COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Documents d'information

SG/Inf(2018)32

Strasbourg, le 14 novembre 2018

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

Rapport d'activité du C-PROC pour la période octobre 2017-septembre 2018

Table des matières

Résumé

Le présent rapport a pour objet d'informer le Comité des Ministres 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 2017 à septembre 2018[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 tous les projets de renforcement des capacités en matière de lutte contre la cybercriminalité. Depuis sa création, le C-PROC a mené ou soutenu quelque 620 activités faisant intervenir plus de 150 pays.

Entre octobre 2017 et septembre 2018, le Bureau a soutenu quelque 220 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. Ces activités ont porté sur l'amélioration de la législation, la formation des juges, des procureurs et des enquêteurs, la coopération public/privé et la coopération internationale, ainsi que sur d'autres mesures destinées à renforcer la réponse apportée par la justice pénale à la cybercriminalité et aux preuves électroniques.

Le Bureau est largement financé par des ressources extrabudgétaires. En septembre 2018, les projets en cours de mise en œuvre par le Bureau représentaient un budget de plus de 26 millions EUR et un effectif de 29 personnes (originaires de neuf États membres). Il est dirigé par le Chef de la Division de la cybercriminalité (DGI), qui partage son temps entre Strasbourg et Bucarest et est secondé par un Chef des opérations expérimenté. Les rémunérations de tous les agents – à l'exception du Chef du Bureau – sont couvertes par les budgets des projets dont ils ont la responsabilité. Les locaux du C-PROC sont situés dans la Maison des Nations Unies à Bucarest, mis gracieusement à sa disposition par le Gouvernement roumain.

L'expérience de l'année passée confirme que le Bureau est à la hauteur des attentes suscitées par sa création :

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

- Le Bureau doit sa pertinence et son influence non seulement au volume des projets et des activités, mais aussi aux fortes synergies qui existent entre la Convention de Budapest, le suivi et les évaluations menés par le Comité de la Convention cybercriminalité (T-CY) et les activités de renforcement des

[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
Pour la période allant d'octobre 2016 à septembre 2017, se reporter à ce document.

capacités menées par le C-PROC. Entre octobre 2017 et septembre 2018, le C-PROC a apporté son soutien et des ressources au T-CY pour répondre aux difficultés liées au Budget ordinaire du Conseil de l'Europe.

- Les activités de renforcement des capacités menées par le C-PROC permettent à des États non membres d'adhérer à la Convention de Budapest. Au cours des douze derniers mois, six États d'Afrique, d'Asie et d'Amérique latine sont ainsi devenus parties à la Convention.

- Les activités sont conçues pour renforcer les droits de l'homme, la démocratie et l'État de droit par la législation, par des formations ciblées et par la protection des données et d'autres mesures de prévention.

- Le Bureau s'avère attractif pour les donateurs. Le volume de projets, qui s'élevait à 4 millions EUR environ à sa création en avril 2014, a atteint plus de 26 millions EUR en septembre 2018. D'autres projets sont en préparation.

- Les autorités compétentes du Gouvernement roumain, mais aussi d'autres États parties à la Convention de Budapest (à l'heure actuelle, l'Allemagne, l'Estonie, la France, 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. Le Bureau et ses projets ont noué d'étroites relations avec de nombreuses autres organisations.

Le Bureau poursuivra dans la même direction et, dans le même temps, des objectifs spécifiques ont été fixés pour les douze mois à venir, notamment :

- accent mis sur la protection des droits de l'homme et de l'État de droit ;

- protection des enfants contre la violence sexuelle en ligne et autres mesures de lutte contre la cyberviolence ;

- levée de fonds destinés à assurer le suivi de projets mis en œuvre dans les pays du Partenariat oriental et en Europe du Sud-Est ;

- renforcement des compétences spécialisées du Bureau.

Le Bureau est à la hauteur des attentes suscitées par sa création et les conditions de son développement sont réunies.

Il est proposé qu'il continue de fonctionner selon les modalités actuelles.

1 Cadre et objet du présent rapport

Le présent rapport a pour objet d'informer le Comité des Ministres du Conseil de l'Europe 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 2017 à septembre 2018.

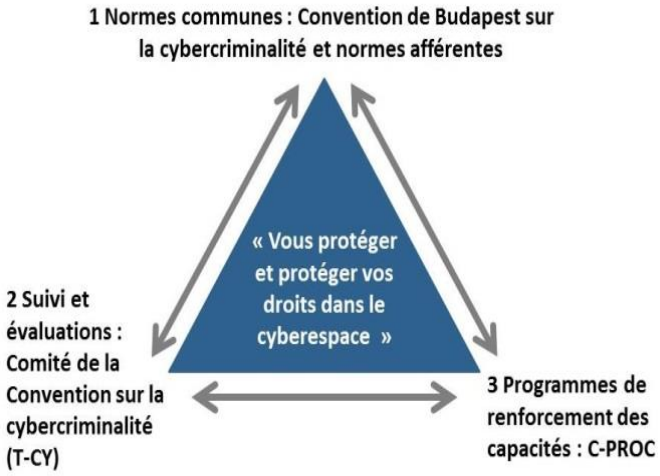
La cybercriminalité – à savoir les infractions commises contre des systèmes informatiques ou au moyen de ces systèmes – est devenue une menace grave pour les droits fondamentaux, la démocratie et l'État de droit ainsi que pour la paix et la stabilité internationales. Parallèlement, la question de la 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, les systèmes électoraux 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.

La question de la cybercriminalité et de la preuve électronique est donc étroitement liée à la mission fondamentale du Conseil de l'Europe, à savoir la promotion des droits de l'homme, de la démocratie et de l'État du droit.

L'approche adoptée par le Conseil de l'Europe pour relever ces défis consiste en un triangle « dynamique » de trois éléments interdépendants :

- La Convention de Budapest sur la cybercriminalité (STE n° 185), ouverte à la signature en 2001[2], qui demeure le traité international le plus pertinent sur cette question. En septembre 2018, 61 États sont Parties à cette Convention et 10 autres l'ont signée ou ont été invités à y adhérer. La Convention de Budapest est donc l'un des traités du Conseil de l'Europe ayant rencontré le plus de succès en termes d'adhésion ;



- 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

[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.

aux nouveaux défis qui se posent. Avec, à l'heure actuelle, 72 membres et États observateurs[3] et onze organisations observatrices, le T-CY est l'un des principaux organes intergouvernementaux intervenant dans le domaine de la cybercriminalité au niveau international. Aujourd'hui, sa priorité est la préparation d'un Protocole additionnel à la Convention sur la cybercriminalité qui portera sur le renforcement de la coopération internationale et l'accès aux preuves dans le nuage ;

- 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. Au demeurant, les débats menés au niveau des Nations Unies début 2013[4] ont confirmé qu'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 la preuve électronique.

La décision prise par le Comité des Ministres en octobre 2013[5], qui faisait suite à une offre du Gouvernement roumain et à une proposition du Secrétaire Général (SG/Inf(2013)29) d'établir un Bureau de programme sur la cybercriminalité à Bucarest (Roumanie), constitue la réponse du Conseil de l'Europe à ce besoin de renforcement des capacités au niveau mondial.

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 spécialisé qui mettrait 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 largement par des ressources extrabudgétaires.

L'expérience montre, après 54 mois de fonctionnement, que ces attentes ont été plus que satisfaites.

---

[3] 61 États Parties, 10 signataires ou États invités à adhérer ainsi que la Fédération de Russie.
[4] Réunion du Groupe d'experts intergouvernemental des Nations Unies sur la cybercriminalité, février 2013.
[5] Décision du 9 octobre 2013 à la 1180e réunion du Comité des Ministres.

2 Mandat du Bureau[6]

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

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 du secteur 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) – et donc 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 allant d'octobre 2017 à septembre 2018

Le C-PROC est chargé d'aider les pays du 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 de ses normes afférentes[7]. Le Bureau s'acquitte de sa mission en mettant en œuvre des projets de renforcement des capacités.

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

[7] 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 2017 à septembre 2018, le C-PROC a apporté son soutien à environ 220 activités[8] relevant des projets suivants :

Intitulé du projet	Durée	Budget	Financement
Cybercrime@Octopus (n° 3021)	jan 2014 – déc 2019	3,5 millions EUR	Contributions volontaires (Estonie, États-Unis, Hongrie, Japon, Monaco, République slovaque, Roumanie, Royaume-Uni et Microsoft)
Cybercrime@EAP II sur la coopération internationale dans les pays du Partenariat oriental (n° 3271)	mai 2015 – déc 2017	800 000 EUR	Programme conjoint UE/CdE (Partenariat pour la bonne gouvernance)
Cybercrime@EAP III sur la coopération public/privé dans les pays du Partenariat oriental (n° 3608)	déc 2015 – déc 2017	1,2 million EUR	Programme conjoint UE/CdE (Partenariat pour la bonne gouvernance)
Cybercrime@EAP 2018 sur la coopération internationale et public/privé dans les pays du Partenariat oriental (n° 1963)	jan 2018 – déc 2018	980 000 EUR	Programme conjoint UE/CdE (Partenariat pour la bonne gouvernance)
GLACY+ projet sur l'Action globale sur la cybercriminalité élargie (n° 3148)	mar 2016 – fév 2021	13,35 millions EUR	Programme conjoint UE/CdE
iPROCEEDS projet ciblant les produits de la criminalité exercée sur internet en Europe du Sud-Est et en Turquie (n° 3156)	jan 2016 – juin 2019	5,56 millions EUR	Programme conjoint UE/CdE
CyberSud projet sur le renforcement des capacités dans les pays du voisinage sud	juil 2017 – juin 2020	3,33 millions EUR	Programme conjoint UE/CdE

En septembre 2018, les projets en cours de mise en œuvre par le C-PROC représentaient un budget cumulé d'environ 26,7 millions EUR. Le projet Cybercrime@Octopus est entièrement financé par des contributions volontaires, tandis que les projets conjoints avec l'Union européenne sont cofinancés à 10 % par le budget du Conseil de l'Europe (environ 2,5 millions EUR).

On observe donc une augmentation par rapport aux années précédentes (septembre 2015: 6 millions EUR, septembre 2016: 22 millions EUR, septembre 2017: 24,4 millions EUR).

Conformément à son mandat, le C-PROC a identifié, développé et négocié l'ensemble de ces projets et réuni les fonds nécessaires à leur financement.

[8] Voir l'annexe pour la liste des activités.

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.

