Documents d'information

SG/Inf(2024)12

5 avril 2024

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

Rapport d'activité du C-PROC pour 2023

Contenu

Résumé

Le Bureau du Programme Cybercriminalité du Conseil de l'Europe (ci-après "C-PROC" ou le "Bureau") à Bucarest, Roumanie, est responsable de la mise en œuvre de projets de renforcement des capacités en matière de cybercriminalité et de preuves électroniques sur la base de la Convention sur la cybercriminalité (STE n° 185) et dans toutes les régions du monde. Le Bureau a été créé il y a dix ans, suite à une décision du Comité des Ministres en octobre 2013. Le présent rapport vise à informer le Comité des Ministres des activités du C-PROC en 2023.

Au cours des dix années qui ont suivi sa création, le C-PROC – à travers plus de 2 100 activités bénéficiant à plus de 130 pays – a contribué de manière significative au renforcement des capacités de la législation et de la justice pénale en matière de cybercriminalité et de preuves électroniques dans le monde entier, conformément à la Convention sur la cybercriminalité et aux exigences en matière de droits humains et d'État de droit. Entre 2013 et 2023, le nombre d'États dotés d'un droit pénal matériel conforme à cette Convention est passé de 70 à 131. Le renforcement des capacités par le C-PROC a été un facteur majeur de l'élargissement de la portée et de l'adhésion à cette convention (de 41 parties en 2013 à 69 à la fin de 2023).

Le Bureau a attiré plus de 60 millions d'euros de ressources extrabudgétaires, qui ont été correctement gérées, comme le confirment les audits et les évaluations. En 2023, l'Union européenne (UE) a été le principal donateur dans le cadre de projets conjoints, et les États-Unis, le Japon, le Royaume-Uni et d'autres pays ont contribué au financement du projet Octopus. Tout en s'appuyant sur des contributions volontaires, le C-PROC est devenu une structure durable qui devrait continuer à fonctionner de la même manière à l'avenir.

En 2023, le Bureau, à travers six projets (avec un budget cumulé de plus de 49 millions d'euros et une quarantaine de personnes), a soutenu 305 activités dans toutes les régions du monde (dont 102 évènements de formation pour les juges, les procureurs et les enquêteurs) avec, en point d'orgue, la conférence Octopus à Bucarest, en Roumanie, du 13 au 15 décembre.

Le C-PROC, en 2022 et 2023, a permis la participation d'experts des Parties et des États invités à adhérer à la Convention sur la cybercriminalité au Comité ad hoc des Nations Unies chargé d'élaborer un traité sur « l'utilisation des technologies de l'information et des communications (TIC) à des fins criminelles » (UN AHC) pour s'assurer que ce futur traité – s'il est adopté – est cohérent avec la Convention sur la cybercriminalité et comprend au moins un minimum de garanties en matière de droits humains et d'État de droit. Jusqu'à présent, ce processus a suscité un intérêt accru pour la Convention sur la cybercriminalité, comme le confirment les nombreuses demandes d'adhésion depuis son lancement.

Avec ou sans traité supplémentaire des Nations Unies, la Convention sur la cybercriminalité avec ses protocoles et le Comité de la Convention sur la cybercriminalité (T-CY) resteront le cadre international le plus pertinent en matière de cybercriminalité dans les années à venir, notamment parce qu'ils sont soutenus par les activités de renforcement des capacités du C-PROC.

En décembre 2023, plusieurs projets du C-PROC ont été achevés, ce qui a entraîné une diminution des ressources disponibles. Cependant, cinq nouveaux projets ont depuis été préparés avec un financement largement mobilisé, et un lancement entre janvier et mars 2024. Des contributions volontaires supplémentaires sont néanmoins nécessaires pour répondre aux demandes croissantes.

Les priorités pour 2024 comprennent le soutien à la mise en œuvre du deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE n° 224), le renforcement des capacités d'utilisation des preuves électroniques pour la poursuite judiciaire des crimes de guerre en Ukraine, l'aide aux pays – en particulier ceux déjà invités à adhérer à la Convention sur la cybercriminalité – pour qu'ils deviennent Parties tout en respectant les exigences en matière de droits humains et d'État de droit, et l'aide aux autorités de justice pénale pour relever les défis liés aux attaques de ransomwares et aux crypto-monnaies.

1. Cadre et objet du présent rapport

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 à Bucarest, Roumanie, en 2023[1].

Le Bureau est devenu opérationnel en avril 2014, à la suite d'une offre du gouvernement roumain[2] et d'une décision du Comité des Ministres en octobre 2013[3]. Son objectif est d'assurer la mise en œuvre des projets de renforcement des capacités sur la cybercriminalité du Conseil de l'Europe dans toutes les régions du monde.

Étant donné que le C-PROC fonctionne maintenant depuis dix ans, ce rapport comprend également un examen sommaire de ses réalisations.

2. Bilan : Dix ans de C-PROC

Fondement

Le Conseil de l'Europe a commencé à soutenir la mise en œuvre de la Convention sur la cybercriminalité[4] par des activités initiales de renforcement des capacités à partir de 2002 et par des projets spécifiques, mais avec des ressources limitées, à partir de 2006.

En février 2013, la deuxième réunion du groupe intergouvernemental d'experts des Nations Unies sur la cybercriminalité a conclu que le renforcement des capacités était non seulement un moyen efficace de relever le défi de la cybercriminalité, mais aussi le domaine qui faisait l'objet du plus large consensus international. Il est apparu clairement qu'une approche plus cohérente de la part de la communauté internationale était nécessaire à cet égard.

La décision du Comité des Ministres en octobre 2013 de créer un bureau dédié chargé de soutenir les pays du monde entier dans le renforcement de leurs capacités de justice pénale, conformément à la Convention sur la cybercriminalité et aux exigences en matière de droits humains et de l'État de droit, a été la réponse du Conseil de l'Europe. Suite à une offre du gouvernement roumain, le C-PROC a été établi à Bucarest.

---

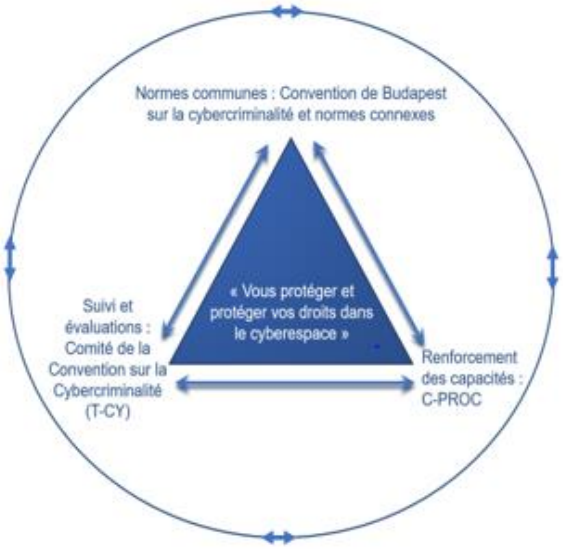
[1] La décision portant création de l'Office demandait au Secrétaire Général de présenter ces rapports annuels.
Pour le rapport couvrant la période d'avril 2014 à septembre 2015, voir ce rapport (disponible en anglais uniquement).
Pour la période d'octobre 2015 à septembre 2016, voir ce rapport (disponible en anglais uniquement).
Pour la période d'octobre 2016 à septembre 2017, voir ce rapport.
Pour la période d'octobre 2017 à septembre 2018, voir ce rapport.
Pour la période d'octobre 2018 à septembre 2019, voir ce rapport.
Pour la période d'octobre 2019 à septembre 2020, voir ce rapport.
Pour la période d'octobre 2020 à septembre 2021, voir ce rapport.
Pour la période d'octobre 2021 à décembre 2022, voir ce rapport.

