COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 24 novembre 2017

Documents d'information
SG/Inf(2017)42

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

Rapport d'activité du C-PROC pour la période d'octobre 2016 à septembre 2017

Table des matières

Résumé
1 Cadre et objet du présent rapport 5
2 Mandat du Bureau 7
3 Projets et résultats pour la période d'octobre 2016 à septembre 2017 7
3.1 Aperçu des projets en cours 8
3.2 Cybercrime@Octopus 9
3.3 Cybercrime@EAP II – Coopération internationale 10
3.4 Cybercrime@EAP III – Coopération public/privé 11
3.5 Projet relatif à l'Action globale sur la cybercriminalité (GLACY) 13
3.6 Projet élargi GLACY+ : Action globale sur la cybercriminalité 15
3.7 Projet iPROCEEDS : Cibler les bénéfices de la criminalité exercée sur internet 16
3.8 Projet CyberSouth sur la cybercriminalité et la preuve électronique dans la région du voisinage du Sud 18
4 Priorités de financement supplémentaires 19
5 Relations avec le Comité de la Convention Cybercriminalité (T-CY) 19
6 Relations avec le gouvernement roumain 20
7 Aspects administratifs et budgétaires 21
7.1. Locaux 21
7.2. Personnel 21
7.3. Aspects budgétaires 22
8 Visibilité 22
9 Conclusions 23
10 Annexe : Inventaire des activités soutenues par le Bureau des Programmes de Bucarest (C-PROC) (octobre 2016 – septembre 2017) 25

Résumé

Le présent rapport a pour objet de tenir le Comité des Ministres informé des activités du Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) à Bucarest, Roumanie, pour la période allant d'octobre 2016 à septembre 2017[1].

Face à la nécessité de renforcer les capacités en matière de lutte contre la cybercriminalité dans le monde entier, le Comité des Ministres a décidé le 9 octobre 2013 (lors de sa 1180e réunion), que le Conseil de l'Europe établirait un Bureau de programme sur la cybercriminalité à Bucarest. Opérationnel depuis le 7 avril 2014, le Bureau met en œuvre toutes les activités de renforcement des capacités en matière de lutte contre la cybercriminalité. Il est financé par des ressources extrabudgétaires.

Entre octobre 2016 et septembre 2017, le Bureau a soutenu quelque 175 activités dans le cadre de sept projets déployés dans les régions prioritaires d'Europe ainsi que dans des pays d'autres régions du monde qui se sont engagés à mettre en œuvre la Convention de Budapest.

En septembre 2017, les projets en cours mis en œuvre par le Bureau représentaient un budget de plus de 24 millions d'euros. Le Bureau compte une équipe de 21 collaborateurs (en provenance de dix États membres différents). Le Bureau est dirigé par le chef de la Division de la cybercriminalité (DG1), qui partage son temps entre Strasbourg et Bucarest. Depuis juillet 2017, il bénéficie du soutien d'un Chef des Opérations.

Tous les membres du personnel – excepté le Chef du Bureau – sont financés sur le budget des projets dont ils sont responsables, et tous les coûts de fonctionnement du Bureau sont couverts par les budgets alloués aux projets.

Le C-PROC est installé dans la Maison des Nations Unies à Bucarest, dans des locaux mis gracieusement à sa disposition par le gouvernement roumain, et rénovés en 2017.

L'expérience de l'année passée confirme que le Bureau répond aux attentes qui ont justifié sa création :

- le Conseil de l'Europe demeure un acteur mondial de premier plan en termes de renforcement des capacités de lutte contre la cybercriminalité et de collecte de preuves électroniques.

[1] Pour la période allant d'avril 2014 à septembre 2015 se reporter au document https://rm.coe.int/168047d1b8
Pour la période allant d'octobre 2015 à septembre 2016 se reporter au document https://rm.coe.int/16806b8a87

- La pertinence et l'impact du Bureau tiennent non seulement au volume des projets et activités mais également aux synergies fortes entre la Convention de Budapest et d'autres normes pertinentes, aux activités de suivi et d'évaluation menées par le Comité de la Convention sur la cybercriminalité et à la consolidation des capacités par le C-PROC.

- Le Bureau mène, avec efficacité et à moindre coût, un grand nombre d'activités. Les conditions sont réunies pour qu'il puisse s'agrandir davantage, absorber et gérer des ressources supplémentaires.

- Le Bureau est attractif pour les donateurs. Il a démarré en avril 2014 avec des projets pour environ 4 millions EUR. En septembre 2016, l'enveloppe était passée à 22 millions EUR et en septembre 2017 à plus de 24 millions EUR. La plus grande partie des fonds provient de Projets Joints avec l'Union Européenne.

- Les autorités compétentes du gouvernement roumain, mais aussi d'autres États parties à la Convention de Budapest (à l'heure actuelle, l'Estonie, la France, l'Allemagne, le Royaume-Uni et les États-Unis), ainsi que le Centre européen de lutte contre la cybercriminalité d'EUROPOL et INTERPOL sont partenaires des projets du C-PROC qu'ils enrichissent de leurs compétences.

Grâce aux projets actuellement en cours, le C-PROC a une base solide pour produire un impact sur les deux ou trois prochaines années. Un financement supplémentaire serait néanmoins nécessaire, en particulier pour des projets dans la région du Partenariat oriental, pour soutenir le Comité de la Convention sur la cybercriminalité, ou pour soutenir la mise en œuvre du Protocole sur la xénophobie et le racisme et pour la protection des enfants contre la violence en ligne.

1 Cadre et objet du présent rapport

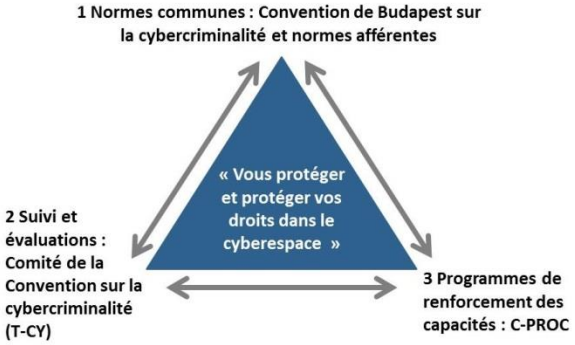
Le présent rapport a pour objet de tenir le Comité des Ministres du Conseil de l'Europe informé des activités menées par le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) à Bucarest, Roumanie, pour la période allant d'octobre 2016 à septembre 2017.

La cybercriminalité – autrement dit les infractions commises contre des systèmes informatiques ou au moyen de ces systèmes – constitue désormais une menace grave pour les droits fondamentaux, la démocratie et l'État de droit ainsi que pour la paix et la stabilité internationales. Parallèlement, la question de la preuve électronique a pris une nouvelle dimension et a gagné en complexité.

Aujourd'hui, toute infraction – qu'il s'agisse de fraude ou d'attaques visant les médias, les parlements ou les infrastructures publiques, de maltraitance infantile ou d'autres formes d'exploitation sexuelle, de vol de données à caractère personnel, de racisme et de xénophobie, de blanchiment de capitaux ou de terrorisme – est susceptible d'être liée à la cybercriminalité ou à la preuve électronique.

Pour relever ces défis, le Conseil de l'Europe a développé une approche fondée sur un triangle de trois éléments interdépendants :

- La Convention de Budapest sur la cybercriminalité (STE n° 185) qui a été ouverte à la signature en 2001[2] reste, quinze ans plus tard, l'accord international le plus pertinent en la matière. En septembre 2017, 56 États sont Parties à cette Convention et 14 autres l'ont signée ou ont été invités à y adhérer.



- Le Comité de la Convention Cybercriminalité (T-CY) procède à des évaluations de la mise en œuvre de la Convention par les Parties, adopte des notes d'orientation et établit des groupes de travail chargés d'apporter des réponses aux nouveaux défis qui se posent. Le T-CY, qui compte actuellement 71 États membres et observateurs[3] et onze organisations observatrices, semble être devenu le principal organe intergouvernemental intervenant dans le domaine de la cybercriminalité au niveau international.

[2] Complétée 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 n°189) de 2003.
[3] 56 Parties, 14 signataires ou États invités à adhérer ainsi que la Fédération de Russie.

- Le renforcement des capacités en matière de lutte contre la cybercriminalité est une composante essentielle de l'approche du Conseil de l'Europe depuis 2006, année de lancement de la première phase du projet global sur la cybercriminalité. Il est largement admis au sein de la communauté internationale que le renforcement des capacités est un moyen efficace d'aider les sociétés à relever les défis que posent la cybercriminalité et les preuves électroniques.

La décision du Comité des Ministres en octobre 2013[4], à la suite d'une offre du Gouvernement de la Roumanie et d'une proposition du Secrétaire Général (SG/Inf(2013)29), d'établir un Bureau des Programmes à Bucarest, Roumanie, répondait au besoin du Conseil de l'Europe de renforcer ses propres capacités pour soutenir la création de capacités dans le monde entier.

Le Bureau est devenu opérationnel le 7 avril 2014 à la suite de l'entrée en vigueur d'un protocole d'accord signé entre le Conseil de l'Europe et le ministère roumain des Affaires étrangères.

Cette décision a été prise dans la perspective :

- qu'un Bureau spécialisé permettrait au Conseil de l'Europe de répondre de manière visible et crédible aux besoins accrus des pays du monde entier en matière de renforcement des capacités dans la lutte contre la cybercriminalité ;

- qu'un Bureau de programme mettant en œuvre des projets de manière efficace et à moindre coût favoriserait la levée de fonds ;

- que les activités de renforcement des capacités menées par le Bureau viendraient compléter les activités intergouvernementales du Comité de la Convention Cybercriminalité (T-CY), qui serait toujours géré depuis Strasbourg ;

- que le Bureau serait financé par des ressources extrabudgétaires.