Parmi les activités menées entre octobre 2017 et septembre 2018, on peut citer l'organisation d'un atelier pour les points de contact du réseau 24/7 dans le cadre de la Convention de Budapest (Strasbourg, juillet 2018), le passage en revue du cadre juridique ou des projets de loi du Koweït, du Qatar, de Samoa et de Vanuatu par rapport aux dispositions de la Convention de Budapest, le passage en revue de la législation coréenne et le dialogue avec le Gouvernement coréen dans le but de l'adhésion de la Corée à la Convention de Budapest, le passage en revue de la législation malaisienne et le dialogue avec les autorités malaisiennes, la préparation – en coopération avec d'autres projets – d'une analyse de l'état de la législation sur la cybercriminalité au niveau mondial, l'aide apportée à l'organisation d'une conférence sur la cybercriminalité et la coopération public/privé en Inde en août 2018, et la contribution à la formation de juges de pays francophones à Paris en juin 2018.

De plus, le projet Cybercrime@Octopus a facilité la participation de parties et d'observateurs à la Convention de Budapest à d'importants événements internationaux, notamment le Groupe d'experts intergouvernemental des Nations Unies sur la cybercriminalité à Vienne en avril 2018, la Commission des Nations Unies pour la prévention du crime et la justice pénale en mai 2018, dont l'axe thématique majeur était la cybercriminalité, le Forum mondial sur la cyberexpertise, la Conférence mondiale sur le cyberespace à New Delhi en novembre 2017 et le Forum sur la gouvernance de l'internet à Genève en décembre 2017.

La Conférence Octopus – organisée dans le cadre de ce projet – demeure l'activité phare du Conseil de l'Europe en matière de cybercriminalité. Elle est organisée une fois tous les 18 mois. L'édition 2018 a eu lieu à Strasbourg du 11 au 13 juillet 2018 et a réuni quelque 360 experts de 95 pays ainsi que de nombreuses organisations des secteurs public et privé. Cette conférence a proposé, entre autres, une plate-forme destinée aux consultations multi-parties sur le 2e Protocole additionnel à la Convention de Budapest.

En outre, Cybercrime@Octopus a vocation à soutenir le Comité de la Convention cybercriminalité (T-CY). Par exemple, il a financé la participation d'États observateurs aux réunions plénières du T-CY, et – grâce à la contribution financière des États-Unis – l'interprétation vers et depuis l'espagnol pour faciliter la participation des pays latino-américains au T-CY. Au printemps 2018, le Royaume-Uni a mis des contributions à disposition afin de soutenir l'organisation des réunions du T-CY destinées à la préparation du 2e Protocole additionnel à la Convention de Budapest. De plus, les agents du C-PROC apportent 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 TC-Y et le C-PROC.

Le projet a jusqu'ici été financé par l'Estonie, la Hongrie, Monaco, la Roumanie (apport en nature), la République slovaque, le Royaume-Uni, le Japon, les États-Unis et Microsoft, les États-Unis étant le plus gros contributeur.

D'une manière générale, Cybercrime@Octopus est un outil flexible qui vise à répondre aux besoins, à renforcer la législation, à promouvoir les partenariats multipartites et à soutenir concrètement l'action du T-CY. Il demeure une ressource à laquelle les donateurs peuvent contribuer pour lutter contre la cybercriminalité et soutenir le T-CY à tout moment sans être pénalisé par la lenteur inhérente à la conception et à l'approbation des projets.

3.3 Cybercrime@EAP II – Coopération internationale

Le projet Cybercrime@EAP II, qui a bénéficié d'un budget de 800 000 EUR et s'est déroulé entre mai 2015 et décembre 2017, visait au renforcement des capacités des pays du Partenariat oriental (Arménie, Azerbaïdjan, Bélarus, Géorgie, République de Moldova et Ukraine) en matière de coopération judiciaire et policière internationale dans le domaine de la cybercriminalité et de la preuve électronique.

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

Il a apporté un renforcement ciblé des capacités dans les pays du Partenariat oriental dans le but d'améliorer les compétences des autorités ainsi que les règles et procédures qui régissent la coopération internationale.

La participation des équipes de pays aux manifestations internationales comme les sessions plénières du Comité de la Convention cybercriminalité (T-CY) et la conférence Octopus, les réunions du Groupe Pompidou et du groupe d'experts des Nations Unies sur la cybercriminalité, les formations et les réunions internationales organisées par EUROPOL/INTERPOL – et d'autres événements régionaux et internationaux – a donné l'occasion de mettre en commun un ensemble de bonnes pratiques au niveau international. Les activités nationales ont ciblé les lacunes des cadres réglementaires, le cadre institutionnel et les capacités et compétences nécessaires à une coopération internationale effective en matière de cybercriminalité et de preuve électronique.

Des progrès importants ont été accomplis pendant cette période :

- Un programme de formation sur la coopération internationale et la coopération avec les prestataires de services multinationaux a été élaboré et dispensé dans tous les pays du Partenariat oriental. Un jeu complet de supports, mis au point

pour ces formations spécialisées, est disponible pour les futures initiatives de renforcement des capacités.

- Des modèles de demandes normalisées d'entraide judiciaire (article 31 de la Convention de Budapest) et de conservation de données (article 29 et 30 de la Convention) ont été élaborés et des ressources en ligne sur la coopération internationale au sein de la communauté Octopus ont été mises au point et testées dans cette région. Ces modèles ont ensuite été améliorés puis adoptés par le T-CY en vue de leur utilisation par l'ensemble des parties à la Convention de Budapest en juillet 2018.

- Le projet a soutenu des réformes de droit procédural dans cinq pays du Partenariat oriental, sachant que les vides juridiques dans la législation nationale de procédure pénale entravent la coopération internationale en matière de cybercriminalité et de preuve électronique.

3.4 Cybercrime@EAP III – Coopération public/privé

Le projet Cybercrime@EAP III, mis en oeuvre entre 2016 et décembre 2017, visait à promouvoir la coopération entre les autorités responsables de la justice pénale dans les pays du Partenariat oriental et les prestataires de services. Il était doté d'un budget de 1,2 million EUR. Ce projet, qui était le premier de ce genre dans la région, a fait ressortir la complexité de la question.

Le projet visait essentiellement à établir une relation de confiance pour préparer la coopération public/privé, en contribuant à ce que les acteurs concernés se rencontrent et en encourageant le dialogue, notamment avec les prestataires de services multinationaux. Des efforts ont été entrepris pour faciliter la conclusion ou la mise à jour d'accords de coopération en Arménie, Géorgie, République de Moldova et Ukraine.

De plus, le projet a fortement insisté sur la nécessité primordiale d'entreprendre des réformes du droit de procédure pénale pour préparer la coopération public/privé, ces réformes consistant à clarifier la législation en vigueur et à établir une relation de confiance avec les entreprises privées. Des ateliers et des auditions ont été organisés à cette fin en Azerbaïdjan, en Arménie, en Géorgie et en Ukraine. Des commentaires écrits sur des projets de loi ont été soumis aux autorités de ces pays. En République de Moldova, le projet a coopéré avec la Commission de Venise, ce qui a donné lieu à un Avis sur les propositions d'amendements aux lois.

La question du renforcement de la législation interne a également été posée au Bélarus en vue d'encourager une réforme du droit procédural qui s'inscrive dans le droit fil de la Convention du Budapest et des exigences de la prééminence du droit.

Gardant à l'esprit la nature régionale du projet, des activités de niveau régional et international sur la question des partenariats public/privé ont été mises à profit pour échanger des données d'expérience sur ce type de coopération.

Grâce aux efforts déployés dans le cadre de ce projet, les pays du Partenariat oriental sont désormais engagés dans un dialogue permanent avec les fournisseurs de services internet et d'autres acteurs nationaux importants, dans le but d'améliorer la coopération entre les pouvoirs publics et l'industrie de l'internet en termes d'accès aux données, tandis que leur participation aux discussions internationales avec les prestataires de services mondiaux leur permet de coopérer plus efficacement avec ces entreprises dans le cadre des enquêtes criminelles.

3.5 Cybercrime@EAP 2018 – Coopération internationale et coopération public/privé

Prolongement des projets Cybercrime@EAP II et Cybercrime@EAP III, le projet PGG 2018 – Cybercrime@EAP 2018 maintient la priorité sur la coopération internationale et les partenariats public/privé en matière de cybercriminalité et de preuve électronique.

Les capacités des autorités publiques chargées de l'entraide judiciaire et de la coopération entre services de police ont été renforcées grâce à la participation à des sessions du Comité de la Convention cybercriminalité (T-CY), à des conférences Octopus, à la conférence conjointe d'Eurojust sur la cybercriminalité, aux réunions du réseau des points de contact 24/7 en vertu de l'article 35 de la Convention de Budapest, à des conférences annuelles d'INTERPOL/EUROPOL sur la cybercriminalité et à des réunions du Groupe Pompidou sur ce même thème. Le Dialogue paneuropéen sur la gouvernance d'internet (EuroDIG) continue d'être la plate-forme de discussions de référence pour la région sur les questions de coopération public/privé.

La seconde édition de l'exercice régional de coopération contre la cybercriminalité, forte du succès de la première édition de l'exercice menée en 2017, a prolongé l'expérience en faisant participer directement des fournisseurs de services internet de la région du Partenariat oriental.

Le projet Cybercrime@EAP 2018 a également ajouté de nouveaux éléments et de nouvelles approches.

À la suite de l'adoption par le TC-Y en juillet 2018 des modèles de demande de conservation et de demande d'entraide judiciaire en vue d'obtenir des informations sur un abonné, le projet a conçu et élaboré une série d'exercices pratiques sur table concernant la coopération internationale, des outils pratiques de test (comme le forum Octopus Cybercrime Community) et des modèles de coopération en situation réelle dans le cadre des articles 29 à 31.

Les compétences pratiques des points de contact du réseau 24/7 et des enquêteurs en matière de cybercriminalité en matière de traitement des données relatives au trafic sont renforcées grâce à des cours techniques sur les enquêtes de réseau et l'analyse forensique de données en temps réel. Ces cours sont

organisés en coopération avec le Groupe européen de formation et d'éducation en matière de cybercriminalité (ECTEG) et au moyen des supports fournis par l'ECTEG.

L'accent mis sur les stratégies de la cybercriminalité pour favoriser la coopération interinstitutions et le dialogue public/privé est renforcé via une série d'ateliers pratiques organisés dans tous les pays du Partenariat oriental. Ces ateliers, qui ont réuni des acteurs majeurs, visaient à cartographier et à analyser les tâches et les responsabilités ainsi que la perception des menaces dans le cyberespace, et à concevoir des réponses stratégiques possibles à ces menaces sur la base de la Déclaration sur « les stratégies prioritaires dans la coopération contre la cybercriminalité dans la région du Partenariat oriental ».

