COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Documents d'information

SG/Inf(2023)1

9 janvier 2023

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

Rapport d'activité du C-PROC pour la période octobre 2021 – décembre 2022

Contenu

Sommaire exécutif

Le Bureau de programme sur la cybercriminalité du Conseil de l'Europe (ci-après « C-PROC » ou «Bureau de programme ») à Bucarest, 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 (STE n° 185), et ce dans toutes les régions du monde. Le présent rapport est destiné à informer le Comité des Ministres des activités menées par le Bureau de programme, pendant la période allant d'octobre 2021 à décembre 2022.

Au cours de cette période, le C-PROC a fonctionné, entre autres, dans le contexte de l'évolution des défis posés par la cybercriminalité et les preuves électroniques, y compris la prolifération des attaques par *ransomware* (ou « rançongiciels»). L'agression russe contre l'Ukraine a soulevé de nouveaux défis liés à la cybercriminalité et aux preuves électroniques. Le processus de l'Organisation des Nations Unies (« ONU ») visant à élaborer un nouveau traité international sur « la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles» a débuté (février 2022). Au cours de cette période, la Convention sur la cybercriminalité a célébré 20 ans d'impact mondial (lors du 20ème anniversaire de la Convention en novembre 2021) et le nouveau Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques (STCE n° 224) fut, quant à lui, ouvert à la signature (mai 2022).

En décembre 2022, le C-PROC constituait l'un des plus grands bureaux extérieurs du Conseil de l'Europe, avec un budget cumulé de plus de 39 millions d'euros pour les projets en cours et 38 agent(e)s. Le Bureau continue de s'appuyer sur des financements externes. Plus de 90 % de son budget est financé par des contributions volontaires ou des contributions de l'Union européenne (« UE ») à des projets communs. L'UE est restée le principal donateur par le biais de programmes conjoints cofinancés par le Conseil de l'Europe. Les États-Unis d'Amérique ont également mis à disposition des fonds importants. Les autres donateurs au cours de cette période ont été la Hongrie, l'Italie, les Pays-Bas, le Royaume-Uni, le Canada et le Japon. Le Bureau bénéficie du soutien du gouvernement de la Roumanie, qui continue à fournir des espaces de bureaux à titre gracieux.

Le C-PROC a soutenu quelques 420 activités dans le cadre de cinq projets impliquant plus de 130 pays entre octobre 2021 et décembre 2022, se concentrant sur :

- une législation nationale conforme à la Convention sur la cybercriminalité et à ses protocoles ainsi qu'aux normes connexes (protection des données, protection des enfants) ;
- les capacités de la justice pénale (pour les enquêtes, les poursuites et les jugements en rapport avec la cybercriminalité et l'utilisation des preuves électroniques) pour les enquêtes financières, pour affronter les attaques par *ransomware* et pour la coopération interinstitutionnelle et internationale ;
- l'élaboration de guides, de ressources en ligne et d'autres outils et exercices pour les praticiens ;
- la coopération public/privé entre les institutions de justice pénale et celles de cybersécurité ;
- la participation d'experts des parties à la convention au processus des traités de l'ONU ;
- un soutien spécifique à l'Ukraine.

Le Bureau a maintenu sa réputation de centre d'excellence en matière de cybercriminalité et a consolidé d'autant plus la position du Conseil de l'Europe en tant que leader mondial du renforcement des capacités en matière de cybercriminalité et de preuves électroniques.

Le soutien du C-PROC est un facteur important dans le succès de la Convention. Les adhésions du Nigeria et du Brésil à la Convention et les invitations à adhérer soumises à la Côte d'Ivoire, à l'Équateur, à Fidji, au Timor oriental, à Trinité-et-Tobago ainsi qu'à Vanuatu au cours de cette période sont également le résultat des activités du C-PROC.

La formule de la Convention sur la cybercriminalité et de ses protocoles en tant que norme commune, soutenue par le Comité de la Convention sur la cybercriminalité (le « T-CY ») et le renforcement des capacités par le biais du C-PROC, a continué à garantir l'impact, les synergies et l'innovation. Avec son nouveau Deuxième Protocole additionnel, la Convention sur la cybercriminalité devrait rester le mécanisme international le plus pertinent en matière de cybercriminalité pour les années à venir.

Plusieurs projets arrivant à leur terme en 2023, il convient de concevoir de nouveaux projets et de trouver des financements pour garantir le succès de cette formule au-delà de l'an prochain.