Après 42 mois d'activité, le Bureau confirme qu'il est à la hauteur de ces attentes.

[4] Le 9 octobre 2013 à leur 1180e réunion.

2 Mandat du Bureau[5]

Le Bureau a pour mission d'assurer la mise en œuvre des projets du Conseil de l'Europe visant au renforcement des capacités en matière de lutte contre la cybercriminalité, dans le monde entier.

Cela passe notamment par :

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

Le Secrétariat du Comité de la Convention Cybercriminalité (T-CY) – c'est-à-dire le volet intergouvernemental des travaux du Conseil de l'Europe dans le domaine de la cybercriminalité – reste à Strasbourg.

3 Projets et résultats pour la période d'octobre 2016 à septembre 2017

Le C-PROC a pour mission d'aider des pays dans le monde entier à renforcer les capacités de leur système de justice pénale en matière de lutte contre la cybercriminalité et de collecte de preuves électroniques, sur la base de la Convention de Budapest sur la cybercriminalité et des normes y afférentes[6]. Le Bureau s'acquitte de sa mission à travers la mise en œuvre de projets de renforcement des capacités.

[5] SG/Inf(2013)29 et protocole d'accord signé le 15 octobre 2013 entre le Conseil de l'Europe et le gouvernement roumain.

[6] Comme 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 n°189), la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201), la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n° 198), et d'autres.

3.1 Aperçu des projets en cours

Pour la période allant d'octobre 2016 à septembre 2017, le C-PROC a apporté son soutien à quelque 175 activités[7] au titre des projets suivants :

Intitulé du projet	Durée	Budget	Financement
Cybercrime@Octopus	jan 2014 – déc 2019	3,5 millions d'euros	Contributions volontaires (Estonie, Hongrie, Monaco, Roumanie, Royaume-Uni, Slovaquie, Japon, États-Unis d'Amérique et Microsoft)
Cybercrime@EAP II sur la coopération internationale dans les pays du Partenariat oriental	mai 2015 – déc 2017	800 000 euros CdE 10%	projet conjoint UE/CdE (Partenariat pour une bonne gouvernance)
Cybercrime@EAP III sur la coopération public/privé dans les pays du Partenariat oriental	déc 2015 – déc 2017	1,2 millions d'euros CdE 10%	projet conjoint UE/CdE (Partenariat pour une bonne gouvernance)
Projet GLACY relatif à l'Action globale sur la cybercriminalité	nov 2013 – oct 2016	3,35 millions d'euros CdE 10%	projet conjoint UE/CdE
GLACY+ projet élargi Action globale sur la cybercriminalité	mars 2016 – fév 2020	10 millions d'euros CdE 10%	projet conjoint UE/CdE
Projet iPROCEEDS : cibler les produits de la criminalité exercée sur internet en Europe du Sud-Est et en Turquie	jan 2016 – juin 2019	5,56 millions d'euros CdE 10%	projet conjoint UE/CdE
Projet CyberSud sur la coopération en matière de lutte contre la cybercriminalité dans la région du Voisinage Sud	juil 2017 – juin 2020	3,33 millions d'euros CdE 10%	projet conjoint UE/CdE

En septembre 2017, les projets mis en œuvre par le C-PROC représentaient un budget cumulé d'environ 24,4 millions d'euros.

7 Voir l'annexe pour la liste des activités.

Ceci représente une augmentation significative par rapport à septembre 2015 (6 millions EUR), le budget restant à la hausse par rapport à septembre 2016 (22 millions EUR).

Comme prévu dans le mandat du Bureau, le C-PROC a identifié, conçu, négocié et mobilise le financement pour tous ces projets.

3.2 Cybercrime@Octopus

Cybercrime@Octopus est un projet financé par des contributions volontaires. Il vise à apporter une aide concrète aux pays nécessitant un soutien, s'agissant notamment de l'élaboration d'une législation.

Dans le cadre de ce projet, le Bureau a par exemple apporté son soutien à une visite d'évaluation au Kazakhstan (juin 2017), à une réunion sur la cybercriminalité en Inde (août 2017) ou encore à un examen documentaire du projet de loi libanais sur la cybercriminalité (mai 2017). En septembre 2017, le projet a organisé une réunion à EUROPOL (La Haye) du réseau de points de contact 24/7 établi au titre de l'article 35 de la Convention de Budapest.

Le projet permet des partenariats avec d'autres organisations. En coopération avec l'Organisation des États américains, un atelier a été réalisé à Buenos Aires en juin 2017 pour renforcer le travail en réseau des procureurs des pays latino-américains spécialisés dans la cybercriminalité et en septembre 2017, le projet a apporté son soutien à un Forum de l'OEA sur la cybersécurité, organisé en Uruguay. En septembre 2017, le projet a soutenu la conférence annuelle EUROPOL/INTERPOL sur la cybercriminalité à La Haye.

Cybercrime@Octopus facilite aussi la conception de nouveaux projets. Par exemple, un atelier organisé en mars 2017 à Bucarest pour des experts d'Algérie, de Jordanie, du Liban, du Maroc et de la Tunisie a débouché sur le nouveau projet CyberSud, qui a ensuite démarré en juillet 2017.

Les Conférences Octopus sont également organisées par le biais de ce projet. Ainsi, du 16 au 18 novembre 2016, la Conférence Octopus sur la coopération contre la cybercriminalité a été organisée à Strasbourg, en conjonction avec le 15e anniversaire de la Convention de Budapest sur la cybercriminalité. La prochaine Conférence Octopus est prévue du 11 au 13 juillet 2018.

Le projet Cybercrime@Octopus étant conçu pour soutenir le travail du Comité de la Convention sur la cybercriminalité (T-CY), il a financé des visites du T-CY à Panama en décembre 2016 et en Argentine, au Chili et au Costa-Rica en mars 2017. Dans le sillage desdites visites, le Chili et le Costa-Rica ont adhéré à la Convention, la loi d'adhésion à la Convention a été soumise au Parlement argentin

et un nouveau projet de loi sur la cybercriminalité a été soumis au Parlement du Panama.

Le projet a en outre financé la participation d'États observateurs aux réunions plénières du T-CY, et – grâce à une contribution financière des États-Unis – l'interprétation vers et depuis l'espagnol pour faciliter la participation des pays latino-américains au T-CY. Les agents du C-PROC apportent en outre un soutien logistique aux réunions plénières du T-CY selon les besoins.

Cela témoigne des liens étroits qui existent entre la Convention de Budapest, le T-CY et le C-PROC.

Cybercrime@Octopus représente une ressource à laquelle des donateurs peuvent contribuer pour lutter contre la cybercriminalité et soutenir le T-CY à tout moment sans que cela entraîne des périodes très longues de conception et d'adoption de projets.

D'une manière générale, Cybercrime@Octopus constitue un outil flexible visant à répondre aux besoins, à renforcer la législation, à promouvoir les partenariats multipartites et à soutenir concrètement l'action du T-CY. Le projet a donc été prolongé jusqu'à décembre 2019 avec un budget augmenté[8].

3.3 Cybercrime@EAP II – Coopération internationale

Cybercrime@EAP II, avec un budget de 800 000 EUR et une durée de vie allant de mai 2015 à décembre 2017, entend renforcer les capacités de pays du Partenariat oriental (Arménie, Azerbaïdjan, Belarus, Géorgie, République de Moldova et Ukraine) dans le domaine de la coopération judiciaire et policière internationale sur la cybercriminalité et la preuve électronique.

Il assure le suivi direct des recommandations relatives à l'entraide judiciaire (MLA) adoptées par le Comité de la Convention sur la cybercriminalité (T-CY) en décembre 2014.

Capitalisant sur les résultats obtenus durant la première année de sa mise en œuvre, entre octobre 2016 et septembre 2017, le projet a poursuivi la consolidation de capacités ciblée dans les pays du Partenariat oriental en vue d'améliorer les compétences des autorités ainsi que les règles et procédures pour la coopération international.

La participation d'équipes par pays à des évènements internationaux tels que les sessions plénières du Comité de la Convention sur la cybercriminalité (T-CY) et la Conférence Octopus, les réunions du Groupe Pompidou et des groupes d'experts

[8] Il lui reste à être pleinement financé.

des Nations Unies sur la cybercriminalité, des formations et des réunions internationales organisées par EUROPOL/INTERPOL, ainsi que d'autres manifestations régionales et internationales, ont donné l'occasion de partager des bonnes pratiques sur le plan international. Des activités dans les pays ont visé les lacunes dans les cadres réglementaires et législatifs, l'organisation institutionnelle et les capacités et compétences nécessaires pour garantir une coopération internationale effective concernant la cybercriminalité et la preuve électronique.

D'importants progrès ont été réalisés :

- un programme de formation à la coopération internationale et à la coopération avec des fournisseurs de services multinationaux a été développé et dispensé dans tous les pays du Partenariat oriental. Un jeu complet de supports pédagogiques, élaboré pour ces formations spécialisées, est disponible pour de futures initiatives de consolidation des capacités ;

- des modèles de demandes standardisées d'entraide judiciaire (article 31 de Convention de Budapest) et de conservation de données (articles 29/30 de la Convention) ont été élaborés et des ressources en ligne sur la coopération internationale dans la Communauté Octopus ont été préparées et testées dans cette région ;

- des réformes du droit procédural ont été soutenues par le projet dans cinq pays du Partenariat oriental, étant donné que des lacunes dans le droit procédural interne font obstacle à la coopération internationale en matière de cybercriminalité et de preuve électronique.

