Documents d'information

SG/Inf(2025)11

29 avril 2025

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

Rapport d'activité du C-PROC pour 2024

Table des matières

1. Cadre et objet du présent rapport 6
2. Contexte : développements pertinents en 2024 6
État d'avancement des adhésions à la Convention sur la cybercriminalité 6
Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques 7
Processus d'élaboration du traité des Nations Unies 7
Décisions du T-CY concernant l'intelligence artificielle et les actifs virtuels 8
Nouveaux projets de renforcement des capacités 8
3. Aperçu des projets et réalisations en 2024 9
Projets 9
Réalisations 11
Capacités en matière de justice pénale 11
Outils et ressources 18
Partenariats et synergies 19
Soutien au Comité de la Convention cybercriminalité (T-CY) 20
Intégration de la dimension de genre dans le renforcement des capacités en matière de cybercriminalité et de preuves électroniques 21
4. Conclusions et perspectives 22

Annexe : Inventaire des activités du C-PROC 2014-2024 (en ligne) (disponible en anglais uniquement)

Résumé

Le Bureau du programme sur la cybercriminalité du Conseil de l'Europe (« C-PROC » ou le « Bureau ») situé à Bucarest en Roumanie est chargé d'assurer la mise en œuvre des projets de renforcement des capacités en matière de cybercriminalité et de preuves électroniques, sur la base de la Convention de Budapest sur la cybercriminalité, et ce dans toutes les régions du monde. Le Bureau est opérationnel depuis 2014, par suite d'une décision du Comité des Ministres de 2013. Le présent rapport a pour objet d'informer le Comité des Ministres des activités menées par le C-PROC en 2024.

En 2024, grâce au C-PROC, le Conseil de l'Europe est resté un acteur de premier plan au niveau mondial en matière de renforcement des capacités et de conseils législatifs sur la cybercriminalité. Plusieurs projets de renforcement des capacités ont été clôturés fin 2023 et cinq nouveaux projets ont été lancés entre janvier et mars 2024. La même année, le C-PROC a ainsi géré sept projets pour un budget cumulé de plus de 34 millions d'euros et soutenu plus de 310 activités de renforcement des capacités dans des régions du monde entier. Depuis sa création il y a onze ans, le C-PROC a accompagné plus de 2 400 activités dans 140 pays. Entre 2013 et 2024, le nombre de pays dotés d'un droit pénal matériel conforme à la Convention sur la cybercriminalité est passé de 70 à 132. Les activités du C-PROC ont aussi largement contribué à l'élargissement de la portée de la Convention et à l'augmentation des adhésions (de 41 États parties en 2013 à 77 à la fin de l'année 2024). Le travail du C-PROC est essentiel au rayonnement mondial du Conseil de l'Europe.

En décembre 2024, le C-PROC employait 54 personnes, y compris — pour la première fois — du personnel basé dans d'autres bureaux du Conseil de l'Europe, notamment à Kiev et à Pristina.

Le principal donateur restait l'Union européenne, qui a contribué à cinq projets conjoints. Les États-Unis, la France, le Japon et le Royaume-Uni ont versé des contributions volontaires au projet Octopus et plusieurs États membres du Conseil de l'Europe — dans le cadre du Plan d'action pour l'Ukraine — ont contribué au renforcement des capacités en matière de preuves électroniques des crimes de guerre en Ukraine.

Les nombreux audits, évaluations et exercices similaires, dont un audit du C-PROC mené par la Direction de l'Audit interne, de l'Évaluation et de l'Investigation (DIO) en 2024, ont confirmé sa gestion des risques et ses contrôles internes, ainsi que sa capacité à respecter ses obligations contractuelles envers les donateurs.

Faits marquants de l'année 2024 concernant le C-PROC :

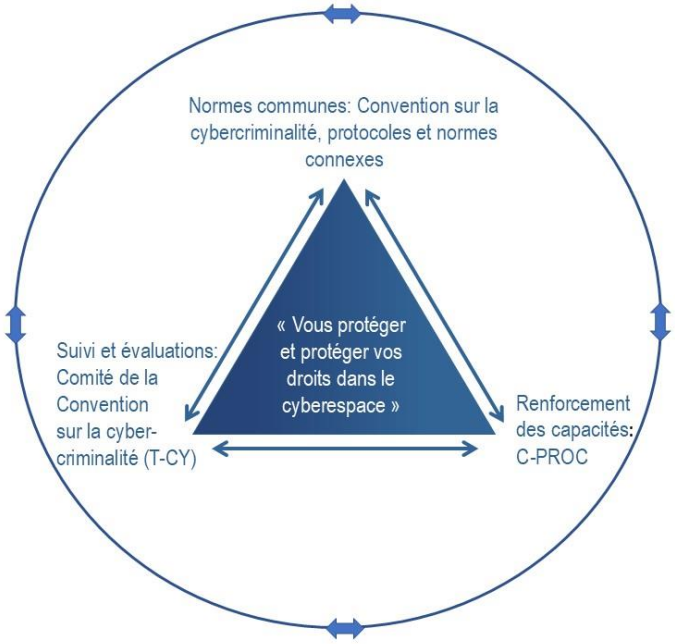
- l'adhésion à la Convention sur la cybercriminalité suscite un intérêt de plus en plus grand. En 2024, le Bénin, la Côte d'Ivoire, l'Équateur, les Fidji, la Grenade, Kiribati, la Sierra Leone et la Tunisie sont devenus parties à la Convention, portant le nombre total de parties à 77. Par ailleurs, le Kenya, le Malawi, le Mozambique et la Papouasie-Nouvelle-Guinée ont été invités à y adhérer. Le nombre croissant d'adhésions à la Convention et la nécessité de relever de nouveaux défis (liés à l'intelligence artificielle, aux rançongiciels, aux actifs virtuels, etc.) entraînent une forte augmentation des demandes de renforcement des capacités ;

- plusieurs Parties ont lancé des réformes juridiques visant à appliquer le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques. Ce Protocole est essentiel, à la fois pour promouvoir l'État de droit dans le cyberespace et pour que la Convention conserve sa pertinence. Soutenir son application et sa ratification sera une priorité pour le C-PROC ;

- l'adoption par l'Assemblée générale des Nations Unies d'un nouveau traité international contre la cybercriminalité en décembre 2024 : le Conseil de l'Europe, par l'intermédiaire du C-PROC et du Comité de la Convention sur la cybercriminalité, a participé aux négociations sur ce nouveau traité entre 2022 et 2024. Bien que largement conforme à la Convention sur la cybercriminalité, et même si celle-ci demeurera le cadre international de référence dans un avenir proche, ce nouveau traité soulève un certain nombre de questions, y compris en ce qui concerne le renforcement des capacités et le rôle du C-PROC.

Le C-PROC entend préparer l'avenir et faire en sorte que le Conseil de l'Europe reste un acteur de premier plan au niveau mondial en termes de renforcement des capacités pour la lutte contre la cybercriminalité. Pour ce faire :

- il s'appuiera sur les facteurs qui ont fait son succès entre 2014 et 2024 (portée mondiale de ses activités ; pleine application du « triangle dynamique » — normes communes, évaluations et renforcement des capacités ; bureau dédié et personnel spécialisé ; développement de projets et recherche de partenariats financiers ; gestion saine et efficace des ressources) ;



- il adaptera ses domaines d'intervention prioritaires (soutenir en priorité l'application du Deuxième Protocole additionnel ; aider les pays à appliquer la nouvelle Convention des Nations Unies contre la cybercriminalité, s'il y a lieu ; renforcer les activités relatives à la protection des enfants en ligne et à la diffusion non consentie d'images intimes ; continuer à lutter contre l'utilisation d'actifs virtuels à des fins criminelles ; élaborer une approche systématique du renforcement des capacités en matière de cybercriminalité, de preuves électroniques et d'intelligence artificielle) ;

- il intensifiera ses activités (multiplication des partenariats et synergies avec d'autres organisations, affectation de personnel dans d'autres bureaux, développement d'outils et de plateformes en ligne).