1. Cadre et objet du présent rapport

Le présent rapport est destiné à informer le Comité des Ministres des activités menées par le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (ci-après « C-PROC » ou le « Bureau ») à Bucarest, Roumanie, entre octobre 2021 et décembre 2022.[1]

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

Le C-PROC est un élément clé de l'approche du Conseil de l'Europe en matière de cybercriminalité, qui consiste en (a) la Convention sur la cybercriminalité (STE n° 185) et les normes connexes, (b) le suivi et les évaluations par le Comité de la Convention sur la cybercriminalité (« T-CY »), et (c) le renforcement des capacités.

2. Contexte

Les défis de la cybercriminalité et des preuves électroniques

La cybercriminalité - c'est-à-dire les infractions commises contre et au moyen de systèmes informatiques – représente une menace significative pour les droits fondamentaux, la démocratie et l'État de droit, ainsi que pour la paix et la stabilité internationales, et elle a un impact social et économique important. La pandémie de covid-19 a accéléré, depuis début 2020, la transformation numérique des sociétés, offrant ainsi davantage d'opportunités d'exploitation criminelle.

Les défis actuels comprennent :

- *Une prolifération des infractions liées aux ransomwares* : celles-ci consistent généralement à crypter des données ou des systèmes informatiques, bloquant ainsi les utilisateurs, puis à demander une rançon contre la (promesse de) restauration de l'accès. Les délinquants peuvent également menacer de divulguer des informations sensibles ou personnelles pour soutirer des paiements aux victimes. Les attaques « WannaCry » et « NotPetya » de 2016/2017 ont touché des ordinateurs et attiré une attention majeure dans le monde entier. Pendant la pandémie de covid-19 en 2020 et 2021, des établissements de santé, y compris des installations de recherche développant des vaccins, ont été victimes d'attaques par *ransomware*. Les entreprises de toutes tailles, les particuliers ainsi que le secteur public sont ciblés par les *ransomwares*. En avril et mai 2022, le gouvernement du Costa Rica a dû déclarer une urgence nationale à la suite d'attaques par *ransomware*. Les institutions publiques du Monténégro ont été

[1] La décision portant création du Bureau a demandé au Secrétaire général de présenter ces rapports annuels.
Remarque : Afin d'harmoniser les périodes de déclaration avec les années civiles, le présent rapport couvre la période d'octobre 2021 à décembre 2022.
Pour le rapport couvrant la période d'avril 2014 à septembre 2015, voir ce rapport (en anglais uniquement)
Pour la période d'octobre 2015 à septembre 2016, voir ce rapport (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.
[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 en vertu d'un protocole d'accord.
[3] Décisions CM/Del/Dec(2013)1180/10.4, 9 octobre 2013, lors de leur 1180ème réunion.

visées en août 2022, et celles d'Albanie en septembre 2022. En réaction à ces attaques :

- Le C-PROC a soutenu un certain nombre d'activités visant à aider les autorités de justice pénale par le biais d'ateliers pendant la conférence Octopus en novembre 2021, d'une formation internationale sur les enquêtes relatives aux *ransomwares* pour les autorités de 34 pays en mai 2022, d'un exercice international sur les enquêtes et les poursuites relatives aux *ransomwares* en Türkiye en juillet 2022, de l'élaboration d'un guide sur les enquêtes relatives aux *ransomwares* et d'une conférence internationale conjointe avec EUROJUST sur ce sujet en novembre 2022.

- En outre, le T-CY a décidé en mai 2022 de préparer une note d'orientation pour expliquer comment les dispositions de la Convention sur la cybercriminalité et de son Deuxième Protocole additionnel sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE nº 224) peuvent être utilisées pour incriminer, enquêter, poursuivre et coopérer contre les infractions liées aux *ransomwares*. Cette note d'orientation fut adoptée en novembre 2022. Les outils de la Convention et de son nouveau Deuxième Protocole additionnel sont donc disponibles pour contrer les infractions liées aux *ransomwares*.[4]

- *L'utilisation de monnaies virtuelles pour obscurcir les flux d'argent criminel, y compris pour le paiement de rançons*. En réponse :
  - un guide sur la saisie des crypto-monnaies a été élaboré en 2021 par le C-PROC dans le cadre du projet iPROCEEDS-2 ;
  - une série de formations sur les crypto-monnaies et les enquêtes sur le dark net a été dispensée en Europe du Sud-Est et en Türkiye entre janvier et mai 2022 dans le cadre du projet iPROCEEDS-2 ;
  - le C-PROC a entamé une coopération avec MONEYVAL[5] dans un exercice de typologie sur les pratiques liées aux actifs virtuels et aux fournisseurs de services d'actifs virtuels.