Le projet continue de soutenir les réformes du droit de procédure pénale qui sont absolument nécessaires pour préparer la coopération public/privé, ces réformes consistant à clarifier la législation en vigueur et à établir une relation de confiance avec les entreprises privées (Azerbaïdjan, République de Moldova, discussion via des réunions régionales). Le cadre institutionnel, la réglementation et les responsabilités applicables à la coopération internationale font l'objet de missions de conseil auprès de certains pays de la région (Arménie, Azerbaïdjan et Ukraine).

Finalement, pour maximiser l'impact et la pérennité des efforts consentis, le projet s'associe et apporte son soutien à diverses enceintes nationales et régionales de coopération dans le cadre de partenariats public/privé, telles que les Forums sur la gouvernance de l'internet en Azerbaïdjan et en Ukraine, la conférence de l'OSCE sur le terrorisme à l'ère du numérique au Bélarus, la conférence géorgienne des innovations dans le domaine des technologies de l'information (GITI) pour l'Arménie et la Géorgie, et des événements « cybersemaine » en République de Moldova.

3.6 GLACY+ : Projet élargi d'action globale sur la cybercriminalité

Forts de l'expérience acquise au cours du projet GLACY, le Conseil de l'Europe et l'Union européenne sont convenus de prolonger le projet à travers GLACY+ « projet élargi d'action globale sur la cybercriminalité ». D'un point de vue technique, le projet, qui est doté d'un budget de 10 millions EUR, a démarré en mars 2016 et se poursuivra jusqu'en février 2020.

Du fait de son incidence et des besoins supplémentaires générés par les demandes d'adhésion (Cap Vert, Nigéria), les adhésions (Chili, Costa Rica), les manifestations d'intérêt pour l'adhésion et les besoins d'assistance exprimés par d'autres pays (Burkina Faso, Gambie, Népal, Samoa, Ouganda, Vanuatu et autres), le budget du projet a été porté à 13,35 millions EUR en mars 2018 et sa durée a été allongée (extension jusqu'en février 2021).

GLACY+ s'articule autour de trois grands 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. Donner les moyens aux forces de police d'enquêter sur les affaires de cybercriminalité et de mettre en place une véritable coopération entre services de police et 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 preuve électronique, et de coopérer à l'échelon international.

En vertu d'un accord conclu avec le Conseil de l'Europe, INTERPOL est un partenaire et il pilote la mise en œuvre du volet du projet relatif à l'application de la loi. Les autres partenaires du projet comprennent l'Estonie (ministère de la Justice), la France (ministère de l'Intérieur), la Roumanie (police nationale, poursuites (DIICOT) et ministère de la Justice), le Royaume-Uni (National Crime Agency) et les États-Unis (ministère de la Justice) ainsi qu'EUROPOL (Centre européen de lutte contre la cybercriminalité).

Entre octobre 2017 et septembre 2018, GLACY+ a apporté son soutien à quelque 95 activités.

À noter, parmi celles-ci, un ensemble de formations organisées par INTERPOL au Ghana, à Maurice, aux Philippines, en République dominicaine, au Sri Lanka et à Tonga.

Outre le grand nombre de formations internes à destination des juges, des procureurs et de la police, cette période a été marquée par des activités régionales et internationales d'importance majeure, parmi lesquelles :

- Forum sur la cybercriminalité et la preuve électronique pour les Amériques (République dominicaine, décembre 2017) avec plus de 200 participants de 40 pays, en partenariat avec l'OEA, le ministère américain de la Justice et INTERPOL, et avec la participation de plusieurs autres organisations ;

- Formations élémentaires et avancées de niveau régional pour les juges et les procureurs des pays anglophones de la CEDEAO (Ghana, décembre 2017 et juillet 2018) ;

- Atelier sur la coopération internationale organisé en coopération avec EUROJUST (La Haye, mars 2018) pour une centaine d'experts de 37 pays ;

- Formation d'échelon régional pour les juges et les procureurs des pays de l'ASEAN (Manille, Philippines, mars 2018) ;

- Atelier de niveau régional sur la cybercriminalité organisé en coopération avec le Réseau des fonctionnaires de justice des îles du Pacifique (PILON) (Tonga, juin 2018) et une formation judiciaire avancée pour la Région pacifique (Tonga, août 2018).

Le projet GLACY+ met fortement l'accent sur l'élaboration de la législation et la formation des juges et procureurs en vue de renforcer l'État de droit, notamment les sauvegardes. De ce fait, le projet œuvre de plus en plus en faveur de l'élaboration d'une législation de protection des données. Par exemple, en septembre 2018, en coopération avec l'unité de la protection des données du Conseil de l'Europe, le projet a aidé le Nigéria dans la rédaction de son projet de loi relatif à la protection des données. Des activités analogues sont programmées pour d'autres pays. En mars 2018 déjà, le projet GLACY+ avait aidé le Nigéria dans la finalisation de son projet de loi « liberté et droits numériques ».

3.7 Projet iPROCEEDS : cibler les produits de la criminalité exercée sur internet en Europe du Sud-Est

Le projet conjoint iPROCEEDS est déployé en Albanie, en Bosnie-Herzégovine, au Monténégro, en Serbie, dans « l'ex-République yougoslave de Macédoine », en Turquie et au Kosovo*[9]. Il a vocation à aider les autorités des pays de la région à renforcer leurs capacités en matière de dépistage, de saisie et de confiscation des produits de la cybercriminalité et de prévention du blanchiment de capitaux sur internet. Doté d'un budget de 5,56 millions EUR, le projet a démarré en janvier 2016 et prendra fin en juin 2019. Il est composé des volets suivants :

- Systèmes de signalement du public ;
- Législation ;
- Coopération entre les unités de lutte contre la cybercriminalité, les unités d'investigation financière et les cellules de renseignement financier ;
- Lignes directrices et indicateurs pour la détection de la fraude en ligne et du blanchiment de capitaux sur internet ;
- Partage d'informations public/privé ;
- Formation judiciaire ;
- Coopération internationale.

Le projet iPROCEEDS assure par conséquent le suivi des recommandations de l'étude typologique menée en 2012 par MONEYVAL et le projet global sur la cybercriminalité.

Le projet iPROCEEDS a contribué à l'amélioration des mécanismes de signalement des cybercrimes et de la collecte des statistiques sur la cybercriminalité. Lors de missions consultatives et d'ateliers organisés dans les sept pays/régions du projet, l'efficacité des systèmes de signalement a été évaluée

[9] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

et des recommandations ont été formulées en vue de réformer et d'améliorer la coopération entre agences et entre le secteur public et le secteur privé. Un exemple de méthodologie encourageant l'adoption d'une démarche plus globale pour la collecte, la réception et l'utilisation des statistiques en vue d'améliorer les enquêtes et les poursuites et d'aider les décideurs et les régulateurs à prendre des décisions stratégiques plus éclairées a été présenté lors de l'atelier régional sur les statistiques de justice pénale concernant la cybercriminalité et les preuves électroniques.

Dans le but d'atténuer les risques de blanchiment de capitaux et de contrôler la fraude en ligne et les flux de capitaux d'origine criminelle sur internet, le projet a continué d'apporter son soutien aux autorités concernées afin qu'elles améliorent et, si besoin, élaborent des indicateurs de prévention et de contrôle de la fraude en ligne et des flux de capitaux d'origine criminelle sur internet destinés aux entités du secteur financier, et qu'elles améliorent la diffusion de ces indicateurs. Au cours de la période couverte par le rapport, des indicateurs de la cybercriminalité ont été élaborés dans « l'ex-République yougoslave de Macédoine », au Kosovo*[10], au Monténégro et en Turquie.

La plupart des activités avaient pour objectif d'accroître les compétences et les capacités des investigateurs spécialisés dans la finance et la cybercriminalité, des procureurs et des représentants des cellules de renseignements financiers (CRF) en matière de dépistage, de saisie et de confiscation des produits du crime en ligne, grâce à des ateliers sur la fraude financière en ligne et la fraude à la carte de crédit, un atelier régional sur les preuves électroniques et un rapport d'évaluation sur la collecte et l'utilisation des preuves électroniques dans le cadre des procédures pénales, des formations spécialisées destinées aux investigateurs et aux spécialistes de l'analyse informatique forensique, et des exercices de coordination et de partenariat pour lutter contre la cybercriminalité.

Le projet iPROCEEDS a donné l'exemple en organisant la Conférence 2018 sur l'économie souterraine, qui a été coorganisée cette année par le Conseil de l'Europe, en ses locaux, à Strasbourg. Cet événement international de premier plan consacré à la sécurité de l'information a réuni quelque 400 représentants des services de répression, de la communauté de la cybersécurité, du secteur privé et des milieux universitaires du monde entier.

La seule manière efficace de s'assurer que les juges et les procureurs ont des connaissances suffisantes pour remplir leur rôle avec efficacité est de mettre en œuvre des programmes de formation judiciaire pérennes sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne. Le projet a donc apporté son soutien à la création d'une équipe de formateurs nationaux dans chaque institut de formation judiciaire des pays concernés par l'IPA, lesquels formateurs ont, au cours de la période couverte par le rapport, achevé avec succès le premier cycle des prestations nationales du module d'introduction de la

[10] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

formation judiciaire sur la cybercriminalité, les preuves électroniques et les produits de la cybercriminalité en ligne dans les sept pays/régions couvertes par le projet. Plus de 200 juges et procureurs ont bénéficié de ce cours et ont renforcé leurs connaissances sur les tendances et les menaces de la cybercriminalité, les technologies, les preuves électroniques, les investigations financières des produits de la cybercriminalité, y compris les lois matérielles et procédurales pertinentes, les typologies du blanchiment de capitaux liées à l'environnement en ligne, ainsi que les moyens et les voies de la coopération internationale en matière de dépistage, de saisie et de confiscation des produits de la criminalité en ligne. En outre, dans le cadre du projet iPROCEEDS, le *Manuel d'autoformation : cours avancé sur le dépistage, la saisie et la confiscation des produits du crime en ligne* destiné aux juges et aux procureurs a été traduit. Désormais disponible en anglais, en albanais, en serbe, en macédonien et en turc, ce manuel a été diffusé à toutes les institutions de formation judiciaire et publié sur le site de la Communauté Octopus.

Les supports élaborés par iPROCEEDS présentent aussi un intérêt pour d'autres projets.

3.8 Projet CyberSud sur la cybercriminalité et les preuves électroniques dans le voisinage sud

Le projet conjoint CyberSud du Conseil de l'Europe et de l'Union européenne couvre la région du voisinage sud, et, dans un premier temps, en priorité l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie. La durée du projet est de 36 mois (juillet 2017 – juin 2020) et le budget de 3,33 millions EUR.