[2] Le C-PROC est situé à la Maison des Nations Unies à Bucarest. L'espace de bureau est alloué à titre gracieux au Conseil de l'Europe par le gouvernement roumain dans le cadre d'un protocole d'accord.

[3] Décisions CM/Del/Dec(2013)1180/10.4, 9 octobre 2013, lors de leur 1180ème réunion.

[4] La Convention de Budapest sur la cybercriminalité (STE n°185) est 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, et le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif à la coopération renforcée et à la divulgation des preuves électroniques (STCE n°224) de 2022. La mise en œuvre de ces protocoles est également soutenue par le C-PROC.

L'approche du Conseil de l'Europe en matière de cybercriminalité consiste en un triptyque : (a) normes communes (Convention sur la cybercriminalité, Protocoles et instruments connexes) ; (b) suivi et évaluations par le Comité de la Convention sur la cybercriminalité (T-CY) ; et (c) renforcement des capacités par le C-PROC.



Le concept de renforcement des capacités en matière de cybercriminalité, tel qu'il a été formulé en 2013[5], s'est avéré valable et continue de guider le travail du C-PROC.

Bien que le C-PROC puisse entamer un dialogue avec tout pays ou territoire et le soutenir dans l'élaboration d'une législation conforme à la Convention sur la cybercriminalité, la priorité est donnée aux États qui sont Parties à ce traité, qui ont demandé à y adhérer ou qui ont été invités à le faire. Les projets du C-PROC soutiennent ensuite les gouvernements respectifs et les institutions de justice pénale dans la mise en œuvre de la Convention (et de ses Protocoles).

Projets, activités et impact

En avril 2014, le Bureau a commencé ses activités en soutenant les pays à travers trois projets avec un budget combiné d'environ 8 millions d'euros. En décembre 2023, le C-PROC gérait des projets dont le budget total s'élevait à plus de 49 millions d'euros. Des ressources extrabudgétaires s'élevant à environ 60 millions d'euros ont été mobilisées au cours des dix dernières années[6].

Entre avril 2014 et décembre 2023, le C-PROC a soutenu plus de 2 100 activités[7] au profit de plus de 130 pays[8] dans toutes les régions du monde.

Les projets ont généralement contribué à renforcer :

- la législation nationale sur la cybercriminalité et les preuves électroniques, ainsi que sur la protection des données ou sur l'exploitation sexuelle des enfants en ligne et les abus sexuels ;

- les stratégies et les politiques en matière de cybercriminalité, y compris la sensibilisation des décideurs politiques ;

- les capacités des services répressifs, notamment par le biais de procédures opérationnelles normalisées, d'outils de saisie des crypto-monnaies et autres ;

[5] Conseil de l'Europe / Projet mondial sur la cybercriminalité (2013) : Renforcement des capacités en matière de cybercriminalité, document de travail. (https://rm.coe.int/16802fa3e6) (disponible en anglais uniquement)
[6] Ce montant ne comprend pas les 10 % de cofinancement du Conseil de l'Europe pour des projets communs avec l'UE. Des informations sur les projets passés et actuels sont disponibles ici : Bureau de programme pour la cybercriminalité (C-PROC) – Cybercriminalité (coe.int).
[7] L'inventaire complet des activités soutenues par le C-PROC depuis avril 2014 est disponible ici : https://rm.coe.int/cproc-reps-inventory-activities-v38-29nov2023/1680ad9884 (disponible en anglais uniquement).
[8] Ce nombre de "130 pays" comprend un soutien détaillé à quelque 35 à 40 pays prioritaires bénéficiant de l'ensemble des activités de renforcement des capacités sur plusieurs années, ainsi qu'un soutien à plus de 95 pays pour des réformes législatives nationales ou la participation de leurs experts en justice pénale à de multiples activités régionales ou internationales de formation et autres. Ce nombre ne comprend pas les experts d'une cinquantaine d'autres pays qui n'ont participé qu'à quelques activités. Seuls 12 des 193 États membres de l'ONU n'ont pas du tout participé aux activités du C-PROC depuis 2014.

- la formation judiciaire sur la cybercriminalité et les preuves électroniques ;

- la coopération public/privé, en particulier entre les prestataires de services et les autorités de justice pénale ;

- la coopération entre les organismes de cybersécurité (y compris les centres de veille, d'alerte et de réponse aux attaques informatiques (Computer Security Incident Response Team – CSIRT)) et les autorités de justice pénale ;

- la coopération internationale, y compris la rationalisation des procédures d'assistance mutuelle, des modèles de demande et d'autres outils, et le renforcement des points de contact 24/7.

Les activités ont également contribué à l'Agenda 2030 des Nations Unies pour le développement durable, en particulier à l'objectif de développement durable 16 (« Promouvoir l'avènement de sociétés pacifiques et inclusives aux fins du développement durable, assurer l'accès de tous à la justice et mettre en place, à tous les niveaux, des institutions efficaces, responsables et ouvertes à tous »).

Les projets et les activités connexes ont produit des résultats et un impact à plusieurs niveaux, à commencer par les fonctionnaires de la justice pénale qui sont plus compétents et mieux équipés pour relever les défis de la cybercriminalité et des preuves électroniques. Le développement des capacités pour une formation durable par les académies de formation judiciaire et d'application de la loi a été une priorité.

Des enquêtes et des poursuites fructueuses, y compris des opérations internationales, sont menées dans le monde entier. Cela est souvent le résultat du cadre juridique associé aux compétences, aux outils et aux plates-formes de coopération fournis par le C-PROC, en plus des relations de confiance résultant des activités régionales et internationales.

Une nette augmentation du nombre de pays dotés d'une législation nationale sur la cybercriminalité et les preuves électroniques peut être attribuée au C-PROC. Pour illustrer ce point, en 2013, quelque 70 États avaient adopté des dispositions sur les infractions commises à l'encontre et au moyen de systèmes informatiques conformément à la Convention sur la cybercriminalité, en comparaison, ils étaient environ 130 en décembre 2023[9].