- *L'obtention de preuves électroniques à utiliser dans le cadre de procédures pénales* : tous les types de criminalité, pas seulement la cybercriminalité, peuvent engendrer des preuves sur des systèmes informatiques. De telles preuves peuvent se trouver dans des juridictions étrangères, multiples ou inconnues, et l'obtention de ces preuves volatiles est un défi complexe. En réponse :
  - le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques a été finalisé et ouvert à la signature en mai 2022 ;
  - des synergies ont été recherchées avec d'autres traités et mécanismes du Conseil de l'Europe relatifs aux questions pénales, afin que ceux-ci puissent bénéficier des outils de procédure et de coopération de la Convention sur la cybercriminalité et du nouveau protocole[6] ;

[4] Le Costa Rica a signé le Deuxième Protocole additionnel à la convention en juin 2022 en faisant spécifiquement référence aux attaques par *ransomware* qu'il avait subies au cours des mois précédents.
[5] Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment d'argent et le financement du terrorisme.
[6] Cela signifie que l'efficacité de nombreux instruments du Conseil de l'Europe relatifs aux questions pénales sera considérablement renforcée si les Parties respectives ont également à leur disposition les outils de procédure et de coopération internationale de la Convention sur la cybercriminalité et de son Deuxième Protocole additionnel. Les exemples vont de la Convention pénale sur la corruption (STE nº 174) aux conventions et/ou protocoles sur le blanchiment d'argent et le financement du terrorisme (STCE nº 198), la traite des êtres humains (STCE nº 197), le terrorisme (STE nº 190, STCE nº 196 et STCE nº 217), la protection des enfants contre l'exploitation et les abus sexuels (STCE nº 201), la violence à l'égard des

- de nombreuses activités de renforcement des capacités en matière de preuves électroniques, y compris sur les outils du nouveau protocole, ont été organisées.

L'agression russe contre l'Ukraine

L'agression russe contre l'Ukraine a été précédée et s'accompagne de cyberattaques contre les infrastructures critiques de l'Ukraine et d'autres formes de cybercriminalité.[7] Les preuves, non seulement de ces infractions mais aussi des crimes de guerre, peuvent prendre la forme de preuves électroniques. [8]

En réponse, le C-PROC a, dans le cadre du projet conjoint CyberEast avec l'Union européenne (« UE ») :

- contribué à la modification du droit pénal national afin d'accroître l'efficacité de l'action de la justice pénale contre les cyberattaques ;
- soutenu la formation sur l'utilisation des renseignements de source ouverte (« OSINT ») et des preuves électroniques dans les procédures de crimes de guerre ;
- examiné la législation sur l'admissibilité de l' « OSINT » dans les procédures pénales ;
- dispensé des formations sur les infractions liées aux *ransomwares* ;
- fourni des formations avancées sur la cybercriminalité et les preuves électroniques aux juges ukrainiens.

Après le début de l'agression russe, le C-PROC a également contribué à l'évacuation des agents du Conseil de l'Europe et de leurs familles, ainsi que de leurs homologues d'Ukraine vers ou en traversant la Roumanie.

Les 20 ans de la Convention sur la cybercriminalité

La Convention sur la cybercriminalité a été ouverte à la signature à Budapest, en Hongrie, le 23 novembre 2001. A l'occasion du 20ème anniversaire de la Convention, une Conférence Octopus et un événement spécial ont été organisés du 16 au 18 novembre 2021 en coopération avec la Présidence hongroise du Comité des Ministres.[9] Plus de 30 ministres et autres hauts fonctionnaires sont intervenus lors de l'événement spécial. Environ 1200 experts en cybercriminalité de quelque 120 pays - issus notamment du secteur public mais également d'organisations internationales et privées,

---

femmes (STCE nº 210), la contrefaçon de produits médicaux (STCE nº 211), la manipulation de compétitions sportives (STCE nº 215), le trafic d'organes (STCE nº 216).
- En ce qui concerne les synergies, voir les études suivantes (en anglais uniquement):
- Traite des êtres humains en ligne et facilitée par la technologie
- Protéger les femmes et les filles de la violence à l'ère numérique - La pertinence de la Convention d'Istanbul et de la Convention de Budapest sur la cybercriminalité pour lutter contre la violence en ligne et celle facilitée par la technologie à l'égard des femmes ".

Voir également la ressource en ligne sur la "cyberviolence".

[7] Voir par exemple :
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_FR.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[8] Voir par exemple :
https://www.justiceinfo.net/en/93111-insights-digital-revolution-war-crimes-probes-ukraine.html
https://www.euronews.com/next/2022/04/06/how-digital-evidence-of-war-crimes-in-ukraine-is-being-collected-verified-and-stored
https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/

[9] Conférence Octopus 2021 (coe.int) Les réunions se sont tenues en ligne en raison de la pandémie de covid-19.

d'organisations de la société civile et du monde universitaire - ont participé à la conférence.

