avril-septembre 2019

### Mai 2019

Cybercrime@Octopus	Conférence Internet et juridiction, Berlin, Allemagne, 3-5 mai 2019
iPROCEEDS	<a href="#">Exercices de simulation de cas sur la cybercriminalité et les enquêtes financières</a> (pour la Macédoine du Nord et la Turquie), Ankara, Turquie, 6-9 mai 2019
Cybercrime@Octopus	Atelier sur la législation relative à la protection des données, Banjul, Gambie, 6-10 mai 2019
GLACY+	<a href="#">Introduction à la formation judiciaire des formateurs sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et avocats et adaptation des matériels au contexte local</a> , Praia, Cap-Vert, 6-10 mai 2019
iPROCEEDS	<a href="#">Exercice sur table sur la coopération internationale dans les affaires de cybercriminalité</a> , Bucarest (Roumanie), 8-9 mai 2019
GLACY+	Cours de formation judiciaire avancée sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et autres magistrats, San Jose (Costa Rica), 13-16 mai 2019
iPROCEEDS	Cours de formation de base sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne à l'intention des juges et des procureurs (1re partie), Tirana (Albanie), 13-14 mai 2019

Cybercrime@Octopus	7 <sup>ème</sup> réunion du Groupe de rédaction du Protocole T-CY, Strasbourg, France, 13-15 mai 2019
GLACY+	<a href="#">Deuxième réunion d'experts sur le Manuel conjoint CdE/FRA sur la cybercriminalité et les droits fondamentaux</a> , Vienne, Autriche, 14-15 mai 2019
iPROCEEDS	<a href="#">Cours de formation de base sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne à l'intention des juges et des procureurs</a> , Ankara (Turquie), 14-17 mai 2019
CyberSud, GLACY+ Cybercrime@Octopus	<a href="#">Free Forensic Tools for the Law Enforcement Community (FREETOOL) - Outils libres pour les enquêtes sur la cybercriminalité et la médecine légale numérique</a> , Bucarest, Roumanie, 15-17 mai 2019
GLACY+	Ateliers nationaux sur la protection des données et les outils et services INTERPOL, ainsi que sur la mise en place et le renforcement des points de contact 24/7 pour la cybercriminalité et les preuves électroniques, Nuku'alofa (Tonga), 15-17 mai 2019
EndOCSEA@Europe	Conférence du Conseil de l'Europe : Coopération multisectorielle pour la prévention et le combat en matière d'exploitation et de maltraitance sexuelle des enfants en ligne, Conférence internationale, Strasbourg, France, 16-17 mai 2019
GLACY+	Mission consultative sur la législation procédurale relative à la cybercriminalité et aux preuves électroniques, San José (Costa Rica) 16-17 mai 2019
GLACY+	Mission consultative et atelier sur les politiques et stratégies en matière de cybercriminalité et de cybersécurité, Manille (Philippines), 20-22 mai 2019
CyberSud	<a href="#">ECTEG Première intervention en ligne, Réunion de cours</a> , Lisbonne, Portugal, 20-24 mai 2019
Cybercrime@Octopus	Groupe Pompidou - Réunion annuelle sur les Drogues en ligne et demande de candidatures du Service de renseignements criminels, Vienne, Autriche, 21-23 mai 2019
GLACY+ Cybercrime@Octopus	Participation au 20 <sup>e</sup> Colloque international sur la lutte contre la cybercriminalité (ISCR 2019), Séoul, Corée, 22-24 mai 2019
GLACY+	Participation à la <a href="#">mission d'évaluation du Modèle de maturité pour la cybersécurité</a> et à la <a href="#">mission consultative sur la législation relative à la cybercriminalité</a> , en coordination avec la Banque mondiale, le FCO britannique et le Secrétariat du Commonwealth, Windhoek, Namibie, 22-24 mai 2019
GLACY+	Mission consultative sur la communication d'informations sur la cybercriminalité et atelier sur la collecte et le suivi des statistiques de la justice pénale sur la cybercriminalité et les preuves électroniques, Manille, Philippines, 23-24 mai 2019