L'objectif est de renforcer la législation et les capacités institutionnelles de lutte contre la cybercriminalité et d'utilisation des preuves électroniques dans la région du voisinage sud, en conformité avec les exigences relatives aux droits de l'homme et à l'État de droit. Le projet met l'accent sur la législation de lutte contre la cybercriminalité, les services de police spécialisés et la coopération entre agences, la formation judiciaire, les points de contact du réseau 24/7 et la coopération internationale, et sur les politiques de lutte contre la cybercriminalité. La conférence de lancement s'est tenue à Tunis en mars 2018.

Pendant la période allant d'octobre 2017 à septembre 2018, entre autres :

- des équipes de projet nationales ont été créées en Algérie, au Liban, au Maroc et en Tunisie. Ces équipes, qui comprennent les principales institutions homologues du projet, veillent à ce que les bénéficiaires se l'approprient et à sa mise en œuvre effective ;

- des visites d'évaluation ont été menées en Algérie, en Jordanie, au Liban et en Tunisie, et des rapports de situation initiale ont été élaborés pour ces pays, avec des recommandations sur la législation et d'autres sujets [11];

[11] Dans le cas du Maroc, ces activités avaient déjà été réalisées au titre du projet GLACY.

- la Tunisie a été invitée à adhérer à la Convention de Budapest en février 2018 et le Maroc a achevé son processus d'adhésion en juin 2018 ;

- des formations judiciaires ont été dispensées au Liban et au Maroc, et un manuel de formation judiciaire a été adapté en vue de son utilisation dans la région couverte par le projet. D'autres guides et supports ont été améliorés ou traduits en arabe ;

- le projet a apporté son soutien à la participation d'experts de pays couverts par le projet à des événements de formation internationaux et à des réunions pertinentes, notamment la conférence EUROJUST en mars 2018, la réunion des responsables des unités cybercriminalité d'INTERPOL de la région MENA (Alger, avril 2018), le Groupe d'experts intergouvernemental des Nations Unies sur la cybercriminalité (Vienne, avril 2018), la Commission des Nations Unies pour la prévention du crime (Vienne, mai 2018), la réunion plénière du TC-Y de novembre 2017 et la conférence Octopus de juillet 2018.

Ces activités menées au cours de la première année de mise en œuvre du projet CyberSud ont préparé le terrain pour les deux années restantes.

CyberSud – comme d'autres projets gérés par le C-PROC – œuvre en faveur des droits de l'homme, de la démocratie et de l'État de droit en dispensant des formations à des juges, des procureurs et des enquêteurs, en normalisant des procédures et des sauvegardes, en renforçant l'indépendance de la justice et en permettant aux services de répression de suivre de bonnes pratiques internationales lorsqu'ils enquêtent sur une affaire de cybercriminalité et qu'ils doivent protéger des preuves électroniques.

4 Autres priorités de financement

Avec les projets engagés, le C-PROC dispose d'une base solide et des ressources nécessaires pour produire ses effets sur les deux à trois ans qui viennent. Parmi les autres priorités concernant les projets et les financements, on peut citer :

- nouveau projet intitulé « Mettre fin à l'exploitation et aux abus sexuels en ligne concernant les enfants ». Les fonds associés à ce projet (1 million USD) ont été reçus. Il sera mis en œuvre conjointement par la Division des droits des enfants du Conseil de l'Europe et par le C-PROC à partir d'octobre/novembre 2018 ;

- soutien accru aux pays du Partenariat oriental, compte tenu du fait que le projet actuel Cybercrime@EAP se termine le 31 décembre 2018. Les discussions avec l'Union européenne à propos d'un nouveau projet sont bien avancées ;

- suite du projet iPROCEEDS sur les flux de capitaux d'origine criminelle en ligne en Europe du Sud-Est, étant donné que le projet actuel doit se terminer en juin 2019 ;

- contributions volontaires additionnelles au projet Cybercrime@Octopus en vue du soutien à apporter aux travaux du Comité de la Convention cybercriminalité ;

- augmentation du budget et prolongement du projet GLACY+ pour répondre aux demandes croissantes d'assistance ;

- 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.

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

Le secrétariat du T-CY est assuré par des agents basés à Strasbourg tandis que toutes les activités de renforcement des capacités sont gérées par le C-PROC. Le C-PROC entretient des liens étroits avec le T-CY : le Secrétaire exécutif de ce dernier est également le Chef du C-PROC et il partage son temps entre Strasbourg et Bucarest.

L'expérience des douze derniers mois confirme les fortes synergies qui existent entre ces deux organes depuis 2014. Les travaux du T-CY alimentent directement les activités de renforcement des capacités, et inversement.

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 au 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.

Les projets portés par le Bureau contribuent aussi en substance au T-CY. Citons, à titre d'exemple, les modèles de demande d'informations sur un abonné et de conservation de données, qui ont été adoptés par le T-CY en juillet 2018 et qui ont été élaborés et testés dans le cadre d'un projet du Partenariat oriental sur la cybercriminalité.

Entre octobre 2017 et septembre 2018, plusieurs activités du T-CY ont été financées ou cofinancées par le budget du projet Cybercrime@Octopus, notamment les réunions plénières du T-CY de novembre 2017 et juillet 2018, et des réunions du groupe de rédaction du protocole du T-CY en février, avril, mai et septembre 2018. Le Royaume-Uni a versé des contributions volontaires expressément au processus de rédaction du protocole via le projet Cybercrime@Octopus. Des contributions volontaires des États-Unis ont permis d'assurer l'interprétation des réunions plénières du T-CY en espagnol.

L'une des fonctions du T-CY est de faciliter l'émergence de positions communes parmi les parties à la Convention de Budapest dans les enceintes internationales. Le C-PROC a contribué à la réalisation de cet objectif à plusieurs reprises et a financé la participation à des réunions pertinentes lorsque cela était nécessaire.

Par ailleurs, la maintenance du site web du T-CY et des autres ressources en ligne a été assurée par des agents rémunérés au titre du projet Cybercrime@Octopus.

6 Relations avec le Gouvernement roumain

Le Gouvernement continue d'honorer ses engagements pris au titre du mémorandum d'accord signé en octobre 2013 et a accéléré l'adoption de la loi ratifiant le mémorandum (ratification début avril 2014).

Un espace de bureaux à la Maison des Nations Unies, emplacement privilégié à Bucarest, est mis à disposition du Conseil de l'Europe gratuitement.

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 ou accueillent des visites d'études de pays liés au projet.

Le Bureau est régulièrement invité à participer et à intervenir lors de 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 Personnel

Entre octobre 2017 et septembre 2018, l'équipe est passée de 21 à 29 personnes.

Le Bureau est dirigé par le Secrétaire exécutif du Comité de la Convention cybercriminalité (également 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.

Face à l'augmentation de l'effectif et des ressources gérées au C-PROC, un chef des opérations, qui est aussi le gestionnaire du centre de coûts, a été recruté en juillet 2017.

En septembre 2018, le Bureau comptait donc 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 (dix chargés de projet de grade B4/5, deux assistants financiers de grade B3 et dix assistants de projet de grade B2).

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

Il est prévu de pourvoir quatre ou cinq autres postes dans les prochains mois. Cela porterait l'effectif total à 34, ce qui correspond à la capacité maximale gérable par le Bureau.

Le niveau d'expertise en matière de cybercriminalité et de preuve électronique au sein du Bureau a considérablement augmenté ces deux dernières années, ce qui non seulement contribue à améliorer encore la qualité des activités de projet, mais fait aussi du Bureau une source de connaissances spécialisées de grande valeur.

7.2 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.

- Les rémunérations de tous les agents – à l'exception du Chef du Bureau – sont couvertes par les budgets des projets dont ils ont la responsabilité[12].

[12] Le poste est financé par les frais généraux prévus dans le cadre des projets mis en œuvre par le C-PROC.

- 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 par rapport à Strasbourg. Entre avril 2014 et septembre 2018, des économies à hauteur de 2,5 millions EUR environ ont pu être réalisées au niveau des dépenses de personnel et 1,2 millions EUR au niveau des frais de fonctionnement, soit quelque 3,7 millions EUR au total.

La mise en œuvre de projets par le C-PROC est et restera rentable et donc attractive 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 dédié (www.coe.int/cybercrime), en contribuant à la communauté Octopus et à ses outils, en diffusant deux fois par mois un « condensé » des affaires de cybercriminalité et en publiant une lettre d'information trimestrielle Cybercrime@COE Update.

9 Conclusions et priorités

On peut tirer les conclusions suivantes :

- Grâce au Bureau de programme sur la cybercriminalité (C-PROC), le Conseil de l'Europe demeure un chef de file mondial en termes de renforcement des capacités de lutte contre la cybercriminalité et de collecte de preuves électroniques. Le C-PROC est une confirmation que le renforcement des capacités est un moyen efficace d'aider les sociétés, quelle que soit la région du monde, à relever le défi majeur de la cybercriminalité ;

- Les projets du C-PROC contribuent à la mise en œuvre et au suivi de la Convention de Budapest ou aux travaux du Comité de la Convention cybercriminalité. Le « triangle dynamique », qui conjugue normes communes (Convention de Budapest), suivi assuré par le T-CY et activités de renforcement de capacités menées par le C-PROC, est toujours très efficace. Étant donné les difficultés budgétaires que rencontre actuellement le Conseil de l'Europe, il est très appréciable que le T-CY s'appuie sur des contributions volontaires par le biais du projet Cybercrime@Octopus pour que la préparation du 2e Protocole additionnel à la Convention de Budapest puisse se poursuivre ;

- La Convention de Budapest fait partie des traités du Conseil de l'Europe présentant le plus d'États parties et dont la portée mondiale est la plus vaste[13]. Avec chaque nouvel État partie, la Convention de Budapest et la coopération internationale en matière de cybercriminalité gagnent en efficacité. Étant donné que tous les États membres du Conseil de l'Europe, sauf un, sont parties ou signataires, les nouvelles parties à la Convention seront nécessairement des États non membres. Entre octobre 2017 et septembre 2018, l'Argentine, le Cap-Vert, le Costa Rica, le Maroc, le Paraguay et les Philippines sont devenus parties à la Convention. Le Bureau contribue à s'assurer que les États qui sont parties à la Convention de Budapest ou qui pourraient le devenir ont la capacité d'appliquer ce traité ;

- Le C-PROC est l'un des bureaux externes du Conseil de l'Europe les plus performants en ce qui concerne la mobilisation des ressources. Le Bureau mène de multiples activités avec efficacité et à moindre coût, ce qui le rend attractif aux yeux des donateurs. En septembre 2018, des projets d'un montant de plus de 26 millions EUR étaient en cours de mise en œuvre ;

- L'Union européenne reste le principal donateur par le biais de projets conjoints cofinancés par le Conseil de l'Europe. Entre octobre 2017 et septembre 2018, des contributions volontaires ont en outre été reçues de l'Estonie, du Japon, de Monaco, du Royaume-Uni et, en particulier, des États-Unis pour le projet Cybercrime@Octopus ;

- Le Gouvernement roumain met gratuitement à disposition les locaux du Bureau, qu'il soutient aussi par son expertise. Le ministère de la Justice, la police nationale roumaine, les services de poursuite (DIICOT), l'école nationale de la magistrature et l'équipe d'intervention en cas d'urgence informatique 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) 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 projet sont menées en partenariat avec des organisations des secteurs public et privé ou font intervenir de telles organisations.