À la suite de la Déclaration de Reykjavik adoptée lors du quatrième Sommet des chefs d'État et de gouvernement du Conseil de l'Europe tenu en mai 2023, concernant la dimension extérieure de l'Organisation, l'expérience du C-PROC pourrait être utile pour promouvoir d'autres conventions ouvertes aux États en dehors de l'Europe, notamment la Convention-cadre sur l'intelligence artificielle et les droits humains, la démocratie et l'État de droit, la Convention sur la protection des données personnelles et sur la protection des enfants.

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 en 2024 par le Bureau du programme du Conseil de l'Europe sur la cybercriminalité (« C-PROC » ou le « Bureau ») situé à Bucarest en Roumanie[1].

Le Bureau a démarré ses activités en avril 2014, à la suite d'une offre du Gouvernement roumain[2] et d'une décision du Comité des Ministres d'octobre 2013[3]. Il est chargé de mettre en œuvre, dans le monde entier, des projets du Conseil de l'Europe de renforcement des capacités pour lutter contre la cybercriminalité.

Le présent rapport offre un aperçu des activités de 2024, tout en faisant le bilan de l'expérience acquise par le Bureau depuis plus de dix ans, de l'augmentation des adhésions à la Convention sur la cybercriminalité (Convention de Budapest, STE n° 185) et des demandes de renforcement des capacités ainsi que des développements internationaux dans ce domaine.

2. Contexte : développements pertinents en 2024

Pour rappel, le Bureau s'inscrit dans un triangle dynamique. Concernant les normes communes de la Convention sur la cybercriminalité et de ses protocoles additionnels, ainsi que les travaux du Comité de la Convention sur la cybercriminalité (T-CY), les développements survenus en 2024 peuvent avoir été influencés par le C-PROC ou, à l'inverse, avoir eu une incidence sur celui-ci. Dans un contexte plus large, l'année 2024 a également été marquée par l'élaboration et l'adoption d'un nouveau traité international contre la cybercriminalité par les Nations Unies.

État d'avancement des adhésions à la Convention sur la cybercriminalité

En 2024, l'intérêt croissant pour la Convention sur la cybercriminalité s'est maintenu, avec l'adhésion du Bénin, de la Côte d'Ivoire, de l'Équateur, des Fidji, de la Grenade, de Kiribati, de la Sierra Leone et de la Tunisie — le nombre de Parties à la Convention a été porté à 77. Par ailleurs, le Kenya, le Malawi, le Mozambique et la Papouasie-Nouvelle-Guinée ont été invités à y adhérer.

Avant ces adhésions — et demandes d'adhésion —, les pays concernés avaient bénéficié du soutien du C-PROC, notamment pour réformer les législations nationales. Le Bureau s'attachant en priorité à fournir aux pays parties à la Convention ou invités à y adhérer un appui qui va au-delà de la seule réforme de leur législation, le nombre de pays ayant besoin d'un soutien renforcé ne cesse d'augmenter. Face à l'augmentation des demandes émanant d'un nombre croissant de pays, le C-PROC est appelé à relever de nouveaux défis.

---

[1] Conformément à la décision portant création du Bureau, le Secrétaire Général est tenu de présenter des rapports d'activité annuels.
Pour le Rapport d'activité couvrant la période d'avril 2014 à septembre 2015 : voir ce rapport (en anglais).
Pour la période octobre 2015-septembre 2016 : voir ce rapport (en anglais).
Pour la période octobre 2016-septembre 2017 : voir ce rapport.
Pour la période octobre 2017-septembre 2018, voir ce rapport.
Pour la période octobre 2018-septembre 2019, voir ce rapport.
Pour la période octobre 2019-septembre 2020, voir ce rapport.
Pour la période octobre 2020-septembre 2021, voir ce rapport.
Pour la période octobre 2021-décembre 2022, voir ce rapport.
Pour 2023, voir ce rapport.

[2] Le C-PROC est installé dans la Maison des Nations Unies à Bucarest, dans des locaux mis gracieusement à sa disposition par le Gouvernement roumain en vertu d'un Mémorandum d'accord.

[3] Décisions CM/Del/Dec(2013)1180/10.4, 9 octobre 2013, 1180e réunion.

Au-delà de l'offre de renforcement des capacités, l'intérêt porté à la Convention depuis 2022 semble dû principalement à deux autres facteurs :

- l'ouverture à la signature du Deuxième Protocole additionnel à la Convention (STCE n° 224), en mai 2022 ;

- la négociation d'un nouveau traité international, à savoir la Convention des Nations Unies contre la cybercriminalité, entre février 2022 et août 2024, suivie de son adoption par l'Assemblée générale des Nations Unies, le 24 décembre 2024[4].

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Les outils innovants prévus dans ce protocole, en particulier ceux ayant trait à la coopération directe avec les fournisseurs sur le territoire d'une autre partie et à l'entraide d'urgence, sont indispensables pour les praticiens de la justice pénale. Avec ce protocole, le cadre de la Convention sur la cybercriminalité conserve toute sa pertinence.

En décembre 2024, le protocole avait été ratifié par deux États (la Serbie et le Japon) et signé par 46 autres. Cinq ratifications sont nécessaires pour qu'il entre en vigueur.

Promouvoir son application et sa ratification restera une priorité du C-PROC dans les années à venir.

Processus d'élaboration du traité des Nations Unies

La Convention des Nations Unies contre la cybercriminalité a été élaborée par un Comité ad hoc qui a tenu huit sessions entre février 2022 et août 2024, tour à tour à New York et à Vienne. Il a examiné attentivement la Convention sur la cybercriminalité et ses deux protocoles additionnels sur la xénophobie et le racisme (STE no 189)[5] et sur l'accès aux preuves électroniques.

Le Conseil de l'Europe a contribué au processus d'élaboration par l'intermédiaire du T-CY (sous la forme de notes d'information) et du C-PROC, qui a soutenu la participation à chaque session d'experts de Parties à la Convention et d'États invités à y adhérer. Le but était de faire en sorte que le nouveau traité soit cohérent avec la Convention sur la cybercriminalité et qu'il inclue des garanties minimales en matière de droits humains et d'État de droit, indispensables pour la coopération internationale.

Des résultats ont été obtenus : les dispositions du traité des Nations Unies sont en grande partie inspirées de la Convention sur la cybercriminalité du Conseil de l'Europe, de la Convention des Nations Unies contre la criminalité transnationale organisée et de la Convention des Nations Unies contre la corruption[6].

Il en résulte que les États connaissent désormais bien mieux la Convention du Conseil de l'Europe sur la cybercriminalité.

---

[4] Titre complet du traité adopté par l'Assemblée générale des Nations Unies en décembre 2024 : « Convention des Nations Unies contre la cybercriminalité ; Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves ».

[5] 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).

[6] Concernant les liens entre les deux conventions, voir : https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1fb99

Aucune des dispositions ambitieuses du Deuxième Protocole additionnel relatif à l'utilisation de preuves électroniques n'ayant été prise en compte dans le traité des Nations Unies, il est probable que d'autres États souhaitent adhérer à la Convention sur la cybercriminalité afin de se prévaloir aussi de son Deuxième Protocole additionnel.

À l'avenir, les partenariats et les synergies créés par les deux conventions pourraient donner lieu à une coopération entre le C-PROC et l'Office des Nations Unies contre la drogue et le crime (ONUDC), dans le cadre d'activités de renforcement des capacités.