iPROCEEDS	Conférence sur la criminalité à l'ère numérique : Renforcement des capacités des institutions de justice pénale dans l'espace de l'OSCE, Vienne, Autriche, 24 mai 2019
GLACY+ Cybercrime@Octopus	<a href="#">Atelier régional PILON sur la cybercriminalité et les preuves électroniques dans le Pacifique. Coopération internationale pour le partage de preuves électroniques dans la lutte contre la cybercriminalité</a> , Port Vila, Vanuatu, 27-31 mai 2019
GLACY+	Mission consultative sur le signalement de la cybercriminalité et atelier sur la collecte et le suivi des statistiques de la justice pénale sur la cybercriminalité et les preuves électroniques, Port Louis (Maurice), 28-29 mai 2019
iPROCEEDS	Soutenir la participation à la Conférence sur l'ISS World Europe - Systèmes de soutien au renseignement pour la surveillance électronique, la surveillance des médias sociaux/réseaux noirs et les enquêtes sur la cybercriminalité, Prague, République tchèque, 28-30 mai 2019
GLACY+	Atelier sur l'élaboration d'enquêtes sur la cybercriminalité ; Atelier national et conseils sur la coopération interinstitutionnelle et la collaboration public-privé dans la lutte contre la cybercriminalité, Saint-Domingue, République dominicaine, 28-30 mai 2019

#### Juin 2019

CyberSud	<a href="#">Réunion de formation du CEPOL sur les preuves électroniques - Contribution du Conseil de l'Europe</a> , Budapest, Hongrie, 3-6 juin 2019
GLACY+	<a href="#">Formation régionale de formateurs pour les premiers intervenants sur la cybercriminalité et les preuves électroniques pour les gendarmeries africaines</a> , Dakar, Sénégal, 3-7 juin 2019
GLACY+	Enquêtes sur les cryptogrammes Formation à l'intention des cyber-unités de police, Santo Domingo, République dominicaine, 3-7 juin 2019
CyberSud	<a href="#">Adaptation du matériel de formation judiciaire au cours de formation judiciaire tunisien</a> , Tunis, Tunisie, 10-14 juin 2019
Cybercrime@Octopus	Le 8 <sup>ème</sup> Sommet annuel sur les droits de l'homme à l'ère numérique, Tunis, Tunisie, 11-14 juin 2019
CyberSud	<a href="#">Atelier régional Euromed sur la police et la justice pour les points de contact euro-méditerranéens sur la cybercriminalité et les preuves numériques</a> , Bucarest, Roumanie, 12-14 juin 2019
iPROCEEDS	Cours de formation de base sur la cybercriminalité, les preuves électroniques et les produits de la criminalité en ligne à l'intention des juges et des procureurs (2e partie), Tirana (Albanie), 12-13 juin 2019
GLACY+	<a href="#">Conférence régionale sur les stratégies et politiques en matière de cybercriminalité et caractéristiques de la Convention de Budapest pour la Communauté des Caraïbes</a> , Saint-Domingue, République dominicaine, 12-14 juin 2019
CyberSud	<a href="#">Formation judiciaire d'intégration sur la cybercriminalité et les preuves électroniques</a> , Alger, Algérie, 16-20 juin 2019
CyberSud	<a href="#">Cours pilote ECTEG Cours d'enquêteurs en ligne (OSINT)</a> , Tunis, Tunisie, 17-21 juin 2019

GLACY+	Participation à l'événement de lancement du cours en ligne HELP sur la protection des données, Bucarest, Roumanie, 18-19 juin 2019
EndOCSEA@Europe	Analyse des lacunes dans la législation, les politiques et les pratiques du OCSEA en Azerbaïdjan, Bakou, Azerbaïdjan, 18-21 juin 2019
Cybercrime@Octopus	Atelier sur la législation relative à la cybercriminalité et aux preuves électroniques, Doha (Qatar), 18-28 juin 2019
Cybercrime@Octopus	Dialogue européen sur la gouvernance de l'Internet, La Haye, Pays-Bas, 19-20 juin 2019
GLACY+	Participation à la conférence ICANN 65 - Policy Meeting, Marrakech, Maroc, 24-27 juin 2019
CyberSud	<a href="#">Formation à l'analyse des logiciels malveillants</a> , Tunis, Tunisie, 24-28 juin 2019
GLACY+	<a href="#">Conférence internationale sur la protection des données pour la région africaine</a> , Accra, Ghana, 24-27 juin 2019
GLACY+	<a href="#">Deuxième réunion annuelle et conférence internationale du Réseau ibéro-américain de cyber-procureurs</a> , Santiago, Chili, 25-26 juin 2019
GLACY+ iPROCEEDS	<a href="#">Atelier international conjoint pour les unités d'enquête sur la cybercriminalité et les Autorités centrales des parlementaires</a> , Singapour, 25-27 juin 2019
iPROCEEDS	<a href="#">Quatrième colloque annuel sur la sensibilisation à la cybersécurité organisé par le Groupe de travail antiphishing</a> , Bucarest, Roumanie, 26 - 27 juin 2019