Le renforcement des capacités par le C-PROC a été un facteur majeur de l'augmentation du nombre de membres de la Convention sur la cybercriminalité :

- En 2013, 41 États étaient Parties, 2 États l'avaient signée et 10 États avaient été invités à y adhérer.

- En décembre 2023, 69 États étaient Parties, 2 États l'avaient signée et 20 États avaient été invités à y adhérer.

Le C-PROC a en outre soutenu le T-CY. Par exemple, le projet Octopus et d'autres projets ont soutenu la participation des représentants des Parties et des États invités à adhérer aux réunions du T-CY. Le projet Octopus a également cofinancé l'interprétation en espagnol lors des séances plénières du T-CY.

[9] Le C-PROC suit de près l'évolution de la législation sur la cybercriminalité dans le monde depuis 2013 et publie une fois par an un aperçu de "l'état mondial de la législation sur la cybercriminalité".
https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0
(disponible en anglais uniquement)

En 2022 et 2023, le C-PROC a également facilité la signature du nouveau Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques[10]. En décembre 2023, 43 États avaient signé ce Protocole (dont deux l'avaient également ratifié)[11].

Le C-PROC a renforcé la réponse de la justice pénale à la cybercriminalité qui est non seulement efficace, mais qui répond également aux exigences en matière de droits humains et d'État de droit, y compris la protection des données. Au niveau politique, le C-PROC a ainsi contribué à un cyberespace libre, ouvert et mondial et au modèle multipartite de gouvernance de l'internet.

Au cours de ces dix années, les projets du C-PROC ont dû s'adapter à de nouveaux défis. C'est le cas, par exemple :

- Afin de lutter contre la prolifération des attaques de ransomware et des flux financiers illicites connexes via les crypto-monnaies, à partir de 2021, le C-PROC a organisé des formations, des ateliers ou des exercices de simulation pratique à l'échelle nationale, régionale et internationale à l'intention des praticiens, et a élaboré un guide sur la saisie des crypto-monnaies et la conduite d'enquêtes criminelles sur les attaques de ransomware. Ces documents complètent la note d'orientation sur les ransomwares adoptée par le T-CY[12].

- La pandémie de covid-19 a contraint le C-PROC à changer le mode d'exécution des activités à partir de mars 2020. En quelques semaines, le C-PROC était prêt à mener des activités en ligne. De nombreuses ressources, guides et autres outils en ligne ont depuis été développés ou améliorés[13]. Le cours d'apprentissage en ligne HELP sur la cybercriminalité et les preuves électroniques a été lancé[14], traduit en 14 langues et plus de 3 800 personnes s'étaient inscrites avant la fin de l'année 2023. La plateforme CYBOX pour la formation en ligne sur la cybercriminalité et les preuves électroniques est sur le point de devenir opérationnelle[15].

- Le début de l'agression à grande échelle de la Fédération de Russie contre l'Ukraine en février 2022, a mis au premier plan la question des preuves électroniques liées aux crimes de guerre et aux violations flagrantes des droits humains. Dans le cadre du projet conjoint CyberEast avec l'Union européenne (EU), le C-PROC a préparé une analyse des lacunes en ce qui concerne la collecte et le traitement de ces preuves, organisé une formation en criminalistique pour les enquêteurs et les procureurs, formé les juges à la cybercriminalité et aux preuves électroniques et, en 2023, conçu un projet spécifique – CyberUA – pour aider l'Ukraine à relever ce défi d'une manière plus globale. Ce projet a été lancé au début de l'année 2024.

[10] Y compris la conférence pour l'ouverture aux signatures en mai 2022.
Opening for signature of the Second additional Protocol to the Cybercrime Convention - Cybercriminalité (coe.int)
[11] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.
[12] https://rm.coe.int/t-cy-2022-14-note-d-orientation-numero-12-logiciels-ranconneurs/1680a9355f.
(disponible en anglais uniquement)
[13] Voir par exemple la ressource sur la cyberviolence Cyberviolence - Cyberviolence (coe.int) ou les ressources disponibles sur le site Home - Octopus Cybercrime Community (coe.int).
[14] Voir https://www.coe.int/fr/web/cybercrime/-/council-of-europe-help-online-course-on-cybercrime-and-electronic-evidence.
[15] Voir https://www.coe.int/fr/web/cybercrime/cybox.

- Dans un nombre croissant de pays, y compris dans certaines Parties à la Convention sur la cybercriminalité ou dans des États qui souhaitent y adhérer, la législation sur la cybercriminalité comprend des dispositions qui criminalisent la "diffusion de fausses informations", les "messages offensants", le fait de "causer du tort", la "propagation de rumeurs" et d'autres comportements. Dans certains cas, ces dispositions peuvent restreindre la liberté d'expression au-delà de ce qui est nécessaire et proportionné. Les projets du C-PROC tiennent compte de cette préoccupation lorsqu'ils fournissent des conseils sur la législation. En décembre 2023, un document de discussion a été produit pour faciliter un dialogue plus structuré sur cette question[16].

- En 2022, la Convention sur la cybercriminalité a été complétée par le Deuxième Protocole additionnel relatif au renforcement de la coopération et à la divulgation des preuves électroniques (STCE n° 224). Le C-PROC a encouragé la mise en œuvre de ce Protocole en 2022 et 2023, et un soutien supplémentaire est désormais intégré dans tous les nouveaux projets du C-PROC.

- En adoptant la résolution 74/247[17] en décembre 2019, l'Assemblée générale des Nations Unies (AGNU) a créé un comité spécial chargé « d'élaborer une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et des communications (TIC) à des fins criminelles ». Les négociations proprement dites ont débuté le 28 février 2022 et devaient s'achever au cours de six sessions de négociation d'ici février 2024[18]. Le C-PROC a soutenu la participation d'experts des Parties et des États invités à adhérer à la Convention sur la cybercriminalité à ce processus conventionnel afin que le futur traité supplémentaire soit conforme aux normes de la Convention sur la cybercriminalité ainsi qu'aux exigences en matière de droits humains et d'État de droit. L'expérience acquise au cours de ces négociations et les dernières versions du projet de texte de la convention des Nations Unies ont confirmé la nécessité et la valeur de ce soutien[19]. En permettant aux États membres des Nations Unies participant à ce processus de mieux comprendre les avantages du cadre de la Convention sur la cybercriminalité, on a suscité un intérêt accru pour cette dernière. Depuis le début de ce processus en février 2022, le Cameroun, la Corée, la Côte d'Ivoire, l'Équateur, la Grenade, le Kazakhstan, Kiribati, le Mozambique, le Rwanda, Sao Tomé-et-Príncipe, la Sierra Leone, le Timor-Oriental et l'Uruguay ont demandé à adhérer à la Convention sur la cybercriminalité. Le Brésil, le Cameroun et le Nigeria y sont également devenus Parties.