Décisions du T-CY concernant l'intelligence artificielle et les actifs virtuels

À sa 12e réunion plénière de décembre 2024, le T-CY a décidé[7] :

- de commencer à travailler sur les actifs virtuels, en particulier sur la pertinence des outils de la Convention sur la cybercriminalité et de son Deuxième Protocole additionnel concernant l'utilisation des actifs virtuels à des fins criminelles ;

- de créer un groupe de travail sur la cybercriminalité, les preuves électroniques et l'intelligence artificielle (IA) chargé de préparer une étude cartographique axée sur la pertinence des outils de la Convention sur la cybercriminalité et de son Deuxième Protocole additionnel.

Le C-PROC soutiendra le T-CY dans ces efforts et ces questions seront une composante importante de ses activités de renforcement des capacités.

Nouveaux projets de renforcement des capacités

La clôture de plusieurs grands projets à la fin de l'année 2023 n'était pas sans risques pour le C-PROC — notamment en raison de l'arrêt possible des activités de projets et de la fin des contrats de travail. Le projet Octopus, entièrement financé par des contributions volontaires, manquait également de financement.

Plusieurs nouveaux projets étaient prêts à l'automne 2023, mais la conclusion des accords de financement avait pris du retard au début de l'année 2024.

Trois projets de coopération entre le Conseil de l'Europe et l'Union européenne — CyberEast+, CyberSouth+, CyberSEE et CyberSPEX — ont néanmoins été lancés entre janvier et mars 2024[8]. Le projet CyberUA sur les preuves électroniques des crimes de guerre en Ukraine a reçu un financement initial dans le cadre du Plan d'action pour l'Ukraine. En octobre 2024, les États-Unis ont contribué à hauteur de plus de 2 millions d'euros au projet Octopus[9]. La France, le Japon et le Royaume-Uni ont également contribué au projet en 2024.

Le C-PROC a ainsi pu compter sur des ressources importantes en 2024. Les dysfonctionnements dus aux retards dans la signature des contrats, début 2024, ont été limités.

---

[7] https://rm.coe.int/t-cy-2024-12-plen31-rep-v5adopted/1680b2df6c

[8] L'accord de financement du projet GLACY-e, qui fait suite à GLACY+, avait déjà été signé au milieu de l'année 2023.

[9] Note : Le 28 janvier 2025, le Conseil de l'Europe a été informé par les autorités américaines que le financement reçu des Etats-Unis serait « suspendu ». Le 13 mars 2025, le Conseil de l'Europe a été informé que cette suspension avait été levée.

Néanmoins, les niveaux de financement actuels restent insuffisants pour répondre à l'augmentation de la demande. De plus, le financement du projet CyberUA et du projet Octopus n'est pas encore totalement garanti.

Le développement de nouveaux projets et la mobilisation de ressources sont des tâches permanentes du C-PROC.

3. Aperçu des projets et réalisations en 2024

Projets

En 2024, six projets de portée régionale et mondiale et un projet national (Ukraine) du C-PROC étaient en cours de mise en œuvre[10]. En décembre 2024, les budgets combinés des projets en cours s'élevaient à 34,6 millions d'euros ; cependant, 5 millions d'euros environ n'étaient pas encore garantis pour les projets CyberUA et Octopus :

Intitulé du projet	Durée	Budget	Financement
Projet Octopus Soutien à la mise en œuvre de la Convention sur la cybercriminalité, de ses protocoles additionnels et des normes connexes dans le monde entier	janvier 2021 - décembre 2027	10 millions d'euros	Contributions volontaires (Canada, France, Hongrie, Islande, Italie, Japon, Pays-Bas, Royaume-Uni et États-Unis[11]) [financement garanti seulement en partie]
Projet GLACY-e Action globale renforcée sur la cybercriminalité	août 2023 - janvier 2026	5,55 millions d'euros	Projet conjoint UE/CdE (dont 10 % BO/PPC CdE)
Projet GLACY+ Action globale sur la cybercriminalité élargie	mars 2016 - février 2024	18,9 millions d'euros	Projet conjoint UE/CdE (dont 10 % BO CdE)
Projet CyberUA Renforcement des capacités sur les preuves électroniques des crimes de guerre et des violations flagrantes des droits humains en Ukraine	février 2024 - juillet 2026	3,5 millions d'euros	Contributions volontaires au Plan d'action pour l'Ukraine[12] et BO [financement garanti seulement en partie]
Projet CyberEast+ Action renforcée contre la cybercriminalité pour la cyberrésilience dans les États du partenariat oriental	mars 2024 - février 2027	3,89 millions d'euros	Projet conjoint UE/CdE (dont 10 % BO/PPC CdE)
Projet CyberSouth+ Coopération renforcée en matière de cybercriminalité et de preuves électroniques dans la région du voisinage méridional	janvier 2024 - décembre 2026	389 millions d'euros	Projet conjoint UE/CdE (dont 10 % BO/PPC CdE)

[10] Hormis le projet « GLACY+ » clôturé en février 2024.

[11] Voir également la note de bas de page 10.

[12] Plan d'action du Conseil de l'Europe pour l'Ukraine « Résilience, redressement et reconstruction » pour 2023-2026.

Projet CyberSEE Coopération renforcée en matière de cybercriminalité et de preuves électroniques en Europe du Sud-Est et en Türkiye	janvier 2024 - juin 2027	5,55 millions d'euros	Projet conjoint UE/CdE (dont 10 % BO/PPC CdE)
Projet CyberSPEX Coopération renforcée des États membres de l'Union européenne en matière de preuves électroniques grâce au Deuxième Protocole à la Convention de Budapest	mars 2024 - février 2026	2,23 millions d'euros	Projet conjoint UE/CdE (dont 10 % BO/PPC CdE)

Entre janvier et décembre 2024, le C-PROC, avec 54 agentes et agents, a soutenu plus de 310 activités dans le cadre de ces projets. Un inventaire des activités financées depuis 2014 est disponible en ligne (en anglais).

Le Bureau dépend de financements externes. Le projet Octopus est financé par des contributions volontaires et le projet CyberUA par des contributions volontaires et le budget ordinaire du Plan d'action pour l'Ukraine. Quant aux projets de coopération avec l'UE, ils sont cofinancés à hauteur de 10 % par la Provision du Conseil de l'Europe (Budget ordinaire) pour les programmes conjoints de l'UE et du CdE (BO/PPC).

L'UE est restée le principal donateur avec des projets conjoints cofinancés par le Conseil de l'Europe. En 2024, les États-Unis ont une nouvelle fois contribué de manière importante au projet Octopus[13], au financement duquel le Japon, la France et le Royaume-Uni ont également contribué. Plusieurs États membres de l'Organisation ont contribué au projet CyberUA dans le cadre du financement du Plan d'action pour l'Ukraine. Le Bureau bénéficie aussi du soutien du Gouvernement roumain, qui continue de mettre gracieusement des bureaux à sa disposition.

[13] Voir note de bas de page 10.

Réalisations

Capacités en matière de justice pénale

En 2024, le C-PROC a considérablement contribué au renforcement des capacités en matière de justice pénale, en particulier dans la quarantaine de pays prioritaires éligibles à une série de mesures d'appui. Une centaine d'autres pays ont participé à quelques-unes au moins des activités.

Exemples d'activités menées dans le cadre de différents projets et résultats obtenus :

- Projet **CyberEast+** — Action renforcée contre la cybercriminalité pour la cyberrésilience dans les États du partenariat oriental :

  En juin 2024, dans le cadre de l'appui au projet, la Géorgie est devenue le 44e État à signer le Deuxième Protocole additionnel à la Convention sur la cybercriminalité.