### Juillet 2019

GLACY+	<a href="#">Mission consultative et atelier sur la législation au FOPREL</a> , San Salvador, El Salvador, 1-2 juillet 2019
GLACY+, CyberSud CyberEast iPROCEEDS Cybercrime@Octopus	21e session plénière T-CY et 4e session plénière de rédaction du Protocole, Strasbourg, France, 8-11 juillet 2019
GLACY+	Visite d'étude de juges sri-lankais en Belgique et atelier sur la cybercriminalité et les preuves électroniques, Bruxelles, Belgique, 8 juillet 2019
CyberSud	<a href="#">CyberSud Troisième comité directeur</a> , Strasbourg, France, 9 juillet 2019
GLACY+ CyberSud CyberEast iPROCEEDS	<a href="#">Conférence internationale des formateurs judiciaires nationaux sur la cybercriminalité et les preuves électroniques</a> , Strasbourg, France, 10-12 juillet 2019
CyberSud	<a href="#">12ème réunion du Groupe de travail du Moyen-Orient et de l'Afrique du Nord sur la cybercriminalité pour les chefs d'unités en coopération avec Interpol</a> , Amman, Jordanie, 16-17 juillet 2019
GLACY+	Mise en place d'un groupe d'enquête sur la cybercriminalité et d'un groupe de criminalistique des données, Abuja, Nigéria 16-19 juillet 2019

GLACY+	Participation au camp d'été sur la cybersécurité 2019, Leon, Espagne, 16-27 juillet
CyberSud	Atelier ECTEG pour les formateurs en criminalistique numérique, Budapest, Hongrie, 22-26 juillet 2019
GLACY+	Mise en place d'un groupe d'enquête sur la cybercriminalité et d'un groupe de criminalistique des données, Praia, Cap-Vert, 22-25 juillet 2019
EndOCSEA@Europe	Recherche documentaire pour l'analyse des lacunes concernant la législation, les politiques et les procédures relatives à l'OCSEA en Arménie, juillet-septembre 2019
EndOCSEA@Europe	Recherche documentaire pour l'analyse des lacunes concernant la législation, les politiques et les procédures relatives à l'OCSEA en Azerbaïdjan, juillet-septembre 2019
EndOCSEA@Europe	Recherche documentaire pour l'analyse des lacunes concernant la législation, la politique et les procédures relatives à l'OCSEA en Ukraine, juillet-septembre 2019
EndOCSEA@Europe	Subventions à la société civile pour sensibiliser le public à l'OCSEA par la participation des enfants et le développement d'outils, juillet 2019 - juillet 2020
EndOCSEA@Europe	Consultations d'enfants pour élaborer une version adaptée aux enfants de la Convention de Lanzarote, juillet-octobre 2019

#### Août 2019

GLACY+	<a href="#">Réunion de suivi avec le FOPREL et réunions bilatérales avec les autorités mexicaines en vue de l'adoption/révision de la législation et de l'adhésion à la Convention de Budapest</a> , Mexico, Mexique, 19-21 août 2019
GLACY+	Formation initiale des formateurs sur la cybercriminalité et les preuves électroniques à l'intention des magistrats et des procureurs, Port-Louis (Maurice), 19-23 août 2019
GLACY+	Réunion préparatoire avec Eurojust pour la conférence conjointe, 23 août 2019

#### Septembre 2019

GLACY+	Formation INTERPOL à l'analyse des logiciels malveillants (Manille (Philippines), 2-6 septembre 2019)
CyberSud CyberEast iPROCEEDS GLACY+	<a href="#">2019 Conférence sur l'économie souterraine</a> , Strasbourg, France, 3-6 septembre 2019