En bref, au cours des dix premières années qui ont suivi sa création, C-PROC :

- a contribué de manière significative au renforcement de la législation et des capacités de la justice pénale en matière de cybercriminalité et de preuves électroniques, conformément à la Convention sur la cybercriminalité et aux exigences en matière de droits humains et d'État de droit dans le monde entier ; le nombre de membres de cette convention a considérablement augmenté grâce au soutien du C-PROC ;

---

[16] Cybercriminalité et liberté d'expression : Un document de réflexion - Cybercriminalité (coe.int) (disponible en anglais uniquement).

[17] La résolution a été proposée par la Fédération de Russie.

[18] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
(disponible en anglais uniquement).
N.B. En février 2024, le AHC de l'ONU a décidé de suspendre la 7ème session et de la reprendre en juillet ou août 2024 afin de parvenir à un accord sur un projet de texte de convention additionnelle. Cette session prolongée doit encore être confirmée.

[19] Note : pour chaque session, le Bureau du Comité de la Convention sur la cybercriminalité a également préparé des notes d'information pour faciliter la coordination et les positions communes des Parties à la Convention.

- a permis un rayonnement mondial, a généré des partenariats et des synergies avec de nombreuses organisations et initiatives, et a produit des résultats et un impact dans toutes les régions du monde ;

- a attiré un financement extrabudgétaire considérable de la part des donateurs ; et

- est devenu synonyme de renforcement des capacités en matière de cybercriminalité et de preuves électroniques.

De nombreux audits et évaluations ont confirmé que le Bureau est géré de manière rentable et que les ressources confiées au Conseil de l'Europe par les donateurs sont utilisées conformément aux règles et procédures.

3. Aperçu des projets et des réalisations en 2023

La Conférence Octopus sur la coopération en matière de cybercriminalité (Bucarest, Roumanie, du 13 au 15 décembre 2023) a été le point culminant d'une nouvelle année de succès du C-PROC en termes de rayonnement et d'impact dans le monde. Plus de 500 experts de quelque 130 pays ont participé à cette conférence à laquelle le Secrétaire Général adjoint du Conseil de l'Europe a également pris la parole. Octopus 2023 a de nouveau servi de catalyseur pour la coopération mondiale en matière de cybercriminalité et de preuves électroniques. Outre les séances plénières et les ateliers, la conférence comprenait des événements de clôture pour les projets qui s'achèvent et des événements de lancement pour les nouveaux projets du C-PROC. Cette conférence a été précédée de plus de 300 autres activités en 2023.

Projets

En 2023, le C-PROC avait cinq projets régionaux et mondiaux en cours de mise en œuvre, et un sixième projet (GLACY-e) a été introduit progressivement à partir d'août 2023.

En décembre 2023, les budgets combinés des projets en cours s'élevaient à quelque 49,7 millions d'euros, ce qui représente une nouvelle augmentation par rapport à l'année précédente[20].

Toutefois, sur ces six projets, quatre étaient en cours d'achèvement ou de finalisation avant la fin de l'année 2023.

Entre janvier et décembre 2023, le C-PROC, avec une quarantaine d'agents, a soutenu environ 305 activités dans le cadre des projets suivants :

[20] Septembre 2015 : 6 millions EUR, septembre 2016 : 22 millions d'euros, septembre 2017 : 24,4 millions d'euros, septembre 2018 : 26,7 millions d'euros, septembre 2019 : 32,3 millions d'euros, septembre 2020 : 38 millions d'euros, septembre 2021 : 38 millions d'euros ; décembre 2022 : 39,2 millions d'euros.

Titre du projet	Durée de l'accord	Budget	Financement
Projet GLACY+ sur l'action globale contre la cybercriminalité élargie	mars 2016 - février 2024	18,9 millions d'euros	Projet conjoint UE/CdE (dont 10% OB/JPP du Conseil de l'Europe[21])
Projet GLACY-e sur l'action globale contre la cybercriminalité renforcée	août 2023 - janvier 2026	5,55 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
Projet OCTOPUS	janvier 2021 - décembre 2027	10 millions d'euros[22]	Contributions volontaires (Canada, États-Unis, Hongrie, Islande, Italie, Japon, Pays-Bas et Royaume-Uni)
Projet iPROCEEDS-2 visant à lutter contre les produits du crime sur l'internet et à sécuriser les preuves électroniques en Europe du Sud-Est et en Turquie	janvier 2020 - décembre 2023	4,95 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
CyberSouth sur le renforcement des capacités dans le voisinage sud	juillet 2017 - décembre 2023	5 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
Projet CyberEast sur l'action contre la cybercriminalité pour la cyber-résilience dans la région du partenariat oriental	juin 2019 - décembre 2023	5,33 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)

Un inventaire détaillé des activités soutenues ou réalisées est disponible en ligne.

Le Bureau dépend de financements externes. Le projet Octopus est entièrement financé par des contributions volontaires, tandis que les projets conjoints avec l'UE sont cofinancés à hauteur de 10 % par le programme commun du budget ordinaire du Conseil de l'Europe.

Au cours de l'année écoulée, plus de 90 % de son budget a été financé par des ressources extrabudgétaires, c'est-à-dire des contributions volontaires et des contributions de l'UE à des projets conjoints. L'UE est restée le principal donateur par le biais de projets conjoints cofinancés par le Conseil de l'Europe. En 2023, les États-Unis d'Amérique ont à nouveau mis à disposition un financement important pour le projet Octopus, auquel le Royaume-Uni, le Japon et l'Islande ont ajouté des contributions. Le Bureau compte également sur le soutien du gouvernement roumain, qui continue à mettre à sa disposition des bureaux à titre gracieux.

Au cours des dix dernières années, le C-PROC a pu compter sur des ressources de plus en plus importantes qui lui ont permis de répondre aux demandes croissantes de soutien émanant d'un nombre de plus en plus important de pays engagés dans la mise en œuvre de la Convention sur la cybercriminalité et de ses Protocoles.

Toutefois, les projets CyberSouth, CyberEast et iPROCEEDS-2 se terminant en décembre 2023, GLACY+ se terminant en février 2024 et le projet Octopus souffrant d'un manque de financement, le C-PROC est confronté à une diminution des ressources disponibles en 2024. Il pourrait s'agir d'un défi temporaire, car plusieurs nouveaux projets devraient commencer au début de 2024 (voir la section 4 ci-dessous).

[21] Programme conjoint du budget ordinaire du Conseil de l'Europe (OB/JPP).
[22] Le financement n'est pas encore totalement assuré.

Réalisations

Capacités de la justice pénale

En 2023, le C-PROC a contribué de manière significative au renforcement des capacités de la justice pénale, en particulier dans les 35-40 pays prioritaires qui étaient éligibles à un large éventail d'assistance. Plus de 90 autres pays ont participé à au moins une partie des activités.