De plus, un rapport détaillé sur « Cybercriminalité : stratégies, compétences procédurales et institutions spécialisées dans la région du Partenariat oriental – État des lieux » ("Cybercrime strategies, procedural powers et specialised institutions in the Eastern Partnership region – state of play") a été préparé et présenté au Panel sur l'État de droit dans les pays du Partenariat oriental, en juin 2017 à Bruxelles. Le rapport identifie les priorités pour les années à venir, concernant le renforcement des capacités dans cette région.

3.4 Cybercrime@EAP III – Coopération public/privé

Le projet Cybercrime@EAP III, lancé en 2016 et qui s'achèvera en décembre 2017, vise à promouvoir la coopération entre les autorités de justice pénale dans les pays du Partenariat oriental et les fournisseurs de services.

Ce projet est le premier du genre et l'expérience acquise en 2016 a mis en évidence la complexité de la question.

Au vu des progrès réalisés, le budget du projet a été augmenté, passant de 700 000 EUR à 1,2 million EUR, ce qui lui a permis de répondre à des défis communs au niveau régional et de traiter des besoins spécifiques aux pays par le biais d'activités nationales.

Une grande partie des travaux menés entre octobre 2016 et septembre 2017 a été consacrée à bâtir la confiance en tant que préalable à une coopération public/privé, en réunissant les différents acteurs et en promouvant le dialogue, y compris avec des fournisseurs de services multinationaux. Des efforts ont été déployés pour soutenir la conclusion ou l'actualisation d'accords de coopération en Arménie, Géorgie, République de Moldova et Ukraine.

De plus, un important travail a été mené dans le cadre de ce projet sur des réformes en matière de procédure pénale, dans la mesure où la clarification du droit applicable contribue à instaurer de la confiance avec les entreprises privées et constitue donc un préalable important à la coopération public/privé. Des ateliers et des auditions ont été organisés pour ce faire en Arménie, Azerbaïdjan, Géorgie et Ukraine. Des observations écrites sur des projets de loi ont été soumises aux autorités de ces pays. En République de Moldova, le projet a coopéré avec la Commission de Venise, ce qui a abouti à un Avis sur des propositions de changements à des lois en décembre 2016 et à un atelier de suivi en septembre 2017.

Le renforcement du droit interne a également été discuté avec le Belarus, afin d'encourager une réforme du droit procédural conformément à la Convention de Budapest et aux exigences de l'état de droit.

Gardant à l'esprit la nature régionale du projet, des activités internationales et régionales sur le thème des partenariats public-privé ont été utilisées comme plateformes de discussion pour les grandes problématiques d'une coopération de ce type.

En participant au premier Exercice jamais organisé sur la coordination et le partenariat en matière de cybercriminalité, au Dialogue européen 2017 sur la gouvernance de l'Internet et à la Réunion régionale du projet consacré aux sauvegardes et garanties et à la coopération avec les fournisseurs de services sur Internet, les pays sont en mesure d'échanger, entre eux et avec des partenaires internationaux, sur les meilleures pratiques et leur expérience.

Grâce au projet, les pays du Partenariat oriental sont engagés dans un dialogue permanent avec des fournisseurs nationaux de services sur Internet et d'autres acteurs nationaux importants pour améliorer la coopération entre les pouvoirs publics et le secteur de l'Internet en termes d'accès aux données, tandis que la participation de ces pays aux discussions internationales sur la coopération avec

des fournisseurs de services mondiaux leur permet de rendre leur coopération avec ces sociétés plus efficiente en matière d'investigations criminelles.

3.5 Projet relatif à l'Action globale sur la cybercriminalité (GLACY)

GLACY est un projet conjoint du Conseil de l'Europe et de l'Union européenne, d'une portée mondiale, qui a démarré en novembre 2013 et s'est achevé le 31 octobre 2016, par une conférence de clôture à Bucarest.

Les pays prioritaires étaient l'Ile Maurice, le Maroc, les Philippines, le Sénégal, l'Afrique du Sud, le Sri Lanka et le Tonga, puisque ces pays s'étaient engagés à adhérer à la Convention de Budapest sur la cybercriminalité.

La France, la Roumanie, la Turquie et le Centre européen sur la cybercriminalité à EUROPOL étaient partenaires du projet.

GLACY a donné les résultats suivants :

- L'Ile Maurice, le Sri Lanka et le Tonga sont devenus Parties à la Convention de Budapest sur la cybercriminalité. GLACY a en outre permis de susciter de l'intérêt pour la Convention dans d'autres pays, dont certains ont entre-temps été invités à adhérer à la Convention (le Cap Vert, le Ghana et le Nigéria).

- Les sept pays prioritaires se sont désormais tous dotés de lois, ou ont soumis des projets de lois à leur parlement, pour mettre leur droit pénal en matière de cybercriminalité et de preuve électronique en conformité avec les normes internationales, c'est-à-dire la Convention de Budapest.

- Des modules sur la cybercriminalité et la preuve électronique ont été intégrés aux programmes des établissements de formation judiciaires. Du matériel pédagogique a été élaboré et adapté, et des cours-pilotes (modules d'introduction ou avancés) ont été dispensés à plus de 900 juges et procureurs, avec l'effet démultiplicateur de la méthodologie consistant à former des formateurs.

- Les unités de lutte contre la cybercriminalité dans les pays prioritaires ont été renforcées par la formation (par exemple, des cours ont été dispensés pour les premiers intervenants et sur l'analyse à chaud de données informatiques à des fins d'enquête), par l'accès à du matériel pédagogique (par exemple, les manuels élaborés par l'ECTEG – *European Cybercrime Training and Education Group*), ainsi que par l'accès à des outils (par exemple la version mise à jour d'un Manuel sur la preuve électronique et un guide sur les Procédures opératoires standard). Les outils et matériels sont également disponibles au niveau de la Communauté Octopus.

Quelque 600 agents ont participé à des activités de formation, y compris la formation de formateurs.

- Les sept pays prioritaires sont maintenant mieux à même de coopérer au niveau international en ce qui concerne la cybercriminalité et la preuve électronique. Par exemple, leurs unités de lutte contre la cybercriminalité, leurs services de poursuite et leurs points de contact 24/7 ont été mises en relation avec leurs homologues dans d'autres juridictions ainsi qu'avec EUROPOL et INTERPOL. Ceci a facilité la coopération internationale sur des affaires concrètes.

- Les gouvernements ont amélioré leur capacité à évaluer les progrès réalisés en matière d'enquête, de poursuite et de jugement d'affaires de cybercriminalité et autres infractions impliquant les preuves électroniques, même s'il reste encore des difficultés pour l'obtention de statistiques de justice pénale fiables en matière de cybercriminalité et de preuve électronique. GLACY a contribué à cette amélioration en commençant par effectuer des analyses de la situation puis en dressant l'état des lieux des progrès.

- Le fait que les décideurs ont été impliqués a joué un rôle capital dans la réussite du projet GLACY, et cet élément demeurera essentiel pour la prévention et le contrôle de la cybercriminalité. Il a été tenu compte des progrès réalisés (« progress review ») dans le processus d'élaboration des politiques et les représentants des pays prioritaires ont adopté une « Déclaration sur les priorités stratégiques pour la coopération concernant la cybercriminalité et la preuve électronique » à l'occasion de la Conférence de clôture du GLACY (octobre 2016). Ces « Priorités stratégiques » peuvent servir de structure-modèle pour tout pays souhaitant se doter de politiques globales en matière de cybercriminalité et de preuve électronique.

Les pays prioritaires du projet GLACY sont à présent membres actifs ou observateurs du Comité de la Convention sur la cybercriminalité.

Le projet GLACY est un autre exemple illustrant le fonctionnement du « triangle dynamique » de la Convention de Budapest, du T-CY et du renforcement de capacités par le C-PROC.

Il a renforcé la crédibilité de la position du Conseil de l'Europe et de l'Union européenne selon laquelle la consolidation de capacités est l'une des voies les plus efficaces pour traiter le problème de la cybercriminalité au niveau international.

A la réunion du Groupe d'experts intergouvernemental des Nations-Unies sur la cybercriminalité (Vienne, avril 2017), le GLACY a été présenté comme un exemple de bonne pratique pour le renforcement de capacités.

3.6 Projet élargi GLACY+ : Action globale sur la cybercriminalité

Forts de l'expérience du projet GLACY, le Conseil de l'Europe et l'Union européenne ont convenu de le prolonger à travers le projet élargi GLACY+ « Action globale sur la cybercriminalité ».

Le projet bénéficie d'un budget de 10 millions d'euros. Il a démarré en mars 2016 et se poursuivra jusqu'en février 2020. La conférence de lancement a été organisée à Bucarest en octobre 2016 juste après la conférence de clôture du GLACY.

GLACY+ s'articule autour de trois axes :

1. Promouvoir des politiques et des stratégies cohérentes en matière de cybercriminalité et de cybersécurité. Cela suppose le renforcement de la coopération avec d'autres organisations internationales et régionales.

2. Renforcer la capacité des forces de police d'enquêter sur les affaires de cybercriminalité et de mettre en place une véritable coopération de police à police, ainsi qu'avec les unités spécialisées en cybercriminalité en Europe et dans d'autres régions du monde.

3. Permettre aux autorités judiciaires pénales d'appliquer la législation, d'engager des poursuites et de statuer sur des affaires de cybercriminalité et de coopérer à l'échelon international.