CyberEast	Évaluation de la structure institutionnelle des pays du partenariat oriental, de leurs capacités, de leurs compétences, de leurs besoins de formation ainsi que des lacunes et des possibilités de coopération interinstitutionnelle, Kiev, Ukraine, 3-5 septembre 2019
CyberEast	Évaluation de la structure institutionnelle des pays du partenariat oriental, de leurs capacités, de leurs compétences, de leurs besoins de formation ainsi que des lacunes et des possibilités de coopération interinstitutionnelle, Erevan, Arménie, 9-10 septembre 2019
CyberEast	Évaluation de la structure institutionnelle des pays du partenariat oriental, de leurs capacités, de leurs compétences, de leurs besoins de formation ainsi que des lacunes et des possibilités de coopération interinstitutionnelle, Bakou, Azerbaïdjan, 12-13 septembre 2019
CyberSud	Participation au Congrès des Dialogues sur la cybersécurité et présentation d'un exposé sur le rôle du Conseil de l'Europe dans le cyberspace, Sibiu, Roumanie 12-13 septembre 2019
CyberSud	<a href="#">Adaptation du matériel de formation judiciaire</a> , Amman, Jordanie, 15-19 septembre 2019
Cybercrime@Octopus	8ème réunion du Groupe de rédaction du Protocole, Paris, France, 16-18 septembre 2019
CyberEast	Évaluation de la structure institutionnelle des pays du partenariat oriental, de leurs capacités, de leurs compétences, de leurs besoins de formation ainsi que des lacunes et des possibilités de coopération interinstitutionnelle, Tbilissi (Géorgie), 16-17 septembre 2019
EndOCSEA@Europe	Visite d'information et atelier d'analyse des lacunes concernant la législation, la politique et les procédures relatives à l'OCSEA, Erevan, Arménie, 16-20 septembre 2019
EndOCSEA@Europe	Visite d'information et atelier d'analyse des lacunes concernant la législation, la politique et les procédures relatives au BCAEE, Kiev, Ukraine, 17-19 septembre 2019
iPROCEEDS	<a href="#">Formation régionale sur les enquêtes d'infiltration en ligne en coopération avec SELEC</a> , Bucarest, Roumanie, 17-20 septembre 2019
CyberEast	Événement de lancement du projet CyberEast, Bruxelles, Belgique, 19-20 septembre 2019
CyberSud	<a href="#">Réunion sur la législation</a> , Amman, Jordanie, 23 septembre 2019
GLACY+	Mission consultative sur l'intégration des modules de formation dans les programmes des établissements de formation judiciaire et des établissements de formation des procureurs, San José (Costa Rica), 23-24 septembre 2019
GLACY+ Cybercrime@Octopus	Conférence régionale africaine sur la cybercriminalité, la cybersécurité nationale et la piraterie sur Internet, Lagos, Nigeria, 23-27 septembre 2019
CyberEast	Soutien à l'Université d'été du PAE sur la gouvernance de l'Internet, Tbilissi, Géorgie, 23-27 septembre 2019
CyberSud	<a href="#">Atelier régional sur les stratégies de formation des services de détection et de répression</a> , Amman, Jordanie, 24-25 septembre 2019

CyberEast	Évaluation de la structure institutionnelle des pays du partenariat oriental, de leurs capacités, de leurs compétences, de leurs besoins de formation ainsi que des lacunes et des possibilités de coopération interinstitutionnelle, Minsk, Bélarus, 24-25 septembre 2019
Cybercrime@Octopus	Accueil d'un panel sur la cybercriminalité et la législation en matière de protection des données en Afrique à FIFAfrica 2019, en collaboration avec l'Unité de protection des données du Conseil de l'Europe, Addis Abeba, Ethiopie, 25-26 septembre 2019
GLACY+	Intégration des matériels de formation ECTEG dans les académies de formation des services de détection et de répression et autres organismes professionnels de formation des services de détection et de répression, Nuku'alofa, Tonga, 25-27 septembre 2019
iPROCEEDS	Forum sur les services fiduciaires - Journée de l'AC, Berlin, Allemagne, 25-26 septembre 2019
GLACY+ CyberEast iPROCEEDS EndOCSEA@Europe	<a href="#">Conférence internationale conjointe Eurojust/COE sur les enquêtes sur Internet : Dark web and online child abuse</a> , La Haye, Pays-Bas, 30 septembre - 1er octobre 2019
EndOCSEA@Europe	Recherche documentaire visant à analyser les stratégies et le matériel de formation du Bureau de la coordination des affaires humanitaires en Arménie, en Azerbaïdjan, en République de Moldova et en Ukraine, septembre-décembre 2019
EndOCSEA@Europe	Conférence annuelle de l'ENOC - Sensibilisation des médiateurs pour enfants, Belfast, Irlande, septembre 2019