Voici quelques exemples d'activités spécifiques :

- **Projet Octopus :** Le projet a favorisé la promotion du dialogue international, la coopération et l'engagement par l'organisation d'initiatives régionales et internationales, telles que la Conférence Octopus, la Conférence internationale sur la coopération en Afrique, des sessions consacrées aux crimes de guerre et aux preuves électroniques lors du FGI 2023 à Kyoto et du Forum mondial pour la démocratie, ainsi que le soutien à des événements tels que la Conférence sur la lutte contre les botnets et les écosystèmes de logiciels malveillants, la Conférence sur la cybercriminalité à Rome, le Sommet RightsCon, la Conférence mondiale sur le renforcement des capacités cybernétiques au Ghana, la 2ème Conférence du Sommet des affaires cybernétiques en Argentine, l'Atelier régional pour les parlementaires des Caraïbes, le Symposium international sur la réponse à la cybercriminalité en Corée du Sud, le Sommet législatif de l'Afrique de l'Est, ou la Conférence annuelle d'EUROPOL sur la cybercriminalité.
  L'accent a été mis en particulier sur la pérennisation de la formation judiciaire en Afrique mais aussi au niveau international, sur l'amélioration des compétences et des connaissances des procureurs ibéro-américains et lusophones spécialisés dans la cybercriminalité, sur la promotion de la coopération public/privé en Amérique latine, sur la lutte contre l'exploitation et les abus sexuels des enfants en ligne, sur le renforcement du réseau des points de contact 24/7, sur le soutien à la mise en œuvre du deuxième Protocole additionnel et sur la mise en œuvre d'une série d'activités consacrées à la xénophobie et au racisme en ligne.
  L' action CYBERKOP au Kosovo*[23] a été lancée.
  Les évaluations législatives et les missions de conseil ont soutenu la Barbade, le Cameroun, le Ghana, le Kazakhstan, la Malaisie, le Malawi, la Mauritanie, le Mexique et les Seychelles, et ont fourni de nouvelles pistes pour renforcer les cadres juridiques.
  Un certain nombre de ressources ont été mises à disposition, telles que l'étude sur la mise en œuvre du premier Protocole additionnel à la Convention sur la cybercriminalité sur la xénophobie et le racisme, un document de réflexion sur la cybercriminalité et la liberté d'expression, la ressource actualisée sur la cyberviolence et la plateforme de formation en ligne CYBOX sur la cybercriminalité et les preuves électroniques.

  Le projet Octopus a soutenu les travaux du T-CY et a facilité la coordination des positions et la participation d'experts d'Afrique, d'Amérique latine, d'Asie-Pacifique, et des Caraïbes au Comité consultatif de l'ONU chargé de préparer un nouveau traité sur la cybercriminalité.

  Le projet a soutenu une soixantaine d'activités en 2023.

[23] *Toutes les références au Kosovo, qu'il s'agisse du territoire, des institutions ou de la population, dans le présent texte doivent être comprises dans le plein respect de la résolution 1244 du Conseil de sécurité des Nations Unies et sans préjudice du statut du Kosovo.

- **CyberEast** : Grâce au soutien du projet, l'Arménie est devenu le 43ème État à signer le deuxième Protocole additionnel à la Convention sur la cybercriminalité en novembre 2023. Le rapport régional sur l'article 15 (sauvegardes et garanties) a été mis à jour pour refléter l'état des lieux en 2023 pour la région du partenariat oriental.
  Le projet s'est concentré sur la réalisation de sessions de formation sur la cybercriminalité et les preuves électroniques à trois niveaux (introduction, intermédiaire et avancé) pour tous les pays du projet, tous les principaux groupes cibles (forces de l'ordre, procureurs, juges), en coopération avec les institutions de formation dans la mesure du possible, et en engageant les avocats de la défense dans le renforcement des capacités pour la première fois en Géorgie et en République de Moldavie.
  En outre, le projet a renforcé les capacités des autorités de justice pénale et la coopération interagences par le biais d'une série de formations sur la gestion des cyber incidents et les types de cybercriminalité, les enquêtes financières, le renseignement de source ouverte, et a organisé deux exercices régionaux de coopération cybernétique phares en Géorgie et en Roumanie.
  Le projet s'est engagé avec la société civile tant au niveau national (République de Moldavie, Ukraine) qu'au niveau régional (EuroDIG 2023) afin d'aborder les questions de contrôle et de responsabilité en matière de lutte contre la cybercriminalité. Parmi les initiatives régionales conjointes, on peut citer l'exercice régional sur les équipes communes d'enquête dans le cadre du deuxième Protocole additionnel, deux discussions régionales sur les enquêtes financières parallèles et le renseignement, et la coopération entre les Centres de veille, d'alerte et de réponse aux attaques informatiques (Computer Security Incident Response Team – CSIRT) et les services répressifs dans le cadre de la semaine de la cybercriminalité en République de Moldavie.
  Le soutien ciblé à l'Ukraine (en plus de son plein engagement dans les activités régionales) comprenait une étude sur les lacunes et les défis concernant les preuves électroniques des crimes de guerre et des infractions connexes, une formation criminalistique de niveau intermédiaire pour les services répressifs, et une formation judiciaire spécifique pour les juges des régions de Dnipro et d'Odessa.
  Le projet s'est achevé en décembre 2023 avec l'adoption d'une nouvelle déclaration sur les priorités stratégiques de la coopération en matière de cybercriminalité dans la région du partenariat oriental.
  41 activités ont été soutenues par ce projet au cours de cette période.

- **iPROCEEDS-2** : Une coopération plus étroite entre les autorités de justice pénale et la communauté de la cybersécurité a été réalisée grâce à des exercices internationaux basés sur des scénarios, des ateliers nationaux, des conférences, des séminaires, des formations, des réunions, des simulations régionales et des symposiums conjoints, axés sur les enquêtes sur les cyberattaques, la gestion des incidents, et la promotion des normes et réglementations internationales.
  Les capacités des services répressifs ont été renforcées grâce à des activités conjointes consacrées aux enquêtes sur les crypto-monnaies, à l'OCSEA (exploitation et abus sexuels d'enfants en ligne), aux enquêtes financières, à l'accès à des bases de données spécialisées et à de nouveaux outils de coopération.
  La réunion annuelle des points de contact 24/7 a servi de plateforme pour l'échange de modèles opérationnels et le renforcement des capacités. Des liens plus étroits entre les secteurs public et privé ont été établis en soutenant des réunions nationales, l'accent étant mis sur la coopération entre les autorités de justice pénale et les prestataires de services. La Conférence sur l'économie souterraine a permis de partager les derniers outils développés par le secteur.

L'expertise des juges et des procureurs dans le traitement des affaires de cybercriminalité a été renforcée grâce à une formation durable sur les preuves électroniques, la coopération internationale et la certification des compétences de formation.
Le projet a soutenu quelque 110 activités au cours de cette période.