INTERPOL – en vertu d'un accord avec le Conseil de l'Europe – est un partenaire et le chef de file pour la mise en œuvre du volet du projet concernant l'application de la loi. Au nombre des autres partenaires figurent l'Estonie (ministère de la Justice), la France (ministère de l'Intérieur), la Roumanie (Police nationale, Parquet (DIICOT) et ministère de la Justice), Royaume-Uni (National Crime Agency) et États-Unis d'Amérique (Department of Justice), ainsi qu'EUROPOL (Centre européen sur la cybercriminalité).

Dans le cadre de GLACY+, la plupart des pays prioritaires du projet GLACY servent désormais de pôles, partageant leurs expériences dans leurs régions respectives[9]. D'autres pays prioritaires désireux d'adhérer à la Convention de Budapest se sont ajoutés (comme le Ghana, le Cap Vert et le Nigéria). Contrairement à GLACY, ce projet apporte également un soutien aux pays latino-américains. La République

[9] Le soutien à l'Afrique du Sud a été suspend à la suite de communications par les autorités d'Afrique du Sud.

dominicaine étant déjà partie à la Convention de Budapest, elle sera le premier pays prioritaire et le premier pôle de cette région.

Outre les pays prioritaires, tout pays peut bénéficier d'un soutien pour le renforcement de sa législation. Ainsi, entre février et juin 2017, Panama et le Guatemala ont bénéficié d'une assistance pour la rédaction de leurs lois contre la cybercriminalité.

GLACY+ est également un outil permettant d'entamer une coopération avec d'autres organisations. Ainsi, en juillet 2017, le gouvernement de l'Ile Maurice, l'Organisation internationale des procureurs et GLACY+ ont co-organisé la Conférence régionale d'Afrique de l'Est sur la cybercriminalité et la preuve électronique pour 12 pays de cette région.

Depuis le lancement de GLACY+, un accord a été conclu entre le Conseil de l'Europe et la (Communauté économique des États de l'Afrique de l'Ouest). Aux termes de cet accord, les deux organisations (respectivement par le biais de GLACY+ et d'autres projets, et de la Commission de la CEDEAO) soutiendront les pays d'Afrique du Sud dans l'amélioration de leur législation. Un atelier commun pour les États membres de la CEDEAO s'est ainsi tenu en septembre 2017. Un accord similaire est actuellement en discussion avec la Commission de l'Union africaine.

Au vu des progrès accomplis depuis le lancement de GLACY+, des discussions sont désormais en cours entre le Conseil de l'Europe et la Commission européenne pour accroître encore le budget du projet et en étendre la durée.

3.7 Projet iPROCEEDS : Cibler les bénéfices de la criminalité exercée sur Internet

Le projet iPROCEEDS est déployé en Albanie, en Bosnie-Herzégovine, au Monténégro, en Serbie, dans « l'ex-République yougoslave de Macédoine », en Turquie et au Kosovo*. Il a vocation à aider les autorités des pays de la région à renforcer leurs capacités en matière de recherche, de saisie et de confiscation des recettes issues de la criminalité en ligne et de prévention du blanchiment de capitaux sur Internet.

Doté d'un budget de 5,56 millions d'euros, le projet a démarré en janvier 2016 et prendra fin en juin 2019.

Il comporte les volets suivants :

* Toute référence au Kosovo mentionnée dans ce texte, que ce soit le territoire, les institutions ou la population, doit se comprendre en pleine conformité avec la Résolution 1244 du Conseil de sécurité des Nations Unies et sans préjuger du statut du Kosovo.

- mise en place de mécanismes publics de signalement ;
- législation ;
- coopération entre les unités cybercriminalité, les structures d'enquête financière et les cellules de renseignements financiers ;
- mécanismes de partage d'information public / privé ;
- formation du personnel judiciaire ;
- coopération internationale.

Le projet iPROCEEDS suit les recommandations de l'étude typologique élaborée en 2012 par Moneyval et le projet global sur la cybercriminalité.

Après de premières visites d'évaluation dans tous les secteurs du projet, au printemps 2016, et la conférence de lancement organisée en juin 2016 en « ex-République yougoslave de Macédoine », des progrès ont été enregistrés dans tous les volets du projet, comme le montrent ces exemples :

- des missions de conseil ont été menées dans tous les secteurs concernant l'établissement ou l'amélioration des mécanismes de reporting ;
- des programmes de formation judiciaire ont été revus et des matériels pédagogiques mis à jour de façon à intégrer des cours sur la cybercriminalité, la preuve électronique et les enquêtes financières en ligne, dans les établissements de formation et pour la formation de formateurs ;
- des réunions ont été organisées avec des fournisseurs de services multinationaux pour améliorer la coopération avec les services répressifs ;
- la coopération a été renforcée entre services et au niveau international pour ce qui est du dépistage, de la saisie et de la confiscation des produits de crimes en ligne ;
- des formations ont été montées sur le darknet et les enquêtes concernant les monnaies virtuelles ;
- des agents des forces répressives de tous les secteurs du projet ont participé au programme de master à distance de l'UCD (University College Dublin) sur les enquêtes en matière de cybercriminalité et l'utilisation de données informatiques aux fins d'enquête ;

- des lignes directrices ont été élaborées pour la prévention et la détection des produits du crime en ligne.

iPROCEEDS est là encore un outil permettant une coopération avec de nombreuses organisations telles qu'EUROPOL, le CEPOL (l'Agence de l'Union européenne chargée de la formation de la police), l'Office des Nations Unies contre la drogue et le crime mais aussi avec des organisations du secteur privé, telles que des associations de banques et des fournisseurs de services sur Internet.

Les supports pédagogiques développés par iPROCEEDS seront également utiles dans d'autres projets.

3.8 Projet CyberSouth sur la cybercriminalité et la preuve électronique dans la région du voisinage du Sud

Le projet conjoint du Conseil de l'Europe et de l'Union européenne CyberSouth couvre la région du voisinage du Sud et comptait comme pays prioritaires initiaux l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie. Il complète et fait partie intégrante de la politique de coopération de l'Organisation avec ses régions voisines.

D'une durée de 36 mois (juillet 2017-juin 2020), le projet dispose d'un budget de 3,33 millions EUR. Il a pour objectif de renforcer la législation et les capacités institutionnelles en matière de lutte contre la cybercriminalité et de preuve électronique dans la région du voisinage Sud, en conformité avec les exigences liées aux Droits de l'Homme et à l'État de droit.

Le projet se focalisera sur la législation relative à la cybercriminalité, les services de police spécialisés et la coopération interservices, la formation judiciaire, les points de contact 24/7 et la coopération internationale, ainsi que les politiques de lutte contre la cybercriminalité.

La phase de démarrage, de juillet 2017 à janvier 2018, servira à faire une évaluation détaillée de la législation et des capacités des institutions, ainsi qu'à constituer des équipes de projets nationales par pays.

La conférence de lancement du projet est prévue pour janvier 2018.

Le Maroc a été invité à adhérer à la Convention de Budapest et a bénéficié d'activités de consolidation de capacités (comme GLACY et GLACY+) depuis un certain temps. CyberSouth devrait assurer que d'autres pays du voisinage du Sud se joignent aux principaux efforts internationaux en matière de cybercriminalité.

4 Priorités de financement supplémentaires

Grâce aux projets en cours, C-PROC dispose d'une base solide et des ressources nécessaires pour produire un impact sur les deux à trois prochaines années. Parmi les autres priorités pour des projets et un financement, on citera :

- un soutien permanent et accru à la région du partenariat oriental étant donné que les projets en cours dans le cadre de Cybercrime@EAP s'achèvent au 31 décembre 2017 ;

- des contributions volontaires additionnelles en faveur du projet Cybercrime@Octopus, afin de soutenir les travaux du Comité de la Convention sur la cybercriminalité ;

- extension du budget et de la durée de GLACY+ pour répondre à l'augmentation des demandes d'assistance ;

- un 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 ;

- un nouveau projet sur la protection des enfants contre la violence sexuelle en ligne, sur la base des Conventions de Budapest et de Lanzarote.

5 Relations avec le Comité de la Convention Cybercriminalité (T-CY)

Des agents basés à Strasbourg assurent le fonctionnement du secrétariat du T-CY tandis que le C-PROC gère l'ensemble des activités de renforcement des capacités. Le C-PROC entretient des liens étroits avec le T-CY, le secrétaire exécutif de ce dernier étant également le chef du C-PROC et partageant son temps entre Strasbourg et Bucarest.

Les douze derniers mois ont confirmé ce qui avait été constaté depuis avril 2014, à savoir l'existence de synergies fortes. Les travaux du T-CY alimentent directement les activités de renforcement des capacités, et réciproquement.

Les projets portés par le C-PROC s'inscrivent dans le prolongement des résultats du T-CY. De nombreux membres du T-CY mettent leurs compétences à disposition en intervenant à titre de formateurs ou de conférenciers dans le cadre des activités de renforcement de capacités.

Le Bureau apporte à son tour un soutien au T-CY : la participation au T-CY d'experts supplémentaires venus d'États parties et observateurs est en effet financée et organisée dans le cadre des projets menés par le C-PROC.

Entre octobre 2016 et septembre 2017, plusieurs activités du T-CY ont par ailleurs été financées par le budget du projet Cybercrime@Octopus, à l'instar des visites en Argentine, au Chili, au Costa Rica et au Panama. Lors des plénières du T-CY de novembre 2016 et de mai 2017, l'interprétation en espagnol a pu être assurée grâce à la contribution des États-Unis au titre du projet Cybercrime@Octopus.

Par ailleurs, la maintenance du site web du T-CY et d'autres ressources en ligne est assurée par des agents rémunérés au titre du projet Cybercrime@Octopus.