  Après une phase de lancement (de mai à juillet 2024), le projet a consisté à collaborer avec des homologues en Arménie, en République de Moldova et en Ukraine sur les exigences relatives à l'application du Deuxième Protocole additionnel, ainsi que sur la conformité avec la Convention sur la cybercriminalité.

  Le programme de formation et de renforcement des capacités a été axé sur les compétences du pouvoir judiciaire (République de Moldova), les enquêtes parallèles sur la cybercriminalité et les enquêtes financières (Arménie) et le soutien spécifique à l'Ukraine dans les enquêtes sur les rançongiciels, les logiciels malveillants et les réseaux, ainsi que sur l'utilisation de la Convention sur la cybercriminalité dans les conflits armés (Ukraine). Le projet a également élaboré un cours de formation révisé sur la coopération internationale, qui a été dispensé en Arménie et en République de Moldova.

  En partenariat avec d'autres projets du C-PROC, des agentes et agents des services répressifs de la région ont pu renforcer leurs compétences en matière de cybercriminalité lors d'une formation spécifique organisée dans le cadre de la Conférence sur l'économie souterraine 2024, ainsi qu'en matière d'enquêtes sur les cryptomonnaies et l'abus sexuels des enfants en ligne.

  Événement phare du projet en 2024, l'exercice régional de coopération contre la cybercriminalité, Cybercrime Co-operation Exercise, a réuni 50 participantes et participants de 12 pays qui ont analysé, lors d'un exercice pratique en temps réel, des scénarios de cyberattaques contre des infrastructures critiques.

  Le projet a donné lieu à un échange avec la société civile au niveau régional (EuroDIG 2024) sur les questions de coopération avec d'autres secteurs (protection des données, IA, gouvernance de l'Internet) dans le cadre de la lutte contre la cybercriminalité.

  Il a également permis d'entamer l'établissement de rapports nationaux sur les menaces et les défis de la cybercriminalité pour chacun des pays du partenariat oriental, en coopération avec des organisations de la société civile.

  Le projet a soutenu la participation d'experts en la matière aux réunions du Comité ad hoc des Nations Unies chargé d'élaborer un nouveau traité international contre la cybercriminalité.

Le projet a soutenu 26 activités durant cette période.

- **CyberUA** — Renforcement des capacités sur les preuves électroniques des crimes de guerre et des violations flagrantes des droits humains en Ukraine

  Depuis son lancement en mars 2024, CyberUA (conjointement avec le projet CyberEast+) a repris ses travaux avec les autorités ukrainiennes en vue de réformer la législation interne et la rendre conforme à la Convention sur la cybercriminalité.

  Le projet s'est notamment attaché à renforcer les capacités des services répressifs et des procureurs/magistrats chargés de traiter les preuves électroniques des crimes de guerre et des violations graves des droits humains.

  Les formations ont porté sur la recevabilité, le traitement et la chaîne de mise en sûreté des preuves électroniques, la conservation et la production de données, les enquêtes sur les cryptomonnaies et l'internet clandestin, l'utilisation des outils de coopération internationale et la coopération entre les services répressifs et les équipes CSIRT[14] (en coopération avec le projet CyberSEE). Lors d'un exercice de coopération avec des homologues clés à Kiev, les participants ont pu tester leurs compétences en matière d'investigations et de criminalistique numérique lors de simulations de cyberattaques contre des infrastructures critiques.

  Des organisations de la société civile et des médias ont été associés au projet lors de formations sur la cybercriminalité et les preuves électroniques, et un forum de consultation avec des entités du secteur privé a été organisé sous la direction du Conseil national de sécurité et de défense. Le projet a ainsi contribué à améliorer les signalements et les échanges de renseignements sur les crimes de guerre et les violations graves des droits humains.

  Une conférence sur les échanges de preuves électroniques dans les affaires de crimes de guerre et de violations graves des droits humains tenue à Strasbourg a réuni les principaux homologues nationaux du projet, des représentants de la société civile et des partenaires internationaux, dans le but d'améliorer la coopération.

  Le projet a également commencé à travailler sur la création de ressources en ligne dédiées aux preuves électroniques et au renseignement d'origine sources ouvertes (*Open Source Intelligence*, OSINT) sur les crimes de guerre et les violations graves des droits humains, ainsi que sur une évaluation des besoins matériels et logiciels des partenaires ukrainiens du projet.

  Le projet a soutenu 20 activités durant cette période.

- Projet **CyberSEE** — Coopération renforcée en matière de cybercriminalité et de preuves électroniques en Europe du Sud-Est et en Türkiye

  Des professionnels de la justice pénale ont amélioré leurs connaissances en matière de coopération judiciaire dans la lutte contre la cybercriminalité, de détection et de confiscation des cryptomonnaies, d'enquêtes sur l'abus sexuels des enfant en ligne, de traitement des preuves électroniques et d'utilisation des outils de criminalistique numérique de pointe dans le cadre de manifestations organisées en coopération avec d'autres organisations.

[14] Équipes dédiées à la gestion des incidents de sécurité informatique.

De nouvelles mesures ont été prises pour intégrer des modules sur la cybercriminalité et les preuves électroniques dans les programmes des écoles de police et des organismes de formation judiciaire lors d'ateliers régionaux au Monténégro et en Türkiye.

Un atelier régional et un exercice international sur l'échange de renseignement en temps réel, tous deux organisés en Albanie, ont renforcé la coopération entre les services répressifs et les équipes CERT (*Computer Emergency Response Team*).

Plus de 500 expertes et experts du monde entier — agentes et agents de services répressifs, spécialistes de la cybersécurité, du secteur privé, des services financiers et du monde universitaire — ont participé à des ateliers thématiques et à des études de cas lors de la Conférence sur l'économie souterraine, qui s'est tenue au Conseil de l'Europe, à Strasbourg, avec des exemples d'opérations internationales contre les botnets et des groupes de rançongiciels.

L'Albanie a bénéficié d'une assistance pour engager des réformes législatives en vue de la ratification du Deuxième Protocole additionnel à la Convention sur la cybercriminalité.

La réunion annuelle du Réseau de points de contact 24/7, soutenue par le projet CyberSEE et d'autres projets du C-PROC, a servi de plateforme pour renforcer la coopération internationale et la coopération public/privé dans le cadre de la Convention sur la cybercriminalité.

Le projet a permis de soutenir la participation d'experts aux réunions du Comité ad hoc des Nations Unies chargé d'élaborer un nouveau traité international contre la cybercriminalité.

Le projet a soutenu 70 activités durant cette période.

- Projet **CyberSPEX** — Coopération renforcée des États membres de l'Union européenne en matière de preuves électroniques grâce au Deuxième Protocole à la Convention de Budapest

  Au lendemain de la cérémonie de lancement en juin 2024, des mesures de coordination bilatérales ont été mises en place pour soutenir l'application du Deuxième Protocole additionnel dans les États membres de l'UE. Des acteurs de l'UE tels que le réseau judiciaire européen en matière de cybercriminalité et le projet SIRIUS[15] ont été mobilisés pour coordonner les futures activités.

  Plus de 140 participantes et participants appartenant aux forces de l'ordre, au pouvoir judiciaire et au pouvoir législatif, ainsi qu'à des organes de l'UE, ont approfondi leurs connaissances sur le Protocole lors d'une série d'ateliers en ligne sur les procédures visant à renforcer la coopération internationale entre les autorités publiques et les mécanismes de coopération directe avec les fournisseurs de services pour la divulgation de données informatiques.

[15] SIRIUS (Support to Investigation and Prosecution in Europe of Serious Crime) est un projet créé par EUROPOL et EUROJUST pour répondre aux demandes transfrontalières d'accès à des preuves électroniques.