Le Bureau continuera à suivre la voie qui a produit de bons résultats et fait sentir ses effets, en partenariat avec d'autres organisations. Les priorités pour les douze mois à venir sont les suivantes :

[13] Elle n'est dépassée que par la Convention conjointe Conseil de l'Europe/OCDE concernant l'assistance administrative mutuelle en matière fiscale (STE n° 127) et par la Convention sur le transfèrement des personnes condamnées (STE n° 112).

- Mettre l'accent sur la sauvegarde des droits de l'homme et de l'État de droit : la cybercriminalité porte atteinte aux droits de l'homme, à la démocratie et à l'État de droit. Mais la lutte contre ce fléau comporte des risques. Les projets menés par le C-PROC contribuent à réduire ces risques et à renforcer les valeurs fondamentales dans toutes les régions du monde, notamment par l'élaboration de législations spécifiques qui prévoient des sauvegardes, par l'application de procédures normalisées et par la forte priorité accordée à la formation des juges. Le Bureau apportera de plus en plus son soutien au développement de la législation relative à la protection des données, en phase avec la nouvelle Convention STE n° 108 sur la protection des données et en coopération avec l'Unité de protection des données du Conseil de l'Europe ;

- Protéger les enfants contre les violences sexuelles en ligne et autres mesures de lutte contre la cyberviolence : un nouveau projet sur l'élimination de l'exploitation sexuelle des enfants « Mettre fin à l'exploitation et aux abus sexuels en ligne des enfants @Europe » a débuté au second semestre 2018, en coopération avec la Division des droits de l'enfant du Conseil de l'Europe et sur la base des normes de la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels. Ceci est un nouvel exemple des synergies qui existent au sein de l'Organisation. De plus, le C-PROC entreprendra la création de ressources en ligne sur la cyberviolence, comme convenu par le T-CY en juillet 2018[14] ;

- Mobiliser des ressources : l'actuel portefeuille de projets couvre les régions prioritaires d'Europe (région du Partenariat oriental, Europe du Sud-Est et Turquie) ainsi que des pays d'autres régions du monde qui se sont engagés à mettre en œuvre la Convention de Budapest. Certains de ces projets s'achèveront d'ici à quelques mois. Il sera nécessaire de concevoir et de négocier un nouveau projet régional conjoint sur la cybercriminalité pour le Partenariat oriental. Il en va de même pour la suite à donner au projet iPROCEEDS pour ce qui concerne l'Europe du Sud-Est. En outre, de nouveaux financements seront recherchés pour les activités au niveau mondial ;

- Renforcer l'expertise du Bureau : le rôle du C-PROC en tant que centre de connaissances spécialisées sera renforcé via la communauté Octopus et grâce à des supports de formation et à des rapports techniques. Aujourd'hui déjà, le Bureau est une source d'informations sur la législation en matière de cybercriminalité unique au monde. Pour atteindre l'objectif susmentionné, des actions de formation continue seront engagées pour les agents actuels du Bureau et des mesures seront prises pour attirer de futurs collaborateurs compétents.

Le Bureau est à la hauteur des attentes suscitées par sa création et les conditions de son développement sont réunies.

Il est proposé qu'il continue de fonctionner selon les modalités actuelles.

[14] Voir les recommandations de l'Étude de cartographie du T-CY sur la cyberviolence.

10 Annexe : Inventaire des activités soutenues par le C-PROC (octobre 2017 – septembre 2018)

Octobre 2017

Cybercrime@Octopus	CyFy 2017 : Conférence de l'Inde sur la cybersécurité et la gouvernance de l'internet, New Delhi, Inde, 3-4 octobre 2017
GLACY+	Participation de 2 délégués des Philippines à la table ronde Cybertipline, Alexandria, Virginie, États-Unis, 3-5 octobre 2017
iPROCEEDS	Atelier régional sur les lignes directrices et les indicateurs visant à prévenir et à dépister les produits de la criminalité en ligne, Ljubljana, Slovénie, 4-5 octobre 2017
CyberCrime@EAP III	Mémorandum de coopération : soutien au Forum sur la gouvernance de l'internet 2017 Ukraine, Kiev, Ukraine, 6 octobre 2017
CyberCrime@EAP II, iPROCEEDS	Conférence régionale sur la cybercriminalité, Bakou, Azerbaïdjan, 9-11 octobre 2017
GLACY+	Soutien à la dispense nationale du cours d'introduction sur la cybercriminalité et la preuve électronique pour les juges et les procureurs, Saint-Domingue, République dominicaine, 10-13 octobre 2017
CyberSud	Mission exploratoire en Tunisie, Tunis, Tunisie, 11 octobre 2017
GLACY+	Réunion avec les chefs des unités d'enquête sur la cybercriminalité de la région en vue d'échanger sur les activités et plans opérationnels et d'organiser une opération conjointe, Port-Louis, Maurice, 11-13 octobre 2017
CyberSud	Mission exploratoire en Algérie, Alger, Algérie, 12 octobre 2017
CyberCrime@EAP III	Mission de suivi en Azerbaïdjan sur diverses questions touchant à la coopération public/privé, Bakou, Azerbaïdjan, 12-13 octobre 2017
iPROCEEDS	Visite d'étude sur la réglementation et l'environnement opérationnel CSIRT/CERT, Bucarest, Roumanie, 12-13 octobre 2017
CyberCrime@EAP III	Soutien à la participation du Bélarus à la conférence CdE/OSCE sur la liberté sur internet, Vienne, Autriche, 13 octobre 2017
GLACY+	Atelier en résidence sur la cybercriminalité et la preuve électronique pour des juges de district et des juges locaux, Kandy, Sri Lanka, 13-15 octobre 2017
CyberCrime@EAP III	Mission de suivi en l'Arménie sur diverses questions touchant à la coopération public/privé, Erevan, Arménie, 16-17 octobre 2017

GLACY+	Mission consultative sur le signalement des cybercrimes et atelier sur la collecte et le suivi de statistiques de justice pénale sur la cybercriminalité et la preuve électronique, Saint-Domingue, République dominicaine, 16-17 octobre 2017
CyberSud	Mission exploratoire au Liban, Beyrouth, Liban, 17-18 octobre 2017
GLACY+	Conférence de l'ONUDC sur les réponses efficaces à l'exploitation sexuelle des enfants en ligne en Asie du Sud-Est, Bangkok, Thaïlande, 17-19 octobre 2017
CyberCrime@EAP III	Mission de suivi en Géorgie sur diverses questions touchant à la coopération public/privé, Tbilissi, Géorgie, 19-20 octobre 2017
CyberCrime@EAP III	Mission de suivi au Bélarus sur diverses questions touchant à la coopération public/privé, Minsk, Bélarus, 23-24 octobre 2017
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Tirana, Albanie, 23-24 octobre 2017 (première partie)
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Podgorica, Monténégro, 23-26 octobre 2017
GLACY+	Semaine de la cybersécurité (pour sensibiliser le public et lancer des initiatives en matière de cybersécurité), Accra, Ghana, 23-27 octobre 2017
CyberCrime@EAP II	Participation à l'assemblée générale de l'ECTEG sur l'accès aux documents et planning de formation pour le réseau 24/7 dans l'EAP, Lisbonne, Portugal, 26-27 octobre 2017
iPROCEEDS	Atelier sur la coopération interinstitutions et internationale en matière de dépistage, de saisie et de confiscation des produits du crime en ligne, Podgorica, Monténégro, 26-27 octobre 2017
GLACY+	Réunion générale annuelle de l'ICANN60, Abou Dabi, Émirats arabes unis, 28 octobre-3 novembre 2017
iPROCEEDS	Conseils et atelier sur l'élaboration des protocoles de coopération interinstitutions, Podgorica, Monténégro, 26 octobre 2017
iPROCEEDS	Atelier sur les protocoles nationaux de partage international du renseignement et des éléments de preuve, 27 octobre 2017
CyberCrime@EAP III, iPROCEEDS	4e Forum régional de l'Europe du Sud-Est sur la cybersécurité et la cybercriminalité, Sofia, Bulgarie, 30-31 octobre 2017
GLACY+	Réunions d'information GLACY+ avec la presse et le secteur public, Bucarest, Roumanie, 31 octobre 2017

Novembre 2017

CyberCrime@EAP III	Mission de suivi en République de Moldova sur diverses questions touchant à la coopération public/privé, Chisinau, République de Moldova, 2-3 novembre 2017
iPROCEEDS	Atelier régional sur la collecte et l'utilisation des preuves électroniques, Bucarest, Roumanie, 2-3 novembre 2017
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Tirana, Albanie, 6-7 novembre 2017 (deuxième partie)
CyberCrime@EAP III	Atelier sur les politiques et pratiques de conservation et d'archivage des données, Bakou, Azerbaïdjan, 6-7 novembre 2017
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Sarajevo, Bosnie-Herzégovine, 6-9 novembre 2017
GLACY+	Formation judiciaire avancée pour les juges, les magistrats et les procureurs, Accra, Ghana, 7-9 novembre 2017
GLACY+	Participation à la formation d'INTERPOL sur la cybercriminalité pour la région pacifique, Suva, Fidji, 6-10 novembre 2017
GLACY+	Mission consultative et atelier sur les politiques en matière de cybercriminalité – analyse du document de politique et de stratégie nationale en matière de cybersécurité, Accra, Ghana, 9-10 novembre 2017
CyberCrime@EAP III	Mission de suivi en l'Ukraine sur diverses questions touchant à la coopération public/privé, 13-14 novembre 2017, Kiev, Ukraine
iPROCEEDS	Exercice de coordination et de partenariat en matière de cybercriminalité, Pristina, Kosovo*[15], 13-16 novembre 2017
CyberSud	Visite d'évaluation en Tunisie, Tunis, Tunisie, 13-17 novembre 2017
CyberCrime@EAP III	Contribution à la manifestation cybersécurité et développement TIC organisée en Géorgie GITI 2017, Tbilissi, Géorgie, 16-17 novembre 2017
Cybercrime@Octopus	Participation à la 3e semaine nationale sur la cybersécurité, Mexique, 16-17 novembre 2017
GLACY+	Cours INTERPOL de formation des instructeurs, à Singapour, avec la participation de tous les pays du projet GLACY+, Singapour, 20-24 novembre 2017