- **CyberSouth** : le travail sur la législation et sa conformité avec les normes du Conseil de l'Europe s'est poursuivi avec la Tunisie en vue de son adhésion à la Convention sur la cybercriminalité, avec la Jordanie et avec le Liban, y compris sur la législation relative à la protection des données.
  Les capacités judiciaires de lutte contre la cybercriminalité ont été renforcées en Algérie, au Liban, au Maroc et en Tunisie, où les modules de formation des formateurs ont conduit à la création de pools de formateurs nationaux et où les institutions nationales ont intégré le programme de lutte contre la cybercriminalité dans les programmes d'études nationaux. Le partenariat public/privé s'est amélioré dans tous les pays prioritaires, y compris avec les fournisseurs de services multinationaux, ce qui a entraîné une augmentation du nombre de demandes internationales.
  Le travail d'application de la loi a été soutenu en facilitant la formation continue et les exercices pratiques. La coopération internationale sur la cybercriminalité dans les régions du Moyen-Orient et de l'Afrique du Nord (MENA) et de l'Afrique a été renforcée grâce à la Conférence internationale organisée à Bouznika (Maroc) avec la participation de 34 pays. Une coordination sur les questions cybernétiques avec la Ligue des États arabes ainsi que des contacts avec les nouveaux partenaires ont été établis en vue de la prochaine phase du projet, CyberSouth+.
  Le projet a soutenu quelque 52 activités au cours de cette période.

- **GLACY+ :** Des réformes législatives et des révisions de politiques ont été soutenues en Afrique, en Amérique latine, en Asie et dans le Pacifique sur la cybercriminalité et les preuves électroniques (Cameroun, Malawi, Mexique, Mozambique, Nauru, Népal, Nigéria, République dominicaine, Rwanda, Timor-Oriental). Des activités spécifiques au Ghana, au Mexique, au Pérou, en République dominicaine et en Uruguay ont renforcé le dialogue entre les décideurs politiques et les praticiens.
  Les ateliers de conseil sur la recherche, la saisie et la confiscation des produits de la criminalité en ligne organisés par INTERPOL, partenaire du projet, au Bénin, en Colombie, au Costa Rica, en République dominicaine, au Sénégal et au Sri Lanka ont permis d'améliorer les connaissances des pays en matière d'enquêtes financières parallèles et certains ont même permis la confiscation des produits de la criminalité en ligne.
  La coopération internationale a été renforcée par une série d'événements annuels axés sur des exercices basés sur des scénarios concernant la conservation des données, l'entraide judiciaire, les enquêtes financières parallèles et d'autres mécanismes de coopération pour l'Afrique et l'Amérique latine. Le cours de formation des formateurs pour les premiers intervenants a été dispensé à quelque 74 futurs formateurs nationaux d'Afrique, d'Amérique latine et d'Asie-Pacifique. Ces formations ont donné lieu à une formation dérivée sur les preuves électroniques pour environ 270 premiers intervenants au Chili, au Paraguay, au Pérou et en République dominicaine, dispensée par des formateurs régionaux/nationaux[24]. 71 professionnels hispanophones[25] ont acquis de meilleures compétences en matière d'enquête, y compris une solide compréhension des méthodologies d'enquête sur les sources ouvertes dans le cadre d'une formation en ligne de six semaines sur les principes fondamentaux de l'enquête sur les sources ouvertes.

[24] Avec un peu de soutien logistique (restauration) ou pas de soutien du tout de la part du projet.
[25] De l'Argentine, du Brésil, du Chili, de la Colombie, du Costa Rica, de l'Équateur, du Paraguay, du Pérou et de l'Uruguay.

GLACY+ a approfondi l'accent mis sur la formation judiciaire en organisant des ateliers de formation nationaux au Chili, en Côte d'Ivoire, au Ghana, au Kenya, au Nigéria et au Pérou, ainsi qu'une série d'ateliers entre praticiens organisés dans le cadre du Réseau international de formateurs judiciaire nationaux de C-PROC.
Plusieurs ateliers et événements thématiques régionaux et internationaux ont été organisés dans le cadre du projet : des Réunions du réseau des procureurs ibéro-américains spécialisés dans la cybercriminalité et du Forum des procureurs lusophones spécialisés dans la cybercriminalité[26], un atelier réalisé en association Eurojust/Conseil de l'Europe sur les dispositions relatives à la coopération internationale du deuxième Protocole additionnel à la Convention sur la cybercriminalité[27], l'exercice de simulation CSIRT/LEA régional pour la coopération inter-agences pour certains pays africains[28], un atelier régional sur la coopération public/privé en Amérique latine[29], une réunion régionale sur les stratégies de formation judiciaire pour certains pays africains[30] et le Réseau international plénier des formateurs judiciaires nationaux[31].
En outre, les pays prioritaires et d'autres pays sélectionnés ont bénéficié du soutien du projet pour participer à un certain nombre d'événements internationaux et régionaux : la Conférence internationale sur la cybercriminalité et les preuves électroniques en Afrique, la formation régionale sur les équipes communes d'enquête et l'amélioration de la coopération avec les prestataires de services étrangers dans le cadre du deuxième Protocole additionnel, la Conférence internationale sur la xénophobie et le racisme commis par le biais de systèmes informatiques, la réunion annuelle 2024 du réseau de points de contact 24/7, la Conférence annuelle d'Europol, la Conférence sur l'économie souterraine 2023 et la Conférence Octopus 2023. Le projet a bénéficié d'une certaine visibilité lors de la Conférence mondiale sur le renforcement des cybercapacités, où il a organisé deux sessions sur la durabilité du renforcement des capacités. Quelque 139 activités ont été soutenues par le projet au cours de cette période.

- **GLACY-e :** Ce projet a débuté en août 2023 avec une phase de lancement parallèle au projet GLACY+. Cette phase a permis de clarifier le rôle des hubs et des pays sélectionnés, et d'élaborer le plan de travail pour 2024. En décembre 2023, l'événement de clôture du projet GLACY+ a également servi de conférence de lancement du projet GLACY-e, ce qui a permis d'évaluer l'impact et les résultats du premier projet et de fixer les priorités du second.

[26] Brésil, mai 2023.
[27] Pays-Bas, septembre 2023.
[28] Maurice, septembre 2023.
[29] Chili, novembre 2023.
[30] France, novembre 2023.
[31] Roumanie, décembre 2023.