Les 27 États membres de l'UE ont tous bénéficié d'un soutien afin d'évaluer l'état d'avancement du processus de mise en œuvre et définir les réformes nécessaires au moyen d'un modèle d'évaluation juridique et d'un guide de mise en œuvre conçus dans le cadre de CyberSPEX.

Un webinaire enregistré et disponible sur une plateforme de l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) a présenté aux agentes et agents des services répressifs les procédures du Protocole en matière de coopération internationale.

Plusieurs réunions et conférences, en particulier la conférence annuelle de SIRIUS[16], ont favorisé la mise en œuvre en parallèle du paquet de mesures de l'UE relatif à la preuve électronique[17] et du Deuxième Protocole additionnel.

Des réunions avec des points de contact des pays scandinaves et baltes (Estonie, Finlande, Lettonie, Lituanie, Suède) ainsi que de la région méditerranéenne (Chypre, Espagne, Grèce, Italie, Malte, Portugal) ont favorisé le partage d'expériences au niveau des régions.

Les pays engagés dans des réformes législatives (Autriche, Estonie, France, République slovaque, Espagne) ont échangé des informations sur l'harmonisation de leurs législations nationales respectives.

Les États membres de l'UE ont pu approfondir leur compréhension de la coopération public/privé dans le cadre des enquêtes et des procédures pénales à l'occasion d'un atelier avec des fournisseurs de services et des entreprises organisé par le T-CY et CyberSPEX.

Le projet a soutenu 19 activités durant cette période.

- Projet **CyberSouth+** — Coopération renforcée en matière de cybercriminalité et de preuves électroniques dans la région du voisinage méridional

  Après une phase préparatoire de trois mois, le projet CyberSouth+ a été officiellement lancé en avril 2024 ; trois nouveaux partenaires, l'Égypte, la Libye et la Palestine*, ont rejoint l'Algérie, le Liban, la Jordanie, le Maroc et la Tunisie dans leurs efforts communs pour lutter contre la cybercriminalité. Une visite en Égypte a donné l'occasion de rencontrer les interlocuteurs concernés et de poser les jalons d'une coopération future.

  La Tunisie est devenue partie à la Convention sur la cybercriminalité en 2024 et le dialogue avec le Gouvernement et le Parlement tunisiens s'est poursuivi en vue d'aligner la législation nationale sur les exigences de la Convention et sur les normes internationales relatives aux droits humains, y compris concernant la liberté d'expression.

---

[16] SIRIUS | Eurojust | European Union Agency for Criminal Justice Cooperation

[17] Règlement relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale.
E-evidence - cross-border access to electronic evidence - European Commission

* Cette dénomination ne saurait être interprétée comme une reconnaissance d'un État de Palestine et est sans préjudice de la position de chaque État membre du Conseil de l'Europe et de l'Union européenne sur cette question.

Les partenaires du projet ont participé à des activités consacrées au Premier 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.

Des modules de formation sur la cybercriminalité et les preuves électroniques, ainsi que des modules de formation de formateurs et des ateliers sur la législation ont été organisés en collaboration avec les écoles nationales de la magistrature en Algérie, en Libye, en Jordanie, au Maroc, en Palestine* et en Tunisie, afin de renforcer les capacités judiciaires de ces pays à combattre la cybercriminalité. Une analyse et un atelier dédié aux programmes de formation sur la cybercriminalité adoptés par ces écoles ont été organisés avec tous les partenaires, en vue d'évaluer la durabilité des capacités nationales à former les futurs magistrats.

Des exercices nationaux et régionaux ont permis à des représentants des forces de l'ordre de continuer à se spécialiser dans les enquêtes sur l'internet clandestin et les cryptomonnaies, l'analyse de données en direct, les attaques par rançongiciel et l'exploitation des enfants et les abus sexuels d'enfants en ligne. Des enquêteurs des huit pays partenaires ont participé.

En Tunisie, le projet a encouragé la coopération interinstitutionnelle entre les acteurs de la lutte contre la cybercriminalité et de la cybersécurité. Il a également permis de renforcer la coopération avec l'AICTO[18], INTERPOL et le DCAF[19], qui ont mené conjointement des activités nationales et régionales.

Le projet a permis à des professionnels de la justice pénale des huit pays partenaires de participer à des ateliers et événements internationaux de premier plan sur la cybercriminalité (Underground Economy 2024, réunion annuelle du Réseau de points de contact 24/7 et conférence EUROPOL sur la cybercriminalité).

Le projet a coordonné les activités avec les bureaux du Conseil de l'Europe à Tunis et à Rabat, avec l'Unité de protection des données et la Division des droits de l'enfant du Conseil de l'Europe, ainsi qu'avec d'autres projets dans la région de l'Union européenne, dont l'Allemagne, et avec le Royaume-Uni, les États-Unis et l'ONUDC.

Le projet a soutenu 58 activités durant cette période.

- Projet **Octopus** — Soutien à l'application de la Convention sur la cybercriminalité, de ses protocoles additionnels et des normes connexes dans le monde entier

  Des pays d'Asie du Sud-Est (Brunéi, Cambodge, Indonésie, Laos, Malaisie, Singapour, Thaïlande et Vietnam), d'Asie centrale (Kazakhstan), d'Afrique (Cameroun, Gambie, Seychelles, Mauritanie, Malawi) et d'Amérique latine (Guatemala) ont reçu un soutien pour réformer leur législation en matière de cybercriminalité et de preuves électroniques.

[18] Organisation Arabe des Technologies de l'Information et de la Communication (sous l'égide de la Ligue des États arabes).
[19] Centre de Genève pour la gouvernance du secteur de la sécurité (DCAF), anciennement Centre de Genève pour le contrôle démocratique des forces armées.

Des efforts importants ont été déployés pour inscrire la formation judiciaire dans la durée, notamment en mettant en place un réseau de formateurs judiciaires nationaux spécialisés dans la cybercriminalité et les preuves électroniques. À titre d'exemple, on peut citer le soutien apporté à la Malaisie, à l'Indonésie, à la Thaïlande, à Maurice, au Brésil, ainsi que dans les régions du Pacifique et de l'Asie du Sud-Est. Le projet a par ailleurs soutenu des activités conjointes du Réseau international des formateurs judiciaires nationaux (webinaires P2P sur l'exploitation et les abus sexuels d'enfants en ligne, la cyberviolence, les enquêtes financières, la coopération dans les situations d'urgence). Il a également contribué à promouvoir la formation judiciaire en impliquant des juges et des procureurs hispanophones.

Les autorités kazakhes ont été soutenues pour participer à des exercices régionaux (notamment sur la coopération services répressifs/équipes CSIRT, ainsi que sur l'application de la loi et les stratégies en matière de formation judiciaire), ainsi qu'à des formations nationales sur les enquêtes financières et les rançongiciels.

Le projet a aidé la Grenade à devenir partie à la Convention sur la cybercriminalité et à satisfaire aux exigences de coopération internationale prévues par le traité.

Au niveau mondial, le projet a facilité les débats d'experts sur les thématiques suivantes : renforcement de la coopération internationale ; détection de la cybercriminalité, enquête et neutralisation ; partage spontané d'informations ; tendances de la cybercriminalité et méthodes utilisées par les forces de l'ordre et le secteur de la cybersécurité pour lutter contre les activités criminelles en ligne ; liberté d'expression et sécurité publique ; escroqueries en ligne, etc. Ces activités ont été complétées par des échanges avec des parlementaires dans les Caraïbes et en Afrique, avec la communauté diplomatique à Bucarest et des échanges de vues avec des fournisseurs de services.