6 Relations avec le gouvernement roumain

Suite à la signature du protocole d'accord en octobre 2013 :

- la loi portant ratification de ce protocole d'accord a fait l'objet d'une procédure accélérée et a été publiée au Journal officiel début avril 2014. Le cabinet du Vice-Premier ministre et le ministère de la Justice sont intervenus pour aider à régler les questions relatives aux locaux et aux aspects juridiques et administratifs ;

- des locaux au sein de la Maison des Nations Unies, emplacement de choix à Bucarest, ont été mis à disposition du Conseil de l'Europe. En 2015, des espaces de bureaux supplémentaires ont été aménagés pour permettre au Bureau de s'agrandir en prévision du lancement de nouveaux projets. En décembre 2016, un accord supplémentaire a été signé entre le Conseil de l'Europe et le ministère roumain des Affaires étrangères sur les modalités d'utilisation de la Maison des Nations Unies par le C-PROC. A l'été 2017, le gouvernement de la Roumanie y a entrepris d'importants de rénovation. Des agents de sécurité sont mis à disposition par le gouvernement roumain.

Le ministère de la Justice, la Direction des enquêtes liées au crime organisé et au terrorisme du Bureau du procureur de la Haute Cour de cassation (DIICOT), la police nationale roumaine, l'école nationale de la magistrature et l'équipe d'intervention en cas d'urgence informatique (CERT-RO) s'emploient à développer une coopération étroite avec le Bureau sur les questions de fond et mettent leurs compétences au service des activités du projet.

Le Bureau est régulièrement invité à participer et à intervenir lors des réunions nationales, régionales et internationales sur la cybercriminalité, la cybersécurité, la criminalité organisée et d'autres questions connexes qui se tiennent en Roumanie.

7 Aspects administratifs et budgétaires

7.1. Locaux

Les locaux sont mis gracieusement à disposition par le gouvernement roumain (voir ci-dessus, point 6).

7.2. Personnel

Entre octobre 2016 et septembre 2017, l'équipe est passée de 18 à 21 personnes. En septembre 2015, le C-PROC comptait six employés.

Comme l'avait proposé le Secrétaire Général, le Bureau est dirigé par le Secrétaire exécutif du Comité de la Convention Cybercriminalité (le Chef de la Division Cybercriminalité) qui se partage entre Strasbourg et Bucarest. Ce mode de fonctionnement permet de maintenir des liens étroits entre les activités du T-CY et celles du C-PROC (voir ci-dessus, point 5).

Compte tenu de l'augmentation des effectifs et des ressources, un chef des opérations (avec les fonctions de gestionnaire du centre de coût) a été recruté et a commencé sa mission le 1er juillet 2017. Le poste est financé par les frais généraux générés dans le cadre des projets mis en œuvre par le C-PROC.

En septembre 2017, le Bureau comptait un chef des opérations recruté au niveau international (grade A2), cinq chefs de projet recrutés au niveau international (grade A1/2) et 14 agents recrutés localement (six chargés de projet de grade B4/5, deux assistants financiers de grade B3 et quatre assistants de projet de grade B2).

Les agents sont originaires de dix États membres différents. Ils sont rémunérés à partir des budgets des projets et se consacrent exclusivement à la mise en œuvre des projets.

Cinq postes supplémentaires étaient à pourvoir et le processus de recrutement était en cours. Deux ou trois positions supplémentaires devraient être pourvues dans les prochains mois, ce qui porterait le total des équipes à 29, soit la capacité maximum d'accueil du Bureau.

7.3. Aspects budgétaires

Tous les coûts du C-PROC, hormis le salaire du Chef du Bureau, sont couverts par des ressources extrabudgétaires :

- les locaux sont mis gracieusement à disposition par le gouvernement roumain ;

- la rémunération de tous les agents – à l'exception de celle du Chef du Bureau – est assurée par les budgets des projets dont ils ont la responsabilité;

- les achats de mobilier et de matériel informatique ont dans un premier temps été financés par une contribution volontaire du Royaume-Uni et le sont désormais par les budgets affectés aux projets respectifs ;

- les frais de fonctionnement du Bureau sont directement couverts par les lignes budgétaires des projets consacrées aux frais généraux et aux coûts de fonctionnement éligibles au niveau local.

Comme prévu, la mise en œuvre des projets de renforcement de capacités depuis Bucarest se révèle plus rentable et présente un ratio plus favorable entre dépenses opérationnelles et dépenses administratives et de personnel. Entre avril 2014 et septembre 2017, près de 1 500 000 euros d'économies ont pu être réalisées au niveau des dépenses de personnel et 700 000 euros au niveau des frais de fonctionnement.

Le financement de projets mis en œuvre par le C-PROC s'avère donc attractif pour les donateurs.

8 Visibilité

Le C-PROC permet d'accroître la visibilité du Conseil de l'Europe en matière de cybercriminalité notamment à travers le site web (www.coe.int/cybercriminalité), en contribuant à la communauté Octopus et à ses outils, en diffusant deux fois par mois un "abstract" des affaires de cybercriminalité et en publiant une lettre d'information trimestrielle Cybercrime@COE Update.

9 Conclusions

- L'action du Bureau des Programmes du Conseil de l'Europe sur la cybercriminalité est dédiée à la consolidation des capacités, dont il est communément admis au niveau international qu'elle est un moyen efficace d'aider les sociétés partout dans le monde à s'attaquer au phénomène de la cybercriminalité. Ce consensus a été réaffirmé lors de la réunion du Groupe d'experts intergouvernementaux des Nations-Unies sur la cybercriminalité (Vienne, avril 2017) ; à cette occasion, le projet conjoint du Conseil de l'Europe et de l'Union Européenne sur une action globale contre la cybercriminalité (Global Action on Cybercrime - GLACY) a été salué comme un exemple de bonne pratique. Grâce au Bureau, le Conseil de l'Europe demeure une référence mondiale pour ce qui est de la consolidation des capacités en matière de cybercriminalité et pour les preuves électroniques.

- La Convention de Budapest (complétée par des instruments connexes sur la protection des données, la protection des enfants, le terrorisme ou le blanchiment de capitaux) est la norme de référence pour les projets du C-PROC, qui contribuent à assurer un impact sur le terrain et renforcent la crédibilité de ce traité dans toutes les régions du monde. Entre octobre 2016 et septembre 2017 – outre Andorre, la Grèce et Monaco – le Chili, le Costa-Rica et le Tonga sont devenues Parties à la Convention de Budapest, et le Cap Vert et le Nigéria ont été invités à y adhérer.

- Les projets de consolidation des capacités facilitent la participation de représentants de la plupart des 70 États Parties et Observateurs (les signataires et les États invités à adhérer) aux travaux du Comité de la Convention sur la cybercriminalité (T-CY), ce qui permet d'adopter une approche inclusive pour les travaux de rédaction d'un Protocole additionnel à la Convention de Budapest, qui ont débuté en septembre 2017.[10]

- Ces projets contribuent en outre à assurer le suivi des recommandations du T-CY. Cela démontre l'efficacité d'un triangle dynamique combinant des normes communes (la Convention de Budapest), un suivi grâce au T-CY et une consolidation des capacités grâce au C-PROC. Les synergies entre les travaux intergouvernementaux du T-CY et les activités de consolidation des capacités ont été significativement renforcées depuis la création du Bureau.

- Le portefeuille du projet couvre des régions prioritaires en Europe (région du Partenariat oriental, Europe du Sud-Est et Turquie) ainsi que des pays

[10] En plus des États membres du CdE, l'Australie, le Canada, le Chili, le Japon, l'Ile Maurice, le Sénégal, le Sri Lanka, le Tonga et les États-Unis ont participé à la première réunion du Groupe de rédaction du protocole, en septembre 2017.

dans d'autres régions du monde qui se sont engagés à mettre en œuvre la Convention de Budapest.

- Le C-PROC mène un grand nombre d'activités, qui produisent un impact de façon efficace et économique. Cela rend le Bureau attractif pour les donateurs. En septembre 2017, les projets en cours représentaient plus de 24 millions EUR ; ils sont mis en œuvre par une équipe de 21 personnes, dont un Chef des Opérations nouvellement nommés, au C-PROC. 6 à 8 personnes supplémentaires seront recrutées dans les prochains moins du fait de l'expansion des projets.

- L'Union européenne demeure le principal donateur. Entre octobre 2016 et septembre 2017 des contributions volontaires ont également été reçues de l'Estonie, de la Hongrie, de Monaco, de la Slovaquie, du Japon et des États-Unis d'Amérique pour le projet Cybercrime@Octopus.

- Le gouvernement roumain met gracieusement les locaux à disposition du Bureau, et lui fournit en outre de l'expertise. Le ministère de la Justice, la Direction des enquêtes liées au crime organisé et au terrorisme du Bureau du procureur de la Haute Cour de cassation (DIICOT), la police nationale roumaine, l'école nationale de la magistrature et l'équipe d'intervention en cas d'urgence informatique (CERT-RO) s'emploient à développer une coopération étroite avec le Bureau, sont partenaires des projets ou s'investissent dans les activités des projets.

- Plusieurs autres États (Estonie, France, Allemagne, Royaume-Uni et États-Unis d'Amérique), ainsi que le Centre européen de lutte contre la cybercriminalité d'EUROPOL et INTERPOL, sont également partenaires d'un ou de plusieurs projets. De nombreuses activités de projets sont menées en partenariat avec une large palette d'organisations du secteur public comme privé, ou en association avec elles.

Le Bureau répond par conséquent aux attentes ayant justifié sa création. Il est proposé qu'il continue de fonctionner selon les modalités actuelles.