[15] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

Cybercrime@Octopus	Forum mondial sur la cyberexpertise (GFCE), New Delhi, Inde, 21 novembre 2017
GLACY+	Participation à la deuxième réunion du Comité technique spécialisé en communication et technologies TIC composé des ministres de la Communication et des Technologies de l'information de la région Afrique, Addis Abeba, Éthiopie, 21 novembre 2017
Cybercrime@Octopus, GLACY+	Participation à la Conférence mondiale sur le cyberespace (GCCS2017), New Delhi, Inde, 23-24 novembre 2017
GLACY+, CyberCrime@EAP II, iPROCEEDS, Cybercrime@Octopus, CyberSud	18e réunion plénière du Comité de la Convention sur la cybercriminalité (T-CY) et 1re réunion plénière de rédaction du Protocole à la Convention, Strasbourg, France, 27-29 novembre 2017
CyberSud	Visite d'évaluation au Liban, Beyrouth, Liban, 27-30 novembre 2017
CyberSud	Participation au 3e Forum sur la lutte contre la cybercriminalité, Beyrouth, Liban, 29 novembre 2017
GLACY+	Comité directeur du projet GLACY+, Strasbourg, France, 30 novembre 2017

Décembre 2017

GLACY+	Forum sur les politiques de renforcement des capacités en matière de cybercriminalité par les organisations internationales/régionales – Amérique latine et Caraïbes, y compris l'atelier régional sur les stratégies en matière de cybercriminalité et de cybersécurité avec la participation d'organisations régionales Caraïbes/Amérique latine conjugué à un atelier sur la coopération internationale pour les pays d'Amérique latine et des Caraïbes, Saint-Domingue, République dominicaine, 5-7 décembre 2017
GLACY+	Soutien à la dispense, dans la région, d'un cours d'introduction sur la cybercriminalité et la preuve électronique pour les juges et les procureurs des pays anglophones de la région CEDEAO, Accra, Ghana, 5-8 décembre 2017
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Belgrade, Serbie, 4-7 décembre 2017
iPROCEEDS	Exercice de coordination et de partenariat sur la cybercriminalité, Belgrade, Serbie, 4-7 décembre 2017
CyberSud	Visite d'évaluation en Algérie, Alger, Algérie, 10-14 décembre 2017
iPROCEEDS	Examen du 2e semestre 2017, programme de Master en informatique forensique et investigation en matière de cybercriminalité, Dublin, Irlande, 11-15 décembre 2017

GLACY+	Atelier international sur les stratégies de formation des magistrats, avec la participation de tous les pays du projet GLACY+ et de tous les pays de l'ASEAN, Cebu, Philippines, 12-14 décembre 2017
GLACY+	Conférence annuelle des juges de district et juges locaux sri lankais, Colombo, Sri Lanka, 18-19 décembre 2017
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Ankara, Turquie, 18-20 décembre 2017
iPROCEEDS	Atelier régional sur la mise en commun de bonnes pratiques sur les mécanismes de signalement en Europe du Sud-Est et en Turquie, Skopje, « l'ex-République yougoslave de Macédoine », 20 décembre 2017
iPROCEEDS	4e réunion du comité directeur du projet iPROCEEDS, Skopje, « l'ex-République yougoslave de Macédoine », 21 décembre 2017
Cybercrime@Octopus	Participation à l'atelier (WS149) « Crime et juridiction dans le cyberespace – des solutions en perspective » au cours du FGI 2017, Genève, Suisse, 20 décembre 2017

Janvier 2018

iPROCEEDS	Exercice de simulation de cas sur la cybercriminalité et les investigations financières, Sarajevo, Bosnie-Herzégovine, 15-18 janvier 2018
GLACY+	Mission consultative sur l'harmonisation de la législation sur la cybercriminalité et la preuve électronique, Kampala, Ouganda, 16-18 janvier 2018
iPROCEEDS	Réunion du groupe de travail pour élaborer/améliorer les lignes directrices et les indicateurs visant à aider les entités du secteur financier à prévenir le blanchiment de capitaux dans l'environnement en ligne, Pristina, Kosovo*[16], 18 janvier 2018
GLACY+	Mission consultative sur l'harmonisation de la législation sur la cybercriminalité et la preuve électronique, Port-Louis, Maurice, 22-24 janvier 2018
GLACY+	Mission consultative sur la normalisation des procédures d'entraide juridique concernant la cybercriminalité et la preuve électronique, Port-Louis, Maurice, 25-26 janvier 2018
iPROCEEDS	Réunion de MASAK avec des sociétés de monnaie électronique sur les lignes directrices et les indicateurs visant à aider les entités du secteur financier à prévenir le blanchiment de capitaux dans l'environnement en ligne, Ankara, Turquie, 30 janvier 2018

[16] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

Février 2018

GLACY+	Première réunion annuelle et conférence internationale du réseau cyber ibéro-américain avec la participation de points de contact du forum cybercriminalité des pays africains de langue officielle portugaise, Lisbonne, Portugal, 5-7 février 2018
Cybercrime@Octopus	Table ronde de haut niveau sur la Convention de Budapest en Malaisie, Kuala Lumpur, Malaisie, 6-7 février 2018
CyberCrime@EAP 2018	Atelier sur les menaces en matière de cybercriminalité, les stratégies et les nouveautés des ressources en ligne, Erevan, Arménie, 6-8 février 2018
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne à destination des juges et des procureurs, Pristina, Kosovo*[17], 7-10 février 2018
Cybercrime@Octopus	Participation à la réunion du groupe d'experts sur l'accès licite aux données numériques par-delà les frontières, Vienne, Autriche, 12-13 février 2018
GLACY+	Participation à la réunion intersessions du groupe de travail sur la sécurité publique, Bruxelles, Belgique, 12-13 février 2018
iPROCEEDS	Réunion sur la coopération public/privé pour lutter contre la cybercriminalité et les produits de la criminalité en ligne, Podgorica, Monténégro, 13 février 2018
CyberCrime@EAP 2018	Atelier sur les menaces en matière de cybercriminalité, les stratégies et les nouveautés des ressources en ligne, Bakou, Azerbaïdjan, 13-15 février 2018
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne (1re partie), Skopje, « l'ex-République yougoslave de Macédoine », 15-16 février 2018
CyberSud	Formation de base sur la cybercriminalité et la preuve électronique pour magistrats, Beyrouth, Liban, 16 février 2018
GLACY+	Mission consultative sur la création de la division cybercriminalité au CID de la police sri lankaise, Colombo, Sri Lanka, 19-21 février 2018
Cybercrime@Octopus	Cours à distance sur les drogues organisé par la direction centrale des services antidrogues et l'université interinstitutions des études avancées pour les agents des services de répression, Rome, Italie, 19-22 février 2018

[17] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

CyberSud	Réunion du mécanisme de suivi, de signalement et de soutien dans la lutte contre le terrorisme (CT Morse), Bruxelles, Belgique, 20 février 2018

iPROCEEDS	Réunion MASAK avec les sociétés d'échange de monnaie virtuelle sur les lignes directrices et les indicateurs visant à aider les entités du secteur financier à prévenir le blanchiment de capitaux dans l'environnement en ligne, Ankara, Turquie, 22 février 2018
CyberCrime@EAP 2018	Atelier sur les menaces en matière de cybercriminalité, les stratégies et les nouveautés des ressources en ligne, Tbilissi, Géorgie, 20-22 février 2018
CyberCrime@EAP 2018	Atelier sur les aspects juridiques et pratiques de la coopération entre les services de répression et les fournisseurs de services internet, Chisinau, République de Moldova, 26-27 février 2018
Cybercrime@Octopus	Participation à la conférence mondiale internet et juridiction, Ottawa, Canada, 26-28 février 2018
GLACY+	Mission consultative sur l'harmonisation de la législation en matière de cybercriminalité et de preuve électronique au Népal, Katmandou, Népal, 26-28 février 2018
GLACY+	Formation judiciaire de base sur la cybercriminalité et la preuve numérique pour la Police Judiciaire, Kenitra, Maroc, 27 février-2 mars 2018
CyberSud	Conférence du partenariat EuroMed sur la justice, Bruxelles, Belgique, 28 février 2018
CyberCrime@EAP 2018	Atelier sur les menaces en matière de cybercriminalité, les stratégies et les nouveautés des ressources en ligne, Chisinau, République de Moldova, 28 février-2 mars 2018
Cybercrime@Octopus	Rédaction d'un Protocole additionnel à la Convention de Budapest, finalisation et présentation du rapport du T-CY sur la cyberviolence, février-décembre 2018

Mars 2018

CyberSud	Atelier sur les réponses à apporter au problème de la cybercriminalité, Amman-Tareq, Jordanie, 5 mars 2018
GLACY+	Conférence « Priorité sur les données », Jakarta et Surabaya, Indonésie, 5-8 mars 2018
iPROCEEDS	Module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne (2e partie), Skopje, « l'ex-République yougoslave de Macédoine », 5-6 mars 2018