Études et guides pour les praticiens

En 2023, le C-PROC a préparé des guides et des études supplémentaires afin de fournir aux praticiens des outils pratiques pour enquêter sur la cybercriminalité et engager des poursuites, traiter les preuves électroniques sur la base des bonnes pratiques internationales, et élaborer une législation garantissant un soutien plus cohérent aux autorités de justice pénale dans différents pays. La même année, les documents suivants ont été élaborés :

- « La liberté d'expression dans le contexte de la lutte contre la cybercriminalité – Considérations pratiques », ce document de réflexion vise à soutenir les décideurs politiques, les législateurs et les praticiens de la justice pénale dans l'élaboration et la mise en œuvre de politiques et de législations sur la cybercriminalité compatibles avec le droit à la liberté d'expression (décembre 2023) ;

- "Mise en œuvre du premier Protocole à la Convention sur la cybercriminalité relatif à la xénophobie et au racisme : Étude des bonnes pratiques" (décembre 2023), qui vise à documenter l'expérience acquise et à faciliter la mise en œuvre de ce protocole.

Plusieurs autres guides, études et enquêtes ont été lancés en 2023 (Guide sur les stratégies de formation à la lutte contre la cybercriminalité, Recherche sur les victimes de la cybercriminalité, Enquête sur les stratégies de lutte contre la cybercriminalité dans les pays de GLACY+) et seront finalisés en 2024.

Plate-forme de formation en ligne sur la cybercriminalité et les preuves électroniques

En 2023, le C-PROC a lancé la version bêta de "CYBOX", la plateforme de formation sur la cybercriminalité et les preuves électroniques, en réponse au besoin d'activités de formation en ligne ou en format hybride. La plateforme doit être pleinement opérationnelle d'ici le printemps 2024, en vue de servir de centre virtuel de formation pour tout pays coopérant avec le Bureau, ainsi que de référentiel de matériel de formation et de cours sur le sujet. En outre, toutes les activités du Réseau international de formateurs judiciaires nationaux seront transférées sur CYBOX dans un espace privé et privilégié qui ne sera accessible qu'à ses membres.

Ressources sur la législation en matière de cybercriminalité

Le renforcement de la législation nationale sur la cybercriminalité et les preuves électroniques est une composante importante de tous les projets. Des exemples de ce type de soutien au cours des dernières années sont présentés ci-dessus.

Le C-PROC suit l'évolution de la législation sur la cybercriminalité dans le monde entier et a publié en décembre 2023 son enquête sommaire actualisée sur « L'état mondial de la législation en matière de cybercriminalité ». Cette étude confirme les progrès réalisés par les pays de toutes les régions du monde dans l'alignement de leur législation nationale sur les normes de la Convention sur la cybercriminalité. En outre, le C-PROC tient à jour des informations sur l'évolution de la législation dans des « wikis pays » et des « profils juridiques » sur la plateforme Octopus.

Partenariats et synergies

Le renforcement des capacités crée des synergies et les activités du C-PROC ont continué d'être menées en partenariat avec de nombreuses organisations, parmi lesquelles la Commission européenne, l'Agence européenne pour la coopération judiciaire en matière pénale (EUROJUST), l'Agence européenne pour la coopération des services répressifs (EUROPOL), l'Agence européenne pour la formation des services répressifs (CEPOL), la Commission de l'Union Africaine, le Groupe européen de formation et d'éducation sur la cybercriminalité (ECTEG), la Communauté des Caraïbes (CARICOM), la Communauté des pays de langue portugaise (CPLP), la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), le Forum des présidents des pouvoirs législatifs en Amérique centrale et dans les Caraïbes (FOPREL), le Forum mondial pour la cyber-expertise (GFCE), l'Association internationale des procureurs (AIP), INTERPOL[32], l'Action Mondiale des Parlementaires (PGA), l'Organisation des États américains (OEA), le Pacific Island Law Officers Network (PILON), l'ONU, le ministère de la Justice des États-Unis, le gouvernement de la Roumanie en tant que pays hôte du C-PROC et bien d'autres encore. En outre, diverses activités ont été menées conjointement avec d'autres projets de renforcement des capacités financés par l'UE (CyberNet, OCWAR-C[33]) qui traitent de la cybercriminalité et des preuves électroniques ou avec le soutien de TAIEX[34], afin de promouvoir des politiques internationales cohérentes en matière de renforcement des capacités dans le domaine de la cybercriminalité. Le C-PROC reste ainsi très bien connecté à de vastes réseaux d'experts et d'institutions dans toutes les régions du monde et est reconnu comme un partenaire clé.

Des synergies sont également créées avec d'autres instruments et actions du Conseil de l'Europe, par exemple en soutenant des activités de renforcement des capacités sur la protection des données conformément à la Convention STE n° 108 telle qu'amendée par la STCE n° 223[35] ou sur la protection des enfants contre l'exploitation et les abus sexuels conformément à la Convention STCE n° 201[36], la création d'une ressource en ligne sur la cyberviolence, ou le soutien à des études typologiques sur le blanchiment d'argent.

[32] Le Global Complex for Innovation (IGCI) d'INTERPOL à Singapour est un partenaire du projet GLACY+. Dans le cadre d'une convention de subvention, INTERPOL est responsable du volet répressif de ce projet.
[33] Réponse de l'Afrique de l'Ouest sur la Cybersécurité et la lutte contre la Cybercriminalité (OCWAR-C)
[34] Un exemple en est la série d'ateliers aux juges et procureurs ghanéens.
[35] 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).
[36] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).

4. Projets C-PROC en 2024

Anticipant l'achèvement de plusieurs projets entre décembre 2023 et février 2024, la préparation de nouveaux projets et la mobilisation de ressources extrabudgétaires ont commencé en 2022 et ont constitué une priorité du C-PROC en 2023. À la fin de l'année 2023, les accords pour cinq nouveaux projets avaient été finalisés et étaient prêts à être signés.

La liste des projets mis en œuvre par le C-PROC en 2024 comprendra les éléments suivants :

Titre du projet	La durée	Budget	Financement
Projet OCTOPUS	janvier 2021 - décembre 2027	10 millions d'euros	Contributions volontaires (Canada, États-Unis, Hongrie, Islande, Italie, Japon, Pays-Bas, Royaume-Uni) [le financement n'est pas entièrement assuré]
Projet GLACY-e sur l'action globale contre la cybercriminalité renforcée	août 2023 - janvier 2026	5,55 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
Projet CyberUA sur le renforcement des capacités en matière de preuves électroniques de crimes de guerre et de 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[37] et au budget ordinaire [le financement n'est pas entièrement assuré]
CyberEast+ : une action renforcée contre la cybercriminalité pour la cyber-résilience dans les États du partenariat oriental	mars 2024 - février 2027	3,89 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
CyberSouth+ projet sur le renforcement de la coopération en matière de cybercriminalité et de preuves électroniques dans la région du voisinage sud	janvier 2024 - décembre 2026	3,89 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
Projet CyberSEE sur le renforcement de la lutte contre la cybercriminalité et les preuves électroniques en Europe du Sud-Est et en Turquie	janvier 2024 - juin 2027	5,55 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)
Projet CyberSPEX sur la coopération renforcée des États membres de l'UE en matière de preuves électroniques grâce au deuxième protocole additionnel à la convention sur la cybercriminalité	mars 2024 - février 2026	2,23 millions d'euros	Projet conjoint UE/CdE (dont 10 % OB/JPP du Conseil de l'Europe)

Avec un budget combiné de plus de 34 millions d'euros – dont la totalité n'a pas encore été garantie – le C-PROC disposera d'un niveau de ressources approprié pour 2024.