10 Annexe : Inventaire des activités soutenues par le Bureau des Programmes de Bucarest (C-PROC) (octobre 2016 – septembre 2017)

octobre 2016

iPROCEEDS	Mission de conseil et atelier sur la fraude en ligne et d'autres mécanismes de signalement de cybercriminalité, Podgorica/Danilovgrad, Monténégro, 3-4 octobre 2016
GLACY, GLACY+	Réunion pour faire le point des progrès accomplis et rapports d'étape sur le projet GLACY et mission d'évaluation initiale pour le projet GLACY+, Maroc, 3-6 octobre 2016
GLACY+, Cybercrime@Octopus	Formation INTERPOL aux investigations dans les affaires de cybercriminalité pour des enquêteurs de pays africains, Abuja, Nigéria, 3 - 7 octobre 2016
CyberCrime@EAP III	Coopération public-privé : Atelier sur la cybercriminalité et le cadre de signalement d'incidents, y compris les CERT nationaux, Chisinau, Moldova, 6-7 octobre 2016
GLACY+	Atelier avec les Chefs des Unités anti-cybercriminalité de pays africains, Abuja, Nigéria, 10 - 11 octobre 2016
GLACY+	Mission d'évaluation initiale pour les objectifs du projet, Accra, Ghana, 10-13 octobre 2016.
iPROCEEDS	Atelier régional pour passer en revue la situation des programmes de formation judiciaire sur la cybercriminalité, la preuve électronique et les produits du crime en ligne, Zagreb, Croatie, 11-12 octobre 2016
CyberCrime@EAP III	Coopération public-privé : Atelier sur la coopération entre les services répressifs et FSI, portant sur la préservation, Bakou, Azerbaïdjan, 12-14 octobre 2016
GLACY+	Participation à l'évènement sur la preuve électronique et la coopération internationale, en marge du COP UNTOC, Vienne, Autriche, 18 octobre 2016
iPROCEEDS	Participation à la formation pilote EMPACT au CEPOL et collaboration avec l'ECTEG sur le Darknet et les monnaies virtuelles, Budapest, Hongrie, 19-21 octobre 2016
CyberCrime@EAP II	Atelier sur la preuve électronique, Chisinau, Moldova, 20-21 octobre 2016
iPROCEEDS / CyberCrime@EAP III	Réunion internationale sur la coopération avec les fournisseurs de services internet multinationaux, Dublin, Irlande, 24-25 octobre 2016
GLACY, GLACY+	International Closing Conference to discuss the results of the GLACY project, present the results of the statistics study et their impact on cybercrime policy, adopt the Declaration on Strategic Priorities, also combined avec launching event for the GLACY+ project, Bucarest, 26-28 octobre 2016

novembre 2016

CyberCrime@EAP III	CyberCrime@EAP III: Évaluation des amendements législatifs moldaves sur la cybercriminalité et la preuve électronique soutenues par les experts du Conseil de l'Europe, Chisinau, Moldova, 2-3 novembre 2016
CyberCrime@EAP III	EAP III: Rapport sur l'Ukraine concernant la coopération public-privé en matière de cybercriminalité, Kyiv, Ukraine, 4 novembre 2016

CyberCrime@EAP III	CyberCrime@EAP III: L'Arménie bénéficiera d'un aperçu des meilleures pratiques sur la coopération public-privé dans la lutte contre la cybercriminalité, Erevan, Arménie, 7-8 novembre 2016
CyberCrime@EAP III	CyberCrime@EAP III: Efforts de réglementation de la coopération public-privé en Géorgie et événement international sur la cybersécurité soutenu par le Conseil de l'Europe, Tbilissi, Géorgie, 9-10 novembre 2016
GLACY+ CyberCrime@EAP II CyberCrime@EAP III iPROCEEDS Cybercrime@Octopus	Réunions plénières du T-CY Strasbourg, France, 14-15 novembre 2016
GLACY+ CyberCrime@EAP II CyberCrime@EAP III iPROCEEDS Cybercrime@Octopus	Coopération contre la cybercriminalité, Strasbourg, France, 16-18 novembre 2016
CyberCrime@EAP II	Atelier sur la coopération de l'EU en matière de cybercriminalité et de preuve électronique, Kyiv, Ukraine, 21-22 novembre 2016
GLACY+	Visite d'étude par les services répressifs marocains à l'équipe PHAROS de la Police nationale française, Paris, France, 24 novembre 2016
iPROCEEDS	iPROCEEDS: Atelier régional sur les mécanismes de signalement: bonnes pratiques internationales, Tirana, Albanie, 25 novembre 2016
GLACY+	Participation au 2e Forum anti-cybercriminalité – Combattre la fraude numérique et le piratage dans les secteurs bancaires et commerciaux au Liban, Beyrouth, 29 novembre 2016
iPROCEEDS	Réunion des organisations partenaires de la mise en œuvre pour la Gouvernance de la sécurité intérieure intégrée dans les Balkans de l'Ouest, Vienne, Autriche, 30 novembre 2016

décembre 2016

GLACY+	Participation à la Master Class sur les cyber-menaces UNICRI, Turin, Italie, 1-2 décembre 2016
Cybercrime@Octopus	Le Conseil de l'Europe à l'édition 2016 du Forum sur la gouvernance de l'Internet, Jalisco, Mexique, 6-9 décembre 2016
CyberCrime@EAP II	Participation à la 4e Réunion annuelle du groupe de travail sur la cybercriminalité du Groupe Pompidou, Strasbourg, France, 6 – 8 décembre 2016.
iPROCEEDS	Workshop on interagency and international cooperation for search, seizure et confiscation of online crime proceeds[4], Pristina, Kosovo*, 8-9 décembre 2016
Cybercrime@Octopus	séminaire sur "Internet, droit et procès", Paris, France, 9 décembre 2016
iPROCEEDS	Regional workshop on Money Laundering risks related to new technologies et 2nd Steering Committee, Bucarest, 12-13 décembre 2016
iPROCEEDS	Workshop on interagency and international cooperation for search, seizure and confiscation of online crime proceeds, Skopje, "ex-République yougoslave de Macédoine", 15-16 décembre 2016
iPROCEEDS	Appel d'offres - 2016AO60 programme de maîtrise à longue distance sur l'investigation de la cybercriminalité, juillet – décembre 2016

janvier 2017

GLACY+	GLACY+: Développement des politiques de cybersécurité et de cybercriminalité au Sénégal Dakar, Sénégal 16-17 janvier 2017
iPROCEEDS	Workshop on online financial fraud and credit card fraud, Belgrade, Serbie, 16-17 janvier 2017
GLACY+	GLACY+: Ghana avance sa stratégie nationale de cybersécurité, Accra, Ghana, 19-20 janvier 2017
iPROCEEDS	iPROCEEDS: 14 policiers commencent le programme de maîtrise à distance sur l'investigation de la cybercriminalité et l'informatique légale - University College Dublin, Irlande, 23 janvier 2017
CyberCrime@EAP III	Développement du cyber-exercice en tant que travail préparatoire pour l'exercice de coordination et de partenariat, Tbilissi, Géorgie, 23-25 janvier 2017
GLACY+	ICANN Atelier de renforcement des capacités pour les forces de l'ordre africaines, Nairobi, Kenya, 25-26 janvier 2017
CyberCrime@EAP II	Soutien au développement et à l'intégration de la formation judiciaire sur la cybercriminalité et la preuve électronique, Tbilissi, Géorgie, 26-27 janvier 2017

février 2017

GLACY+	Support meetings et activities carried out by regional et international organizations, La Haye, Pays-Bas, 3 février 2017
CyberCrime@EAP III	seminar on communication and information sharing with local Internet service providers, Kyiv, Ukraine, 8-9 février 2017
CyberCrime@EAP III	Atelier sur des amendements législatifs liés à la cybercriminalité et à la preuve électronique, Kyiv, Ukraine, 9-10 février 2017
GLACY+	Mission de conseil sur des textes législatifs liés à la cybercriminalité et à la preuve électronique, Guatemala City, Guatemala - 13-15 février 2017
CyberCrime@EAP II	Workshop on reform of legislation to ensure compliance with Articles 16 et 17 of the Budapest Convention on Cybercrime, Bakou, Azerbaïdjan, 13-15 février 2017
CyberCrime@EAP III	Passage en revue du train de mesures d'amendement législatif concernant la cybercriminalité et la preuve électronique et Table ronde sur la réforme des textes législatifs et réglementaires sur la cybercriminalité, Tbilissi, Géorgie, 16-17 février 2017
iPROCEEDS	Workshops on inter-agency and international cooperation for search, seizure et confiscation of online crime proceeds, Sarajevo, Bosnie-Herzégovine, 16-17 février 2017
iPROCEEDS	Mission de conseil et atelier sur la fraude en ligne et d'autres mécanismes de signalement de cybercriminalité, Skopje, "ex-République yougoslave de Macédoine", 20-21 février 2017
CyberCrime@EAP III, iPROCEEDS	Development of the cyberexercise as a preparatory work for the Coordination and partnership exercise, Tbilissi, Géorgie, 23-24 février 2017
GLACY+, CyberCrime@EAP II	Workshop on strengthening the 24/7 points of contact for cybercrime and electronic evidence organized in cooperation with another EU/CoE project GLACY+, as well as Interpol, Singapour, 27 février – 1 mars 2017
iPROCEEDS	Pilot training on Investigation on Darknet and Virtual Currencies, Bucarest, Roumanie, 28 février – 3 mars 2017