Le projet Octopus a continué à soutenir les travaux du T-CY, notamment la finalisation de l'évaluation de l'article 19 de la Convention (« Perquisition et saisie de données informatiques stockées »).

Il a également soutenu la participation d'experts aux réunions du Comité ad hoc des Nations Unies chargé d'élaborer un nouveau traité international contre la cybercriminalité.

Des praticiens de la justice pénale du monde entier ont pu enrichir leurs connaissances grâce aux ressources gérées par le projet — ressource sur la Cyberviolence, cours HELP sur la cybercriminalité, traductions du document de travail sur la liberté d'expression et plateforme Octopus. Enfin, CYBOX, la nouvelle plateforme en ligne d'échange, de formation et de partage de ressources sur la cybercriminalité et les preuves électroniques, a été lancée en 2024.

En 2024, de nouvelles contributions volontaires ont été reçues des États-Unis, de la France, du Japon et du Royaume-Uni[20].

[20] Voir note de bas de page 10.

L'action **CYBERKOP**[21] du projet Octopus a permis aux praticiens de la justice pénale au Kosovo* d'améliorer leurs connaissances en matière de coopération judiciaire pour lutter contre la cybercriminalité (rédaction d'accords de coopération judiciaire dans les affaires pénales, conservation des données, information spontanée, instruments de coopération internationale de l'UE pertinents, enquêtes sur l'abus des enfants en ligne, les actifs virtuels et l'utilisation d'outils de criminalistique). Les groupes de travail nationaux ont reçu un soutien spécialisé pour élaborer des textes législatifs, des cadres réglementaires et des procédures opérationnelles normalisées. Des praticiens de la justice pénale, des experts en cybersécurité et le secteur privé ont renforcé leur coopération lors d'un atelier national sur la lutte contre les menaces de cybersécurité. Un atelier sur les cryptomonnaies a permis aux experts du renseignement financier, aux agentes et agents des services répressifs, aux procureurs et à la Banque centrale d'améliorer leur capacité à prévenir et à contrôler l'utilisation des actifs virtuels à des fins criminelles.

Le projet a soutenu 73 activités durant cette période.

- Projet **GLACY-e** — Action globale renforcée sur la cybercriminalité

  En 2024, six pays participants du projet (Bénin, Côte d'Ivoire, Équateur, Fidji, Kiribati et Sierra Leone) sont devenus parties à la Convention sur la cybercriminalité ; quatre autres (Mozambique, Malawi, Kenya et Papouasie-Nouvelle-Guinée) ont été invités à y adhérer. Par ailleurs, le Bénin a adhéré au Premier Protocole additionnel à la Convention et la Sierra Leone a signé le Deuxième Protocole additionnel.

  Le projet GLACY-e a aidé le Guatemala, le Lesotho, la Mauritanie, le Malawi, le Nigéria, le Panama, le Rwanda et la Gambie à réformer leur législation sur la cybercriminalité.

  Concernant les capacités de formation judiciaire, il a contribué au renforcement des compétences des formateurs nationaux et au développement des réseaux de formateurs nationaux au Brésil, en Colombie, à Maurice et aux Philippines. Des ateliers de formation judiciaire et des visites d'étude ont également été organisés aux Fidji, en Thaïlande, au Costa Rica et au Pérou, et une série d'ateliers P2P a été organisée dans le cadre du Réseau international de formateurs judiciaires nationaux du C-PROC.

  Le projet s'est également attaché à améliorer les connaissances des « pays pivots »[22] et d'autres pays sélectionnés en matière d'enquêtes financières et de cryptomonnaies, dans le cadre d'une série de formations régionales virtuelles sur les actifs (pays d'Afrique) et d'une formation à la demande sur les cryptomonnaies (« pays pivots » d'Amérique latine).

[21] L'action CyberKOP consiste en une série d'activités menées par le projet Octopus au Kosovo*.
* Toute référence au Kosovo dans le présent document, 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.

[22] Les « pays pivots » sont des pays qui sont parties à la Convention sur la cybercriminalité et avec lesquels le C-PROC coopère depuis longtemps. Ces pays servent désormais de « pivots » pour partager leur expérience au sein de leur région respective.

Plusieurs ateliers et événements thématiques régionaux et internationaux ont été proposés dans le cadre du projet GLACY-e : Digital Security Challenge 2024,[23] formation régionale sur la cybercriminalité et les preuves électroniques destinée aux ministères publics et aux services judiciaires (région Pacifique), atelier régional sur le Deuxième Protocole additionnel en Amérique latine, atelier sur les informations spontanées coorganisé par Eurojust et le Conseil de l'Europe et plénière du Réseau international de formateurs judiciaires nationaux.

Le projet a soutenu la participation d'experts aux réunions du Comité ad hoc des Nations Unies chargé d'élaborer un nouveau traité international contre la cybercriminalité.

Enfin, des pays prioritaires et d'autres pays sélectionnés ont été soutenus pour participer à plusieurs rencontres internationales et régionales : réunions des Groupes de travail INTERPOL sur la cybercriminalité pour les chefs des unités de lutte contre la cybercriminalité en Afrique, en Asie, dans le Pacifique Sud et dans les Amériques, Atelier INTERPOL sur le piratage numérique, Conférence sur l'économie souterraine 2024, réunion annuelle du Réseau de points de contact 24/7, et la Conférence EUROPOL.

Le projet a soutenu 104 activités durant cette période.

Outils et ressources

Parmi les nombreux guides, plateformes et autres outils et ressources établis ou étoffés en 2024, on peut citer :

- la plateforme CYBOX d'échange, de formation et de partage de ressources en ligne sur la cybercriminalité et les preuves électroniques qui a été lancée sous la direction du projet Octopus. Pensée comme une solution mutualisée basée sur la plateforme Moodle Workplace, CYBOX propose une nouvelle approche du renforcement des capacités et de la formation par le C-PROC ;

- des modèles et un guide visant à simplifier la préparation des textes législatifs et l'application du Deuxième Protocole additionnel à la Convention sur la cybercriminalité qui ont été élaborés dans le cadre du projet CyberSPEX ;

- un guide sur la manière d'élaborer et de mettre en œuvre des stratégies de formation judiciaire qui a été finalisé avec la contribution de tous les projets du C-PROC ;

- le projet CyberSEE qui a mis en ligne des ressources sur les attaques par rançongiciel ; en 2024, le Conseil de l'Europe est également devenu membre de la Counter Ransomware Initiative (CRI).

- Le projet Octopus a mis à jour ses ressources en ligne sur la cyberviolence.

[23] 47 participants de 21 pays ont pu tester leurs compétences lors du Digital Security Challenge, un tournoi de CTF (*capture-the-flag competition*).

Partenariats et synergies

Pour le C-PROC, les partenariats et les synergies avec d'autres organisations sont un élément indispensable du renforcement des capacités. Ils permettent de développer ses activités et de multiplier les messages et leur impact. En 2024 :

- le C-PROC a coopéré et établi des partenariats, avec les organisations suivantes : Commission de l'Union africaine, Communauté des pays de langue portugaise (CPLP), Counter Ransomware Initiative (CRI), Commission européenne, Agence de l'Union européenne pour la coopération judiciaire en matière pénale (EUROJUST), Agence de l'Union européenne pour la coopération des services répressifs (EUROPOL), Agence de l'Union Européenne pour la formation des services répressifs (CEPOL), European Cybercrime Training and Education Group (ECTEG), Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), Forum of Presidents of Legislative Powers in Central America and the Caribbean (FOPREL), Global Forum for Cyber Expertise (GFCE), Association internationale des procureurs (AIP), INTERPOL[24], Ligue des États arabes, Organisation pour la sécurité et la coopération en Europe (OSCE), Organisation des États américains (OEA), Pacific Islands Law Officers Network (PILON), Action mondiale des parlementaires (PGA), Southeast Europe Police Chiefs Association (SEPCA), ONUDC et Western Balkans Cyber Capacity Centre (WB3C). Par ailleurs, le C-PROC coopère avec les autorités nationales de divers pays (dont la Police fédérale australienne (AFP), le Département d'État à la Justice des États-Unis, le Gouvernement roumain en tant que pays hôte du C-PROC, etc.) ;

- des activités diverses ont été menées conjointement avec d'autres projets de renforcement des capacités financés par l'Union Européenne (CyberNet, EL PACCTO 2.0, SIRIUS) portant sur la cybercriminalité et les preuves électroniques, ou avec le soutien de TAIEX,[25] en vue de promouvoir des politiques internationales cohérentes en matière de renforcement des capacités pour lutter contre la cybercriminalité. Le C-PROC entretient d'excellentes relations avec des réseaux d'experts et des institutions de premier plan dans toutes les régions du monde et est reconnu comme un partenaire clé.