[37] Plan d'action du Conseil de l'Europe pour l'Ukraine « Résilience, relance et reconstruction » (2023-2026)

5. Conclusions

Au cours des dix années qui ont suivi sa création, le C-PROC – par le biais de ses projets et de plus de 2100 activités – a apporté une contribution significative 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 aux exigences en matière de droits humains et d'État de droit. Conférence Octopus 2023 (Bucarest, 13-15 décembre 2023), qui a réuni plus de 500 experts en cybercriminalité de quelque 130 pays, a illustré la portée de la Convention et du C-PROC. Cette conférence a été précédée par plus de 300 autres activités soutenues par le Bureau en 2023. Grâce au travail du C-PROC, le Conseil de l'Europe reste un leader mondial en matière de renforcement des capacités dans ce domaine.

Depuis 2013, le C-PROC a attiré des ressources extrabudgétaires considérables qui ont été correctement gérées, comme le confirment les audits et les évaluations. Tout en s'appuyant sur des contributions volontaires, le C-PROC est devenu une structure durable qui devrait continuer à fonctionner de la même manière.

Permettre la participation d'experts des Parties et des États invités à adhérer à la Convention sur la cybercriminalité au Comité ad hoc des Nations Unies chargé d'élaborer un traité sur « l'utilisation des technologies de l'information et des communications (TIC) à des fins criminelles » contribuera à garantir que ce futur traité – s'il est adopté – sera cohérent avec la Convention sur la cybercriminalité et comportera les garanties nécessaires en matière de droits humains et d'État de droit. Cela a également permis aux États membres des Nations Unies de mieux comprendre les avantages du cadre de la Convention sur la cybercriminalité et a suscité de nombreuses demandes d'adhésion à cette convention.

Avec ou sans traité additionnel des Nations Unies, la Convention sur la cybercriminalité avec son Protocole sur la xénophobie et le racisme (STE n° 189) et son deuxième Protocole additionnel relatif au renforcement de la coopération et à la divulgation des preuves électroniques, ainsi que le T-CY, restera le cadre international le plus pertinent en matière de cybercriminalité dans les années à venir, notamment parce qu'elle est soutenue par le renforcement des capacités par C-PROC.

Les demandes de renforcement des capacités adressées au C-PROC ne cessent d'augmenter en raison de l'intérêt croissant pour la Convention sur la cybercriminalité et ses Protocoles et de l'adhésion à ces instruments, ainsi qu'en raison des défis nouveaux et de plus en plus complexes qui nécessitent des solutions innovantes et plus sophistiquées.

L'achèvement de plusieurs projets entre décembre 2023 et février 2024 entraîne une diminution des ressources disponibles pour le C-PROC. Toutefois, de nouveaux projets ont été préparés et sont prêts à démarrer début 2024 :

- Projet CyberUA sur le renforcement des capacités en matière de preuves électroniques de crimes de guerre et de violations flagrantes des droits humains en Ukraine (contributions volontaires ; pas encore entièrement financé) ;

- CyberEast+ sur l'action renforcée contre la cybercriminalité pour la cyber-résilience dans les États du partenariat oriental (projet conjoint avec l'UE) ;

- Projet CyberSouth+ sur le renforcement de la coopération en matière de cybercriminalité et de preuves électroniques dans la région du voisinage méridional (projet conjoint avec l'UE) ;

- Projet CyberSEE sur l'amélioration de la lutte contre la cybercriminalité et les preuves électroniques en Europe du Sud-Est et en Turquie (projet conjoint avec l'UE) ;

- Projet CyberSPEX sur le coopération renforcée des États membres de l'UE en matière de preuves électroniques grâce au deuxième Protocole additionnel à la Convention sur la cybercriminalité (projet commun avec l'UE).

En outre, le projet Octopus en cours et le projet conjoint GLACY-e sur l'action globale contre la cybercriminalité renforcée sont disponibles pour une diffusion mondiale. Toutefois, des ressources supplémentaires sont nécessaires, en particulier pour le projet Octopus[38].

Les priorités pour 2024 sont les suivantes :

- Soutenir la mise en œuvre du deuxième Protocole additionnel à la Convention sur la cybercriminalité par le biais de tous les projets, y compris le projet CyberSPEX pour les États membres de l'UE.

- Renforcer les capacités de collecte et d'utilisation des preuves électroniques dans le cadre des poursuites engagées contre les auteurs de crimes de guerre et de violations flagrantes des droits humains en Ukraine.

- Aider les pays – en particulier ceux qui ont déjà été invités à adhérer à la Convention sur la cybercriminalité – à satisfaire à leurs exigences et à devenir Parties.

- Aider les autorités de justice pénale à relever les défis liés aux attaques de ransomware et aux crypto-monnaies, et améliorer leur coopération avec les organismes responsables de la cybersécurité.

- Soutenir le renforcement des garanties en matière de droits humains et d'État de droit dans les pays participant aux activités du projet. Il s'agit notamment de soutenir la mise en œuvre de la "Convention 108+"[39] sur la protection des données et de répondre aux préoccupations concernant l'impact de la législation relatif à la lutte de la cybercriminalité sur la liberté d'expression.

- Promouvoir de nouvelles synergies entre la Convention sur la cybercriminalité et ses Protocoles et d'autres instruments pertinents du Conseil de l'Europe, notamment ceux relatifs à la protection des données[40], à l'exploitation et aux abus sexuels concernant les enfants[41], à la violence à l'égard des femmes et à la violence domestique[42], au blanchiment d'argent et au financement du terrorisme[43]. D'autres partenariats et synergies avec d'autres organisations seront également recherchés.

---

[38] Le projet Octopus a été financé par les États-Unis, le Royaume-Uni et le Japon, mais aussi par l'Islande et l'Italie. Remarque : le projet Octopus soutient également les activités du T-CY.
[39] Convention STE n° 108 comme amendé par le 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).
[40] 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).
[41] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).
[42] Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE n° 210).
[43] Convention du Conseil de l'Europe relative au blanchissement, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n° 198).

- Lancer la plateforme en ligne CYBOX pour la formation et l'échange – développée dans le cadre du projet Octopus – afin de permettre l'élargissement de la formation en ligne sur la cybercriminalité et les preuves électroniques.

Bien que le C-PROC ait été très efficace au cours des dix dernières années, les demandes de renforcement des capacités ne cessent de croître. Il convient de réfléchir à la manière d'y répondre dans les années à venir. L'élaboration d'un concept pour le futur renforcement des capacités en matière de cybercriminalité et de preuves électroniques est donc également à l'ordre du jour pour 2024.