L'événement spécial et la conférence Octopus ont confirmé l'impact de la Convention dans le monde entier les dernières 20 années.[10] L'enquête actualisée sur « l'état mondial de la législation en matière de cybercriminalité » publiée en décembre 2022 a montré comment la Convention a façonné le droit pénal de plus de 80% de tous les États.[11]

En décembre 2022, 68 États étaient devenus parties à la Convention (les derniers en date étant le Brésil et le Nigeria). Quinze autres États avaient signé la Convention ou avaient été invités à y adhérer. Au cours de l'année écoulée - également à la suite des activités du C-PROC sur la législation nationale - la Côte d'Ivoire, l'Équateur, les Fidji, le Timor oriental, Trinité-et-Tobago ainsi que le Vanuatu ont été invités à adhérer. Fin décembre 2022, d'autres demandes d'adhésion étaient en cours de traitement.

Le Premier Protocole additionnel à la Convention sur les actes de xénophobie et de racisme commis par le biais de systèmes informatiques (STE n° 189)[12] comptait 33 Parties fin décembre 2022. 12 autres l'ont signé. En janvier 2023, ce Protocole fêtera son 20ème anniversaire.

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques. [13]

Compte tenu de la prolifération de la cybercriminalité et de la complexité croissante de l'obtention de preuves électroniques qui peuvent être stockées dans des juridictions étrangères, multiples, changeantes ou inconnues, les outils actuels ne sont pas suffisants pour une réponse efficace de la justice pénale et pour permettre aux gouvernements de remplir leur obligation positive de protéger les individus contre la criminalité.

Par conséquent, le Comité de la Convention sur la cybercriminalité (T-CY) a négocié un nouveau protocole à la Convention sur la cybercriminalité entre 2017 et 2021. Le 12 mai 2022, ce Deuxième Protocole additionnel fut ouvert à la signature. A cette occasion, 22 États ont signé, suivis de deux autres États en mai et en juin 2022 et de six Etats supplémentaires le 30 novembre 2022[14].

Le protocole prévoit des outils efficaces pour renforcer la coopération et la divulgation des preuves électroniques, ainsi qu'un système solide de garanties en matière d'État de droit et de protection des données :

- une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaine ;
- une base pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés (« divulgation directe ») ;
- des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic (« donner effet ») ;
- la coopération immédiate en cas d'urgence (« divulgation accélérée » et « entraide d'urgence ») ;

[10] https://rm.coe.int/octopus-conference-2021-key-messages-v18nov2021/1680a494e6
[11] https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137
Voir également les « wikis pays » et les profils juridiques sur la plate-forme Octopus https://www.coe.int/en/web/octopus/home.
[12] 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.
[13] Le Protocole peut être consulté ici.
[14] Le tableau des signatures et des ratifications peut être consulté ici.

- des outils d'entraide (« vidéoconférence », « équipes communes d'enquête et enquêtes conjointes ») ;
- des garanties en matière de protection des données pour permettre le flux de données à caractère personnel en vertu du protocole.

Grâce à ce protocole, la Convention sur la cybercriminalité restera pertinente et efficace. Elle démontre qu'une coopération efficace avec l'État de droit et les garanties de protection des données est possible, et que la Convention continuera à défendre un internet libre et ouvert où les restrictions sont limitées aux cas d'abus criminels.

Le C-PROC a facilité la préparation du protocole sous le projet Cybercriminalité@Octopus et le projet Octopus qui en découle.[15] Après l'ouverture à la signature, les projets du C-PROC ont organisé de nombreuses activités pour partager des informations sur les outils de ce nouveau traité. Ces derniers aident désormais les pays à mettre en œuvre le protocole.

Il était important que le protocole soit achevé avant le processus des traités de l'ONU.

Comité ad hoc de l'ONU sur « la lutte contre l'utilisation des technologies de l'information et des communications (TIC) à des fins criminelles »

En adoptant la résolution 74/247[16] en décembre 2019, l'Assemblée générale des Nations Unies (AGNU) a créé le « comité intergouvernemental spécial d'experts à composition non limitée chargé d'élaborer une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles ». En mai 2021, l'AGNU a adopté les modalités du processus d'élaboration du traité par la résolution 75/282. Au total, six sessions de négociation de deux semaines chacune sont prévues à New York et à Vienne, afin de finaliser le projet de traité d'ici février 2024.