Des synergies ont été créées avec d'autres instruments et actions du Conseil de l'Europe, par exemple :

- activités de renforcement des capacités en matière de protection des données (conformément à la Convention STE n° 108[26], telle que modifiée par la Convention STCE n° 223[27]) ou de protection des enfants contre l'exploitation et les abus sexuels (conformément à la Convention de Lanzarote[28]), création de ressources en ligne sur la cyberviolence, contribution à des études typologiques sur le blanchiment de capitaux ;

[24] Le Complexe mondial INTERPOL pour l'innovation (CMII) basé à Singapour est partenaire du projet GLACY+. En vertu d'un accord de subvention, INTERPOL est chargé du volet application de la loi du projet.
[25] Instrument d'assistance technique et d'échange d'informations de la Commission européenne (TAIEX), par exemple pour la formation judiciaire régionale des Chief Justices de la région Pacifique.
[26] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108).
[27] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223).
[28] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).

- le projet CyberSEE, en partenariat avec le projet visant à mettre fin à l'exploitation et aux abus sexuels d'enfants en ligne (EndOCSEA@Europe+), a organisé, au Monténégro, une formation conjointe sur la prévention et la lutte contre l'exploitation et les abus sexuels d'enfants en ligne pour les services répressifs, les juges et les procureurs ;

- en marge de la plénière du T-CY et de l'Atelier régional sur la cybercriminalité, les preuves électroniques et l'exploitation et les abus sexuels d'enfants en ligne en Asie du Sud-Est, le projet Octopus a organisé des manifestations sur l'exploitation et les abus sexuels d'enfants en ligne, en coopération avec la Division des droits de l'enfant ;

- le C-PROC s'est par ailleurs associé au Centre Nord-Sud du Conseil de l'Europe pour lutter contre le racisme et la xénophobie en ligne et a coordonné toutes les activités dans les régions du sud de la Méditerranée et du sud-est de l'Europe avec les bureaux locaux.

Soutien au Comité de la Convention cybercriminalité (T-CY)

Le triangle dynamique — normes communes, suivi/évaluations et renforcement des capacités — explique en grande partie l'efficacité globale du cadre de la Convention sur la cybercriminalité. Un exemple illustre le fonctionnement de ce triangle dans la pratique et le soutien du C-PROC au T-CY en 2024 :

En juin 2024, le T-CY a chargé son Bureau de préparer une Note d'orientation sur l'article 26 de la Convention (« Information spontanée ») et d'inviter les Parties à répondre à un questionnaire établi par le Secrétariat du T-CY et le C-PROC.

En septembre 2024, le C-PROC a organisé une manifestation internationale à ce sujet à La Haye, conjointement avec EUROJUST.

En décembre 2024, le rapport présentant les conclusions de cet événement et les réponses au questionnaire (préparé conjointement par le Secrétariat du T-CY et le C-PROC) a été présenté à la plénière du T-CY.

Ces conclusions aideront le Bureau du T-CY à élaborer un projet de Note d'orientation pour juin 2025.

En 2024, le C-PROC a également aidé le Bureau du T-CY à élaborer un projet de questionnaire sur les pratiques des Parties à la Convention concernant les actifs virtuels et la pertinence de la Convention sur la cybercriminalité et de son Deuxième Protocole additionnel. Ce questionnaire a été adopté à la 31e plénière du T-CY, en décembre 2024.

La participation de plusieurs experts aux plénières de juin et de décembre 2024 du T-CY a été financée par des projets du C-PROC.

Enfin, le C-PROC gère le fonctionnement du Réseau des points de contact 24/7 (établi en application de l'article 35 de la Convention sur la cybercriminalité) et organise ses réunions annuelles.

Intégration de la dimension de genre dans le renforcement des capacités en matière de cybercriminalité et de preuves électroniques

Les cyber infractions ne touchent pas les femmes et les hommes de la même manière. Certains types de violences fondées sur le genre et facilitées par la technologie, fréquemment signalés, incluent le cyberharcèlement, le harcèlement sexuel, les abus basés sur des images ou messages menaçants, mais aussi l'exploitation et les abus sexuels d'enfants en ligne (OCSEA). Les femmes et les filles sont particulièrement exposées à ces types d'infractions. Parallèlement, les femmes ont un rôle crucial à jouer pour que la justice pénale lutte efficacement contre ce phénomène — tant au niveau des autorités politiques et législatives qui élaborent et adoptent les lois sur la cybercriminalité qu'au niveau des autorités judiciaires chargées des enquêtes, des poursuites et des condamnations dans des affaires de cybercriminalité et d'infractions connexes.

Dans ce contexte, le C-PROC met à disposition plusieurs outils pour soutenir les autorités nationales, notamment des ressources sur la cyberviolence gérées par le projet Octopus, qui font suite à une étude cartographique du T-CY sur la cyberviolence (2017).

Pour lutter contre la cyberviolence, les projets du C-PROC encouragent les synergies entre les accords du Conseil de l'Europe, en particulier la Convention sur la cybercriminalité, la Convention d'Istanbul (STCE n° 210)[29] et la Convention de Lanzarote (STCE n° 201).

Les actions du C-PROC s'appuient également sur la Stratégie du Conseil de l'Europe pour l'égalité de genre (2024-2029).

Exemples d'activités menées en 2024 :

- formation spécialisée sur les aspects genrés de la cybercriminalité, élaborée par le projet GLACY-e en coopération avec des experts équatoriens ; il s'agit d'une formation pilote qui sera ensuite fournie dans d'autres pays et régions ;

- formation régionale sur la cybercriminalité et les preuves électroniques destinée aux enquêteuses et procureures de la région du sud de la Méditerranée, organisée par le projet CyberSouth+.

L'expérience montre que le C-PROC :

- doit développer ses activités dans des pays du monde entier pour lutter contre la cybercriminalité et la cyberviolence, y compris les aspects liés au genre de ces infractions, comme la diffusion non consentie d'images intimes ;

- doit promouvoir le rôle des femmes dans la lutte contre les cyber infractions et les infractions connexes, les enquêtes à ce sujet et les poursuites contre leurs auteurs.

[29] Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE 210).

4. Conclusions et perspectives

Avec 18 projets et plus de 2 400 activités au profit de quelque 140 pays en dix ans d'existence (2014-2024), le C-PROC peut se prévaloir de résultats, de réalisations et d'effets notables, notamment un intérêt accru pour la Convention sur la cybercriminalité et une augmentation des adhésions, l'alignement[30] des législations nationales sur les normes de la Convention[31] et le renforcement des capacités de leurs praticiens de la justice pénale. Il a établi des partenariats et créé des synergies avec des institutions très variées et s'est adapté aux nouveaux défis (COVID, la guerre d'agression de la Russie contre l'Ukraine, augmentation des attaques par rançongiciel, atteintes à la liberté d'expression, etc.). Par ailleurs, le C-PROC a soutenu les négociations du Deuxième Protocole additionnel à la Convention sur la cybercriminalité ainsi que son application après qu'il a été adopté.