mars 2017

GLACY+	Accord de subvention avec INTERPOL pour la mise en œuvre des activités de l'Objectif 2 – Capacités des services répressifs, 1er mars 2017 – 29 février 2020
Cybercrime@Octopus	Atelier d'évaluation et de planification pour un soutien supplémentaire à la consolidation des capacités de pays de la région méditerranéenne, Bucarest, Roumanie, 6-7 mars 2017
CyberCrime@EAP II	Training Programme on International Cooperation, including multinational ISPs, for the Eastern Partnership region, Erevan, Arménie, 6 – 9 mars 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Tirana, Albanie, 13 mars 2017
CyberCrime@EAP II	Programme de formation à la coopération international, incluant des FSI multinationaux, pour la région du Partenariat oriental, Bakou, Azerbaïdjan, 13 – 16 mars 2017
GLACY+	GLACY+ devient régional: Première formation régionale des formateurs sur la cybercriminalité et la preuve électronique pour les pays d'Afrique de l'Ouest, Dakar, Sénégal, 14-17 mars 2017
GLACY+	Development of cybercrime investigations, digital forensics capabilities, Colombo, Sri Lanka, 14-17 mars 2017
iPROCEEDS	Workshops on inter-agency and international cooperation, Tirana, Albanie, 15-16 mars 2017
iPROCEEDS	Mission de conseil et atelier sur la fraude en ligne et autres mécanismes de signalement en matière de cybercriminalité, Ankara, Turquie, 15-16 mars 2017
Cybercrime@Octopus	Visite du T-CY au Costa Rica (Costa Rica, Chili, Argentine), 16-24 mars 2017
GLACY+	Visite d'étude de la délégation des Philippines au CERT de l'Ile Maurice, Port-Louis, Ile Maurice, 23-24 mars 2017
CyberCrime@EAP III	Atelier sur les partenariats public-privé selon une approche spécifique par secteur, Minsk, Belarus, 23-24 mars 2017
iPROCEEDS	Mission de conseil et atelier sur la fraude en ligne et autres mécanismes de signalement en matière de cybercriminalités, Sarajevo, Bosnie-Herzégovine, 27-28 mars 2017
CyberCrime@EAP II	Programme de formation à la coopération international, incluant des FSI multinationaux, pour la région du Partenariat oriental, Tbilissi, Géorgie, 27 – 30 mars 2017
GLACY+	International workshop on criminal justice statistics on cybercrime et electronic evidence, Accra, Ghana, 29-31 mars 2017
GLACY+	Mission de conseil sur la législation relative à la cybercriminalité et à la preuve électronique, Panama, Panama, 30-31 mars 2017
GLACY+	Residential training on cybercrime and electronic evidence for Prosecutors, Panadura, Sri Lanka, 31 mars – 2 avril 2017
Cybercrime@Octopus	Soutien apporté au Bureau du T-CY (1) dans la finalisation du projet de rapport T-CY(2017)2 sur les suites données par les Parties au rapport TCY(2013)17rev sur l'entraide judiciaire et (2) pour la préparation d'une étude de cartographie du TCY concernant le cyber-harcèlement et d'autres formes de violence en ligne, mars – décembre 2017

avril 2017

GLACY+	Introductory Cybercrime and Electronic Evidence Training of Trainers

	Course, Accra, Ghana, 3-7 avril 2017
CyberCrime@EAP II	Programme de formation à la coopération international, incluant des FSI multinationaux, pour la région du Partenariat oriental, Chisinau, Moldova, 3-6 avril 2017
iPROCEEDS	Workshop on inter-agency cooperation et on international cooperation for search, seizure et confiscation of online crime proceeds, Ankara, Turquie, 3-4 avril 2017
GLACY+	Participation à la 3e Réunion du Groupe de travail Amériques d'INTERPOL sur la cybercriminalité pour les Chefs d'unités, Bridgetown, La Barbade, 5-7 avril 2017
CyberCrime@EAP III	Atelier sur la réforme de la loi relative à la cybercriminalité, Kyiv, Ukraine, 6-7 avril 2017
iPROCEEDS	Meeting on Public-private cooperation for fighting cybercrime and online crime proceeds, Belgrade, Serbie, 10 avril 2017
GLACY+, CyberCrime@EAP II iPROCEEDS	3e réunion du Groupe d'experts intergouvernementaux des Nations-Unies sur la cybercriminalité, Vienne, Autriche, 10 – 13 avril 2017
CyberCrime@EAP II	Programme de formation à la coopération internationale, incluant des FSI multinationaux, pour la région du Partenariat oriental, Kyiv, Ukraine, 10-13 avril 2017
iPROCEEDS	Workshop on inter-agency cooperation and on international cooperation for search, seizure et confiscation of online crime proceeds, Belgrade, Serbie, 19-20 avril 2017
CyberCrime@EAP III iPROCEEDS	Coordination and Partnership Cyber Exercise, Géorgie, Tbilissi, 24-28 avril 2017
GLACY+	Formation à l'analyse des maliciels, organisée par INTERPOL, Manille, Philippines, 24-28 avril 2017
GLACY+	Training of trainers and development of training materials for basic et advanced modules for each country, Saint-Domingue, République dominicaine 24-28 avril 2017

mai 2017

CyberCrime@EAP III	Développement de l'Étude sur la stratégie de communication avec les fournisseurs de services multinationaux, mai – juin 2017
GLACY+	Réunion de bilan de la formation sur le darkweb et les monnaies virtuelles, EUROPOL, La Haye, 2-5 mai 2017
CyberCrime@EAP II	Programme de formation à la coopération internationale, incluant des FSI multinationaux, pour la région du Partenariat oriental, Minsk, Belarus, 2 – 5 mai 2017
CyberCrime@EAP III	Atelier sur la réforme de la loi sur la cybercriminalité, Erevan, Arménie, 3 – 5 mai 2017
CyberCrime@EAP III	Atelier sur la réforme de la législation pour une meilleure conformité avec la Convention de Budapest sur la cybercriminalité, Bakou, Azerbaïdjan, 10 – 12 mai 2017
GLACY+	Actualisation de matériel pédagogique pour la formation judiciaire & création d'un cahier d'audience pour les magistrats – réunion de brainstorming, Bucarest, Roumanie, 15-16 mai 2017
CyberCrime@EAP III	Public Hearings on the Cybercrime Law Reform and Planning meeting, Kyiv, Ukraine, 17-19 mai
GLACY+	Session introductive pour la formation de formateurs sur la

	cybercriminalité et la preuve électronique 22-25 mai 2017, Rabat, Maroc
GLACY+	Session nationale du cours de formation des formateurs judiciaires sur la cybercriminalité et la preuve électronique Koforidua, Ghana 22-26 mai 2017,
iPROCEEDS	Soutien à la participation à l'examen 2017 (session d'été) du Master en informatique forensique et investigations liées à la cybercriminalité, University College Dublin, Irlande, 22 mai – 3 juin 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Sarajevo, Bosnie-Herzégovine, 22-23 mai 2017
GLACY+	Pacific Islands Law Officers' Network Cybercrime Workshop, Nuku'alofa, Tonga, 23-25 mai 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Ankara, Turquie, 25-26 mai 2017
GLACY+	Mission de conseil sur la rationalisation des procédures pour l'entraide judiciaire liée à la cybercriminalité et à la preuve électronique, Nuku'alofa, Tonga, 26 mai 2017
Cybercrime@Octopus	Premier projet d'analyse des dispositions de la Loi libanaise sur les transactions électroniques et les données personnelles par rapport aux exigences de la Convention de Budapest et rédaction des recommandations nécessaires, 30 mai 2017
GLACY+	Participation à la deuxième réunion annuelle GFCE, Bruxelles, Belgique, 31 mai - 1 juin 2017
Cybercrime@Octopus	Visite d'évaluation des besoins et atelier sur la cybercriminalité et la preuve électronique, Astana, Kazakhstan, 31 mai – 2 juin 2017

juin 2017

CyberCrime@EAP III	Développement de l'Étude sur les responsabilités des fournisseurs de services sur Internet, région du Partenariat oriental, juin – juillet 2017
Cybercrime@Octopus	Conférence régionale pour les services de poursuite spécialisés, portant sur la cybercriminalité et la preuve électronique, Buenos Aires, Argentine, 1 – 2 juin 2017
GLACY+	Conférence lors de la formation spécialisée sur le droit pénal international et les menaces mondiales à l'encontre de la paix et de la sécurité, UNICRI, Turin, 5 juin 2017
GLACY+	Participation à la 5e réunion du Groupe de travail Eurasie d'INTERPOL sur la cybercriminalité pour les Chefs d'unités ; participation à la réunion opérationnelle organisée en marge sur la compromission de correspondance électronique professionnelle, Madrid, Espagne, 5-8 juin 2017
CyberCrime@EAP II CyberCrime@EAP III	Steering Committee meeting and participation in the Euro DIG 2017 conference, Tallinn, Estonie, 5-7 juin 2017
GLACY+ CyberCrime@EAP II iPROCEEDS Cybercrime@Octopus	17e réunion plénière du Comité de la Convention sur la cybercriminalité t (T-CY), Strasbourg, France, 7-9 juin 2017
iPROCEEDS	3rd meeting of the iPROCEEDS Project Steering Committee (PSC), Luxembourg, 12 juin 2017
iPROCEEDS	International workshop on search, seizure and confiscation of proceeds from crime online, Luxembourg, 12-13 juin 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online