CyberSud CyberCrime@EAP 2018, GLACY+ iPROCEEDS	Conférence internationale sur la coopération judiciaire dans les affaires de cybercriminalité, La Haye, Pays-Bas, 7-8 mars 2018
GLACY+	Réunion d'analyse technique du projet de loi relative aux droits numériques et à la liberté, Uyo, État Akwa Ibom, Nigéria, 8-10 mars 2018
iPROCEEDS	Réunion de MASAK avec des sociétés de monnaie électronique sur les lignes directrices et les indicateurs visant à aider les entités du secteur financier à prévenir le blanchiment de capitaux dans l'environnement en ligne, Ankara, Turquie, 9 mars 2018
GLACY+	Participation au Forum de la communauté ICANN 61, San Juan, Puerto Rico, 10-15 mars 2018
GLACY+	Réunion avec des chefs d'unité responsables des investigations en matière de cybercriminalité de la région pour discuter des activités opérationnelles et programmer et organiser une opération conjointe, Hong Kong, 12-16 mars 2018
GLACY+	Mission consultative pour l'élaboration de la législation en matière de cybercriminalité et de preuve électronique, Ouagadougou, Burkina Faso, 12-15 mars 2018
GLACY+	Atelier sur la cybercriminalité et la cybersécurité pour les pays membres de l'initiative de la baie du Bengale pour la coopération technique et économique multisectorielle (BIMSTEK), Bangladesh, 13-15 mars 2018
iPROCEEDS	2e réunion du conseil du projet Gouvernance de la sécurité interne et intégrative (IISG) dans les Balkans occidentaux, Ljubljana, Slovénie, 15-16 mars 2018
GLACY+	Atelier en résidence sur la cybercriminalité et la preuve électronique pour les juges de district et les juges locaux, Colombo, Sri Lanka, 16-18 mars 2018
iPROCEEDS	Participation à la 2e conférence sur la cybersécurité, Sarajevo, Bosnie-Herzégovine, 20 mars 2018
GLACY+	Participation à l'assemblée générale de l'ECTEG et à la manifestation de démonstration de FREETOOL, La Haye, Pays-Bas, 20-22 mars 2018
GLACY+	Cours initial de la formation d'instructeurs sur la cybercriminalité et la preuve électronique pour les juges, les magistrats et les procureurs de la région ASEAN, Manille, Philippines, 20-23 mars 2018
CyberSud	Conférence de lancement de projet, Tunis, Tunisie, 21-23 mars 2018
iPROCEEDS	Atelier sur la fraude financière et la fraude à la carte de crédit en ligne, Sarajevo, Bosnie-Herzégovine, 21-22 mars 2018

Cybercrime@Octopus	Mise au point d'une étude sur la législation pour le Koweït, 23 mars 2018
GLACY+	Atelier sur la normalisation des procédures d'entraide judiciaire en matière de cybercriminalité et de preuve électronique, Dakar, Sénégal, 26-27 mars 2018
CyberCrime@EAP 2018 GLACY+	2e exercice régional de coopération sur la cybercriminalité, Chisinau, République de Moldova, 27-30 mars 2018

Avril 2018

GLACY+ CyberCrime@EAP 2018 iPROCEEDS Cybercrime@Octopus CyberSud	Réunion du Groupe d'experts intergouvernemental des Nations Unies sur la cybercriminalité, Vienne, Autriche, 3-7 avril 2018
iPROCEEDS GLACY+ CyberCrime@EAP 2018 CyberSud	Réunion du Groupe de rédaction du protocole du T-CY, Vienne, Autriche, 6-7 avril 2018
CyberSud	11e réunion du groupe de travail du Moyen-Orient et de l'Afrique du Nord sur la cybercriminalité pour les chefs d'unité, Alger, Algérie, 4-5 avril 2018
GLACY+	Intégration des supports de formation de l'ECTEG dans les instituts de formation de la police et d'autres organes de formation des services de répression professionnels, Colombo, Sri Lanka, 4-6 avril 2018
iPROCEEDS	Réunion du groupe de travail chargé d'élaborer/améliorer les lignes directrices et les indicateurs visant à aider les entités du secteur financier à prévenir le blanchiment de capitaux dans l'environnement en ligne, Pristina, Kosovo*[18], 5 avril 2018
iPROCEEDS	Réunion du groupe de travail chargé d'élaborer/améliorer les lignes directrices et les indicateurs visant à aider les entités du secteur financier à prévenir le blanchiment de capitaux dans l'environnement en ligne, Skopje, « l'ex-République yougoslave de Macédoine », 11 avril 2018
GLACY+	Politiques de cybersécurité et de lutte contre la cybercriminalité pour les diplomates africains, Addis Abeba, Éthiopie, 11-13 avril 2018

[18] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

CyberCrime@EAP 2018	Atelier sur les menaces de cybersécurité, les stratégies, les accords de coopération et les ressources en ligne, Kiev, Ukraine, 11-13 avril 2018
GLACY+	Première visite d'évaluation au Chili, Santiago, Chili, 16-19 avril 2018
iPROCEEDS	Exercice de simulation de cas sur la cybercriminalité et les investigations financières, Tirana, Albanie, 16-19 avril 2018
GLACY+	Intégration des documents de l'ECTEG dans la stratégie de formation des agents des services de répression, Accra, Ghana, 18-20 avril 2018
CyberCrime@EAP 2018	Réunion du Groupe de travail sur la cybercriminalité au Groupe Pompidou, Dublin, Irlande, 18-19 avril 2018
iPROCEEDS	2e dispense nationale du module de formation initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Podgorica, Monténégro, 19-20 avril 2018 (1re partie) et 17-18 mai 2018 (2e partie)
CyberCrime@EAP 2018	2e festival de la cybersécurité organisé par l'Initiative de développement de l'internet et l'Université de Géorgie, Tbilissi, Géorgie, 20 avril 2018
CyberSud	Participation à la 1re conférence EuroMed sur la preuve numérique, Lisbonne, Portugal, 23-25 avril 2018
GLACY+	Première visite d'évaluation au Nigéria, Abuja, Nigéria, 24-27 avril 2018
CyberCrime@EAP 2018	Mission consultative sur les points de contact du réseau 24/7 – fonctions et structure institutionnelle, Erevan, Arménie, 25-26 avril 2018

Mai 2018

GLACY+	Mission consultative sur l'harmonisation de la législation sur la cybercriminalité et la preuve électronique, Banjul, Gambie, 2-4 mai 2018
iPROCEEDS CyberCrime@EAP 2018	Réunion régionale sur la coopération internationale en matière de cybercriminalité et de preuve électronique, Kiev, Ukraine, 3-4 mai 2018
GLACY+	Formation régionale des formateurs sur la cybercriminalité et la preuve électronique pour les premiers intervenants des forces de l'ordre, Dakar, Sénégal, 7–11 mai 2018
Cybercrime@Octopus	Cours à distance sur les drogues organisé par la direction centrale des services antidrogues (C.D.A.S.) et l'université interinstitutions des études avancées pour les agents des services de répression, Rome, Italie, 7-11 mai 2018
CyberSud	Visite d'étude d'unités spécialisées sur la cybercriminalité au Liban, Beyrouth, Liban, 7-10 mai 2018
CyberSud	Mission consultative conjointe chargée d'analyser les capacités des forces de sécurité intérieures, Beyrouth, Liban, 8-11 mai 2018

GLACY+	Cours d'introduction en résidence sur la cybercriminalité et la preuve électronique pour les procureurs et les juges, Cebu, Philippines, 8-10 mai 2018
GLACY+	Réunion INTERPOL avec les chefs d'unité responsables des investigations de cybercriminalité de la région en vue d'examiner les activités opérationnelles, de programmer et d'organiser une opération conjointe, Téhéran, Iran, 8-10 mai 2018
iPROCEEDS	Soutien à la participation au Master en informatique forensique et investigations de cybercriminalité, Université de Dublin, session d'examen du 3e semestre, Dublin, Irlande, 8-12 mai 2018
CyberSud	Conférence CyFy Africa 2018, Tanger, Maroc, 10-12 mai 2018
GLACY+	Conférence sur la Convention de Budapest, programme de Master en cybersécurité, Université LUISS, Rome, Italie, 11 mai 2018
GLACY+	Comité directeur du projet GLACY+, Vienne, Autriche, 14 mai 2018
CyberSud	Formation judiciaire de base sur la cybercriminalité et la preuve électronique, Rabat, Maroc, 14-17 mai 2018
GLACY+ CyberCrime@EAP 2018 iPROCEEDS Cybercrime@Octopus CyberSud	Participation à la 27e session de la Commission des Nations Unies pour la prévention du crime et la justice pénale « Mesures de justice pénale propres à prévenir et à combattre la cybercriminalité sous toutes ses formes, y compris par le renforcement de la coopération aux niveaux national et international », Vienne, Autriche, 14-18 mai 2018 Activité parallèle sur l'état de la législation relative à la cybercriminalité (Conseil de l'Europe en partenariat avec les Gouvernements de l'Argentine, du Portugal, de la Roumanie, du Royaume-Uni et du Sri Lanka, et de l'Union européenne), Vienne, Autriche, 15 mai 2018
iPROCEEDS GLACY+ CyberCrime@EAP 2018 CyberSud	Réunion du groupe de rédaction du protocole du T-CY, Vienne, Autriche, 11-13 mai 2018
iPROCEEDS	Atelier régional sur les statistiques de justice pénale sur la cybercriminalité et la preuve électronique, Bucarest, Roumanie, 14-15 mai 2018
iPROCEEDS	Exercice de simulation de cas sur la cybercriminalité et les investigations financières, Ankara, Turquie, 21-24 mai 2018
GLACY+	Première visite d'évaluation au Costa Rica, San José, Costa Rica, 21-24 mai 2018
CyberCrime@EAP 2018	Atelier sur les menaces en matière de cybercriminalité, les stratégies et les ressources en ligne, Minsk, Bélarus, 22-24 mai 2018

iPROCEEDS	2e dispense nationale du module de formation judiciaire initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Tirana, Albanie, 30-31 mai 2018 (1re partie)
GLACY+	Analyse documentaire du projet de loi sur la cybercriminalité au Brésil, mai-juin 2018

Juin 2018

CyberCrime@EAP 2018	Comité directeur et participation au dialogue EuroDIG 2018, Tbilissi, Géorgie, 4-6 juin 2018
CyberSud	Visite d'évaluation en Jordanie, Amman, Jordanie, 4-6 juin 2018
GLACY+	Visite d'évaluation initiale au Cap-Vert, Praia, Cap-Vert, 4-7 juin 2018
GLACY+	Formation sur la cybercriminalité organisée par la police italienne, Naples, Italie, 4-15 juin 2018
iPROCEEDS CyberCrime@EAP 2018	Dialogue européen sur la gouvernance de l'internet (EuroDIG) 2018, Tbilissi, Géorgie, 5-6 juin 2017
iPROCEEDS	Participation à la 3e conférence internationale « Cybercriminalité : tendances et menaces – l'Europe et les dimensions internationales », Nicosie, Chypre, 11-12 juin 2018
GLACY+	Formation de l'ECTEG, formation spécialisée en cybercriminalité et analyse forensique pour les agents des forces de répression (analyse forensique de données volatiles), Saint-Domingue, République dominicaine, 11-15 juin 2018
CyberCrime@EAP 2018	Contribution à la réunion du comité directeur du plan d'action de l'Arménie, Erevan, Arménie, 12 juin 2018
GLACY+	Réunion régionale de soutien entre pays concernés et organisations internationales/régionales – 2e atelier annuel sur la cybercriminalité PILON : lutter contre la maltraitance enfantine en ligne dans le Pacifique, Nuku'Alofa, Tonga, 12-15 juin 2018
iPROCEEDS	2e dispense nationale du module de formation judiciaire initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Belgrade, Serbie, 12-15 juin 2018
GLACY+	Cours INTERPOL de formation des instructeurs, Singapour, 18-22 juin 2018
Cybercrime@Octopus	Cybercriminalité et preuve numérique, Paris, 18-22 juin 2018
iPROCEEDS	2e dispense nationale du module de formation judiciaire initiale sur la cybercriminalité, la preuve électronique et les produits de la criminalité en ligne, Tirana, Albanie, 18-19 juin 2018 (2e partie)