Grâce à ces activités, il a démontré que les normes du Conseil de l'Europe pouvaient être étendues à l'échelle mondiale. L'expérience du C-PROC - avec la coopération et la confiance qu'il a établi avec les autorités de pays de toutes les régions du monde et son mode de fonctionnement - est unique au Conseil de l'Europe. L'action du Conseil de l'Europe en matière de cybercriminalité, notamment par l'intermédiaire du C-PROC, peut servir de modèle et faciliter le rayonnement au-delà de l'Europe, y compris en ce qui concerne d'autres traités du Conseil de l'Europe.

Les principaux facteurs de sa réussite sont les suivants :

- le C-PROC représente le volet renforcement des capacités du triangle dynamique composé : a) des normes communes de la Convention sur la cybercriminalité et de ses protocoles, ainsi que des normes connexes ; b) du suivi et des évaluations par le Comité de la Convention sur la cybercriminalité (T-CY) ; c) du renforcement des capacités par le C-PROC. Ces trois éléments relèvent de la compétence de la Division Cybercriminalité ;

- le C-PROC intervient dans toutes les régions du monde ;

- les principales responsabilités du C-PROC sont, entre autres, le développement de projets et l'obtention de financements. Entre 2014 et 2024, il a préparé et mis en œuvre 18 projets pour un budget cumulé de 86 millions euros. À cet égard, il a mobilisé 76 millions d'euros de ressources extrabudgétaires ;

- une gestion saine et efficace des ressources est indispensable pour avoir la confiance des donateurs. Les nombreux audits, évaluations et autres exercices similaires ont confirmé la gestion des risques et les contrôles internes du Bureau, ainsi que sa capacité à respecter ses obligations contractuelles envers les donateurs. Les locaux du Bureau sont mis gracieusement à disposition par le Gouvernement roumain.

[30] En 2013, 53 États étaient parties à la Convention (41), l'avaient signée (2) ou avaient été invités à y adhérer (10). Fin 2024, 95 États étaient parties à la Convention (77), l'avaient signée (2) ou avaient été invités à y adhérer (16).
[31] En 2013, par exemple, le droit pénal de 70 États, dont seulement six en Afrique, réprimait des infractions pénales similaires à celles visées par la Convention sur la cybercriminalité. Fin 2024, ce nombre était passé à 132 États, dont 34 États africains.

Le Conseil de l'Europe entend, par l'intermédiaire du C-PROC, conforter sa position d'acteur de premier plan au niveau mondial en termes de renforcement des capacités pour la lutte contre la cybercriminalité, et continuer à promouvoir les droits humains, la démocratie et l'État de droit dans le cyberespace. Pour ce faire, il devra :

- soutenir ou renforcer le triangle dynamique de la Convention sur la cybercriminalité et de ses protocoles additionnels, le T-CY et le C-PROC ;

- étendre la portée mondiale des activités du C-PROC et faciliter ainsi la diffusion d'autres normes de l'Organisation hors d'Europe — conformément à la Déclaration de Reykjavik — par exemple dans les domaines de l'IA, de la protection des données ou de la protection des enfants ;

- élargir les partenariats et les synergies à d'autres organisations afin d'accroître la portée et l'impact des projets et activités ;

- soutenir l'application du Deuxième Protocole additionnel sur les preuves électroniques — une priorité du C-PROC —, ce Protocole étant essentiel pour que le cadre de la Convention sur la cybercriminalité conserve toute sa pertinence ;

- développer les activités de renforcement des capacités dans trois domaines : a) la protection des enfants en ligne et la diffusion non consentie d'images intimes ; b) les actifs virtuels en relation avec la cybercriminalité et les preuves électroniques ; c) l'IA ;

- soutenir de manière constructive le nouveau traité des Nations Unies contre la cybercriminalité, notamment en coopérant avec l'ONUDC ;

- préparer de nouveaux projets et mobiliser des ressources extrabudgétaires ;

- allouer les ressources nécessaires à la gestion du Bureau.

En 2024 aussi, le C-PROC a grandement contribué au renforcement de la législation et des capacités de la justice pénale en matière de cybercriminalité et de preuves électroniques dans le monde entier, conformément à la Convention sur la cybercriminalité et à ses protocoles additionnels, ainsi qu'aux obligations en matière de droits humains et d'État de droit. Pour ce faire, il a déployé plus de 310 activités dans le cadre de sept projets, pour un montant cumulé de plus de 34 millions d'euros.

L'intérêt accru pour la Convention sur la cybercriminalité et l'adhésion à celle-ci, ainsi que l'alignement des législations nationales de pays du monde entier sur ses dispositions sont autant de réussites à mettre au compte des activités menées par le C-PROC depuis 2014.

La coopération entre le Bureau et le T-CY a été particulièrement fructueuse en 2024, le C-PROC ayant facilité les travaux du T-CY sur l'article 26 de la Convention (« Information spontanée ») et sur les actifs virtuels, et ayant organisé les échanges du T-CY avec les entreprises (en plus de cofinancer la participation aux sessions plénières du T-CY). La valeur du triangle dynamique — normes communes, suivi/évaluations et renforcement des capacités — s'en est trouvée une nouvelle fois soulignée.

L'élaboration de projets et la mobilisation des ressources ont continué de représenter une part importante des activités du C-PROC. En 2024, le Bureau a lancé cinq nouveaux projets, qui tous visaient, entre autres, à soutenir l'application du Deuxième Protocole additionnel sur les preuves électroniques. L'un de ces projets porte spécifiquement sur les preuves électroniques des crimes de guerre en Ukraine (son financement n'est toutefois pas encore entièrement garanti).

L'audit interne réalisé par la Direction de l'Audit interne, de l'Évaluation et de l'Investigation en 2024 a confirmé les conclusions des nombreux audits et évaluations précédents, notamment en ce qui concerne la gestion des risques et les contrôles internes du Bureau, ainsi que sa capacité à respecter ses obligations contractuelles envers les donateurs.

Entre 2022 et 2024, le C-PROC a soutenu la participation d'experts des Parties à la Convention et des États invités à y adhérer au processus de négociation du traité des Nations Unies. Leur participation a contribué à ce que le traité contre la cybercriminalité adopté par l'Assemblée générale des Nations Unies en décembre 2024 soit largement conforme à la Convention sur la cybercriminalité et prévoie un minimum de garanties en matière de droits humains.

Le C-PROC devrait conserver son statut d'acteur mondial du renforcement des capacités pour lutter contre la cybercriminalité. D'importantes ressources supplémentaires seront nécessaires pour répondre à l'augmentation des demandes d'un nombre croissant de pays. En 2025 et au-delà, le C-PROC devra en priorité :

- soutenir l'application at la ratification du Deuxième Protocole additionnel sur les preuves électroniques ;
- répondre aux défis de l'IA concernant la cybercriminalité et les preuves électroniques ;
- lutter contre l'utilisation des actifs virtuels à des fins criminelles ;
- prendre des mesures contre l'exploitation et les abus sexuels d'enfants en ligne ainsi que la diffusion non consentie d'images intimes ;
- élargir la portée des normes du Conseil de l'Europe relative à l'IA, à la protection des données, à la protection des enfants, etc. au-delà de l'Europe ;
- soutenir l'application du nouveau traité des Nations Unies contre la cybercriminalité en coopération avec l'ONUDC, le cas échéant.