	crime proceeds, Podgorica, Monténégro, 13-14 juin 2017
GLACY+ CyberCrime@EAP II iPROCEEDS	International Workshop on Cybercrime Training Strategies for Law Enforcement Agencies and access to ECTEG materials, Bruxelles, Belgique, 15-16 juin 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Skopje, "ex-République yougoslave de Macédoine", 15-16 juin 2017
GLACY+	Counseling on the streamlining of procedures for Mutual Legal Assistance related to Cybercrime and Electronic Evidence, Tagaytay, Philippines, 19-20 juin 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Pristina, Kosovo* , 19-20 juin 2017
GLACY+	GLACY+ : Le cours de formateurs pour les 1ers intervenants sera intégré dans la formation initiale des officiers de gendarmerie d'Afrique de l'Ouest, Dakar, Sénégal, 19 – 26 Juin 2017
iPROCEEDS	Regional training of trainers (ToT) on delivery of the introductory training module on cybercrime, electronic evidence and online crime proceeds, Budva, Monténégro, 20 -24 juin 2017
GLACY+	Development of cybercrime investigations, digital forensics capabilities combined with National workshop et advice on interagency cooperation et public private collaboration to fight cybercrime, Manille, Philippines, 21-23 juin 2017
iPROCEEDS	Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Belgrade, Serbie, 22-23 juin 2017
iPROCEEDS	Meeting on Public-private cooperation for fighting cybercrime and online crime proceeds, Skopje, "ex-République yougoslave de Macédoine", 23 juin 2017
CyberCrime@EAP II	Participation à la Conférence régionale de l'IAP sur l'Europe orientale et l'Asie centrale, Tbilissi, Géorgie, 26-28 juin 2017
GLACY+	Participation à la 59e réunion de politique de l'ICANN, Johannesburg, Afrique du Sud, 26-29 juin 2017
GLACY+	ASEAN Regional meeting in view of sharing good practices and promote harmonisation of legislation on Cybercrime et EE as well as rule of law et human rights safeguards, Cebu City, Philippines, 27-29 juin 2017
CyberCrime@EAP II	8e Conférence régionale de l'IAP sur l'Europe orientale et l'Asie centrale (International Association of Prosecutors), Tbilissi, Géorgie, 28 juin 2017
iPROCEEDS	Meeting on Public-private cooperation for fighting cybercrime and online crime proceeds, Pristina, Kosovo* , 29 juin 2017

juillet 2017

GLACY+	Mission de conseil sur les capacités du CERT, laboratoires forensiques numériques et Coopération public-privé, Nuku'alofa, Tonga, 3-5 juillet 2017
CyberCrime@EAP III	seminar on CSIRT/CERT Regulations and Operational Environment, Minsk, Belarus, 5-7 juillet 2017
GLACY+	Atelier sur les mécanismes de signalement d'affaires de cybercriminalité et sur la collecte et le contrôle des statistiques de justice pénale relatives à la cybercriminalité et à la preuve électronique, Nuku'alofa, Tonga, 6 juillet 2017
GLACY+	Mission de conseil et atelier sur cybercriminalité et les politiques et

	stratégies en matière de cybersécurité, Port Louis, Ile Maurice, 6-7 juillet 2017
CyberCrime@EAP II	Mission de conseil sur les constats et recommandations concernant le point de contact 24/7, Tbilissi, Géorgie, 10-12 juillet 2017
GLACY+	East African Regional Conference on Cybercrime and Electronic Evidence, en collaboration avec le GPEN et avec la participation d'organisations régionales et internationales de pays pertinents de la région de l'Afrique de l'Est, Pointe aux Piments, Ile Maurice, 10-12 juillet 2017
GLACY+	- Développement d'investigations dans des affaires de cybercriminalité, capacités d'informatique forensique ; - atelier dans le pays et conseils sur la coopération interservices et la collaboration public-privé pour lutter contre la cybercriminalité, Nuku'alofa, Tonga, 10-14 juillet 2017
GLACY+	Le Nigéria invité à adhérer à la Convention de Budapest , Strasbourg, 11 juillet 2017
GLACY+	Residential workshop for High Court Judges on cybercrime and electronic evidence, Kalutara, Sri Lanka, 28-30 juillet 2017
iPROCEEDS	Actualisation du matériel du cours de base sur la cybercriminalité, la preuve électronique et les produits du crime en ligne à la suite de la formation régionale pour former les formateurs afin qu'ils puissent dispenser à des juges et des procureurs le module de base sur la cybercriminalité, la preuve électronique et les produits du crime en ligne, étude documentaire, juillet 2017

août 2017

iPROCEEDS	Réunion préparatoire pour convenir des aspects/éléments, notamment les solutions techniques, du Scénario du Cyber-exercice qui doivent être révisés/actualisés/développés afin d'être ensuite repris au niveau national (C-PROC, consultants), Bucarest, Roumanie, 9-11 août 2017
GLACY+	Support to the Residential Workshop on Cybercrime and Electronic Evidence for Intake of New Judges, Colombo, Sri Lanka, 9-13 août 2017
GLACY+	- Développement d'investigations dans des affaires de cybercriminalité, capacités d'informatique forensique ; - atelier dans le pays et conseils sur la coopération interservices et la collaboration public-privé pour lutter contre la cybercriminalité, Port Louis, Ile Maurice, 15-18 août 2017
Cybercrime@Octopus	La Convention de Budapest et son rapport explicatif enfin disponibles en arabe, Bucarest, Roumanie, 16 août 2017
GLACY+	Special training on cybercrime and electronic evidence for Nepal judicial officers, Katmandou, Népal, 16-20 août 2017
GLACY+	Soutien à l'organisation au niveau national du Cours d'introduction sur la cybercriminalité et la preuve électronique pour les procureurs, Premier groupe, Ada, Ghana, 17-18 août 2017
GLACY+	Soutien à l'organisation au niveau national du Cours d'introduction sur la cybercriminalité et la preuve électronique pour les procureurs, Deuxième groupe, Kumasi, Ghana, 21-22 août 2017
GLACY+	Workshop for priority countries on data protection and overall police capabilities implemented by INTERPOL, Dakar, Sénégal, 21-23 août 2017
iPROCEEDS	Élaboration d'un Questionnaire sur l'obtention et l'utilisation de la preuve électronique dans les procédures pénales dans le cadre du droit interne

	respectif des pays bénéficiaires, étude documentaire, août 2017
Cybercrime@Octopus	Participation au 10e Sommet annuel ASSOCHAM sur la cyber-sécurité et la sécurité des réseaux, New Delhi, Inde, 31 août 2017

septembre 2017

iPROCEEDS	Participation à la Conférence 2017 sur l'économie souterraine, Barcelone, Espagne, 05 - 08 septembre 2017
CyberCrime@EAP III	Séminaire sur le mémorandum de coopération : aspects techniques, et présentation des principes d'un mémorandum à la Réunion annuelle des Télécoms d'Ukraine, Kyiv, 7-8 septembre et Odessa, Ukraine, 9 – 10 septembre 2017
CyberCrime@EAP III	4th Regional meeting on public/private cooperation: Legislation, Safeguards and Cooperation with Service Providers, Chisinau, Moldova, 11-12 septembre 2017
GLACY+	Regional Conference on Harmonization of legislation on Cybercrime et Electronic Evidence with rule of law et human rights safeguards, Abuja, Nigéria, 11-13 septembre 2017
GLACY+	Cours ECTEG, Formation spécialisée sur la Cybercriminalité et l'informatique forensique pour les agents des services répressifs (Linux comme outil d'investigation), Accra, Ghana, 11-15 septembre 2017
CyberCrime@EAP III	Atelier pour soutenir la révision de la Loi 161 dans le cadre des suites à donner à un Avis de la Commission de Venise, Chisinau, Moldova, 14 septembre 2017
Cybercrime@Octopus	Supports Training on Cybercrime and E-Evidence for Prosecutors in Argentina, Mendoza, Argentine, 14-15 septembre 2017
iPROCEEDS	Online Financial Fraud and Credit Card Fraud Workshop, Podgorica, Monténégro, 18-19 septembre 2017
CyberCrime@EAP II	Atelier sur le soutien au développement de la Loi de l'Arménie sur la coopération internationale en matière pénale/entraide judiciaire, Erevan, Arménie, 19-20 septembre 2017
GLACY+	Ateliers dans le pays sur la protection des données et les Outils et Services d'INTERPOL combinés à un soutien sur les modalités de création et de renforcement des points de contact 24/7 sur la cybercriminalité et la preuve électronique, Kenitra, Maroc, 20-22 septembre 2017
GLACY+	Residential Workshop on Cybercrime and Electronic Evidence for District Judges et Magistrates, Colombo, Sri Lanka, 22-24 septembre 2017
GLACY+	Mission de conseil sur la rationalisation des procédures pour l'entraide judiciaire concernant la cybercriminalité et la preuve électronique, Rabat, Maroc, 25-26 septembre 2017
GLACY+	Participation à la réunion du GFCE sur des bonnes pratiques mondiales, La Haye, Pays-Bas, 25-26 septembre 2017
iPROCEEDS	Cybercrime Simulation Exercise on cybercrime and financial investigations, Skopje, "ex-République yougoslave de Macédoine", 25-28 septembre 2017
GLACY+	Introductory Cybercrime and Electronic Evidence Training of Trainers Course for the Pacific Region, Nuku'alofa, Tonga, 25-29 septembre 2017
Cybercrime@Octopus, GLACY+, CyberCrime@EAP II, iPROCEEDS	Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime, La Haye, Pays-Bas, 26-27 septembre 2017

Cybercrime@Octopus	Participation au Forum sur la Cybersécurité Forum et Symposium pour la région des Amériques, Montevideo, Uruguay, 26-29 septembre 2017
GLACY+, CyberCrime@EAP II, iPROCEEDS	Participation à la 5e Conférence INTERPOL – Europol, La Haye, Pays-Bas, 27-29 septembre 2017