GLACY+	Formation judiciaire avancée sur la cybercriminalité et la preuve électronique pour les juges, les magistrats et les procureurs de la région ASEAN, Cebu, Philippines, 19-22 juin 2018
CyberCrime@EAP 2018	Mission consultative sur la coopération internationale par l'intermédiaire des points de contact du réseau 24/7 et entraide judiciaire, Bakou, Azerbaïdjan, 19-21 juin 2018
CyberSud	Réunion de coordination CEPOL, Budapest, Hongrie, 26 juin 2018
GLACY+	Atelier national sur la protection des données et les outils et services INTERPOL, Saint-Domingue, République dominicaine, 26-28 juin 2018
GLACY+	3e réunion du groupe d'experts d'INTERPOL sur l'analyse forensique numérique, Heathrow, Royaume-Uni, 27-29 juin 2018
GLACY+	Participation à la réunion du groupe de travail A du forum GFCE – politique et stratégie de cybersécurité, La Haye, Pays-Bas, 28 juin 2018
Cybercrime@Octopus	Colloque à la Cour de cassation, Le droit pénal international face à la cybercriminalité, Paris, 28 juin 2018

Juillet 2018

Cybercrime@Octopus GLACY+	Mission de consultation sur la législation en matière de cybercriminalité à Samoa et phase 1 – Formation des parties prenantes, Apia, Samoa, 2-3 juillet 2018
GLACY+	Atelier sur la cybercriminalité et la preuve électronique pour les juges et les magistrats, Apia, Samoa, 4-6 juillet 2018
CyberCrime@EAP 2018 CyberSud GLACY+	19e réunion plénière du Comité de la Convention sur la cybercriminalité et 2e réunion plénière de rédaction du Protocole, Strasbourg, France, 9-11 juillet 20118
iPROCEEDS	Formation de l'ECTEG sur l'analyse forensique des données volatiles, Pristina, Kosovo*[19], 9-13 juillet 2018
Cybercrime@Octopus iPROCEEDS	Réunion du Réseau des points de contact 24/7 de la Convention de Budapest sur la cybercriminalité, Strasbourg, France, 11 juillet 2018
Cybercrime@Octopus iPROCEEDS CyberSud	Conférence Octopus 2018 sur la coopération contre la cybercriminalité, Strasbourg, France, 11-13 juillet 2013
GLACY+	Visite du procureur général du Népal à Eurojust et en Belgique, La Haye, Pays-Bas, Bruxelles et Mechelen, Belgique, 16-20 juillet 2018

[19] * Toute référence au Kosovo dans le présent texte, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo.

GLACY+	Formation judiciaire avancée sur la cybercriminalité et la preuve électronique pour les juges, les procureurs et les avocats avec la participation des pays anglophones de la région CEDEAO, Ghana, 17-20 juillet 2018
GLACY+	Université d'été sur la cybersécurité organisée par l'OEA et l'INCIBE, en collaboration avec INTERPOL, EUROPOL et FIRST, Leon, Espagne, 17-28 juillet 2018
iPROCEEDS	1re réunion préparatoire d'élaboration d'un scénario d'exercice sur la cybercriminalité (C-PROC et consultants), Bucarest, Roumanie, 23-25 juillet 2018
GLACY+	Intégration des supports de formation de l'ECTEG dans les instituts de formation de la police et d'autres organes de formation des services de répression professionnels, Port-Louis, Maurice, 30 juillet-1er août 2018
CyberSud	Adaptation de la formation judiciaire, Strasbourg, France, 30 juillet-3 août 2018

Août 2018

GLACY+	Programme spécial sur la cybercriminalité et la preuve électronique pour les juges de la Cour suprême, Port-Louis, Maurice, 1er-3 août 2018
Cybercrime@Octopus	Analyse comparative du cadre juridique du Qatar, août 2018
GLACY+	Cours de l'ECTEG, formation spécialisée en cybercriminalité et analyse forensique numérique pour les agents des services de répression, Manille, Philippines, 13-18 août 2018
GLACY+	Cours de l'ECTEG, formation spécialisée en cybercriminalité et analyse forensique numérique pour les agents des services de répression, Nuku'alofa, Tonga, 20-24 août 2018
GLACY+	Mission consultative sur la législation de Vanuatu en matière de cybercriminalité, élaboration/révision du cadre juridique sur la cybercriminalité et la preuve électronique, et atelier de sensibilisation à la Convention de Budapest, Vanuatu, 20-24 août 2018
CyberSud	Mission consultative sur les points de contact du réseau 24/7, Tunis, Tunisie, 27 août 2018
GLACY+	Formation judiciaire avancée sur la cybercriminalité et la preuve électronique pour les juges, les procureurs et autres officiers de justice de la région Pacifique, Nuku'alofa, Tonga, 27-30 août 2018
GLACY+	Atelier international conjoint pour les unités d'investigation en cybercriminalité et les autorités centrales d'entraide judiciaire, Singapour, 27-31 août 2018

Cybercrime@Octopus	Symposium international sur la réponse à donner à la cybercriminalité, Séoul, République de Corée, 29-31 août 2018
CyberSud	Mission consultative en vue d'un atelier d'experts destiné à examiner les possibilités d'adoption d'une stratégie de cybersécurité, Aramoun, Liban, 29-30 août 2018
GLACY+	Intégration/normalisation des modules de formation sur la cybercriminalité et la preuve électronique dans le programme de formation judiciaire des instituts de formation, Nuku'alofa, Tonga, 30 août 2018
Cybercrime@Octopus GLACY+	Activités de soutien au 11e sommet de l'Inde sur la sécurité, New Delhi, 31 août 2018

Septembre 2018

CyberSud	Réunion de sensibilisation à la Convention de Budapest et à ses instruments, Alger, Algérie, 2 septembre 2018
CyberCrime@EAP 2018 GLACY+ iPROCEEDS CyberSud	Conférence sur l'économie souterraine 2018, Strasbourg, France, 4-7 septembre 2018
GLACY+	Participation à la 4e réunion du groupe de travail INTERPOL des Amériques sur la cybercriminalité pour les chefs d'unité, Rio de Janeiro, Brésil, 4-6 septembre 2018
CyberSud	Réunion de sensibilisation à la Convention de Budapest et à ses instruments, Tunis, Tunisie, 6-7 septembre 2018
GLACY+	Atelier en résidence sur la rédaction de la législation de protection des données, Calabar, Nigéria, 10-14 septembre 2018
CyberCrime@EAP 2018	Exercice sur table de coopération internationale en matière de cybercriminalité, Erevan, Arménie, 10-11 septembre 2018
iPROCEEDS	Réunion sur la coopération public/privé pour la lutte contre la cybercriminalité et les produits de la criminalité en ligne, district de Brcko, Bosnie-Herzégovine, 11 septembre 2018
CyberSud	Formation judiciaire de base, Beyrouth, Liban, 11-15 septembre 2018
Cybercrime@Octopus	Réunion informelle du groupe d'États G77 sur la cybercriminalité, Vienne, Autriche, 11-12 septembre 2018
iPROCEEDS	Réunion sur la coopération public/privé pour la lutte contre la cybercriminalité et les produits de la criminalité en ligne, Banja Luka, Republika Srpska, Bosnie-Herzégovine, 12 septembre 2018

CyberSud	Réunion de l'ECTEG sur la formation des premiers intervenants, Bruxelles, Belgique, 13 septembre 2018
CyberCrime@EAP 2018	Exercice sur table sur la coopération internationale en matière de cybercriminalité, Bakou, Azerbaïdjan, 13-14 septembre 2018
Cybercrime@Octopus	Groupe de rédaction du Protocole du T-CY, Strasbourg, France, 17-19 septembre 2018
CyberSud	Visite d'étude de l'unité cybercriminalité, de l'unité forensique et de l'équipe CERT, Bucarest, Roumanie, 17-18 septembre 2018
GLACY+ iPROCEEDS CyberSud CyberCrime@EAP 2018	Réunion des chefs des unités cybercriminalité et/ou des départements investigation criminelle en vue de la mise en commun des expériences avec d'autres pays dans le cadre du projet. Participation à la 6e conférence INTERPOL-EUROPOL sur la cybercriminalité, Singapour, 18-20 septembre 2018
iPROCEEDS	Participation à la Conférence ministérielle régionale sur la criminalité de haute technologie et la sécurité de l'information « Connect securely! », Belgrade, Serbie, 20-21 septembre 2018
CyberSud	Formation judiciaire de base, Alger, Algérie, 23-27 septembre 2018
GLACY+	Participation à la Conférence judiciaire du Pacifique, Apia, Samoa, 24 septembre 2018
CyberCrime@EAP 2018	Atelier sur les services de répression et la coopération CSIRT/CERT en matière de cybercriminalité, Kiev, Ukraine, 24-26 septembre 2018
iPROCEEDS	2e réunion préparatoire chargée de finaliser le scénario de l'exercice cybercriminalité (C-PROC, consultants), Bucarest, Roumanie, 24-26 septembre 2018
GLACY+	Mission consultative sur la législation en matière de cybercriminalité pour le Chili, en coopération avec l'OEA, Washington D.C., États-Unis, 24-26 septembre 2018
GLACY+	Conférence du Nigéria sur la cybercriminalité et la preuve électronique (NaCCEE, 2018), Abuja, Nigéria, 26-28 septembre 2018
GLACY+	Participation à la réunion bisannuelle du réseau des politiques publiques dans le Pacifique, organisée par la police fédérale australienne, Fidji, 26-28 septembre 2018
GLACY+	Forum sur la liberté sur internet en Afrique (FIFAfrica), Accra, Ghana, 26-28 septembre 2018
CyberCrime@EAP 2018	Activités de soutien au Forum sur la gouvernance de l'internet (FGI) et à Jeunesse FGI 2018 Ukraine, Kiev, Ukraine, 27-28 septembre 2018
CyberSud	Réunion de l'OSCE, Rome, Italie, 27-28 septembre 2018