Après une première session à New York (février/ mars 2022)[17], la deuxième s'est tenue à Vienne (mai/ juin) et la troisième à New York (août/ septembre 2022).

Le C-PROC a soutenu la participation d'experts des Parties à la Convention sur la cybercriminalité et des observateurs du T-CY à ces sessions, afin d'assurer la cohérence d'un futur traité avec les dispositions de la Convention et le respect des exigences en matière de droits de l'homme et d'État de droit.

L'une des trois sessions tenues jusqu'à présent a conclu que la Convention sur la cybercriminalité s'est établie comme norme de référence et que les propositions de dispositions du futur traité de l'ONU qui sont basées sur celles de la Convention sur la cybercriminalité sont les plus susceptibles de trouver un accord. Une deuxième constatation est que le processus de traité de l'ONU semble renforcer l'attrait et l'intérêt de l'adhésion à la Convention sur la cybercriminalité.

[15] Le soutien au T-CY, y compris le cofinancement, fait (faisait) partie de ces projets.
[16] La résolution a été proposée par la Fédération de Russie.
[17] Cette première session a débuté le 28 février 2022, c'est-à-dire quatre jours après le début de l'agression russe contre l'Ukraine.

3. Résumé des projets et des résultats pour la période octobre 2021 à décembre 2022

Projets en cours

Entre octobre 2021 et décembre 2022, le C-PROC a soutenu environ 420 activités dans le cadre des projets énumérés ci-dessous :

Titre du projet	Durée	Budget	Financement
Projet GLACY+ sur l'action mondiale contre la cybercriminalité[18]	mars 2016 - février 2024	18,9 millions d'euros	JP UE/CoE (y compris 10% du budget ordinaire – BO - du Conseil de l'Europe)
Projet OCTOPUS	janvier 2020 - décembre 2024	5 millions d'euros	Contributions volontaires (Canada, Hongrie, Italie, Japon, Pays-Bas, Royaume-Uni et États-Unis)
Projet iPROCEEDS-2 visant les produits du crime sur internet et la sécurisation des preuves électroniques en Europe du Sud-Est et en Türkiye.	janvier 2020 - juin 2023 [19]	4,95 millions d'euros	UE/CoE JP (10% BO)
CyberSouth sur le renforcement des capacités dans le voisinage sud	juillet 2017 - décembre 2023	5 millions d'euros	UE/CoE JP (10% BO)
Projet CyberEast sur l'action contre la cybercriminalité pour la résilience cybernétique dans la région du partenariat oriental	juin 2019 - décembre 2023	5,33 millions d'euros	UE/CoE JP (10% BO)

À partir de mars 2022, avec la levée progressive des restrictions liées à la covid-19, elles se sont déroulées en présentiel, en format hybride ou en ligne.

Un inventaire détaillé des activités soutenues ou réalisées est disponible en ligne (en anglais uniquement).

En décembre 2022, le budget combiné des projets en cours s'élevait à quelque 39,2 millions d'euros (septembre 2015 : 6 millions d'euros, 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).

Le Bureau s'appuie sur des financements externes. Au cours de l'année écoulée, plus de 90 % de son budget a été financé par des ressources extrabudgétaires, c'est-à-dire par des contributions volontaires et des contributions de l'UE à des programmes conjoints. L'UE est restée le principal donateur par le biais de projets conjoints cofinancés par le Conseil de l'Europe. Les États-Unis d'Amérique ont également apporté un financement important. La Hongrie, l'Italie, les Pays-Bas, le Royaume-Uni, le Canada et le Japon ont également contribué. Le Bureau compte également sur le soutien du gouvernement de la Roumanie, qui continue à fournir des espaces de bureaux à titre gracieux.

[18] Note : En novembre 2022, la Commission de l'Union Européenne et le Conseil de l'Europe ont signé un accord de contribution supplémentaire pour un nouveau projet « Action mondiale renforcée contre la cybercriminalité » (GLACY-e) avec un budget de 5,56 millions d'euros commençant en août 2023 et devant se terminer en février 2026.

[19] Note : prolongation sans frais jusqu'en décembre 2023 acceptée en principe par la Commission européenne.

Alors que le projet Octopus est entièrement financé par des contributions volontaires, les programmes conjoints avec l'UE comprennent un cofinancement de 10% du budget du Conseil de l'Europe.

Si le financement disponible pour 2023 semble approprié, d'importantes ressources supplémentaires devront être mobilisées dans les mois à venir, pour les raisons suivantes :

- le retour aux activités en présentiel (en combinaison avec les formats en ligne et hybrides) signifie que le coût des activités augmente, ce qui est aggravé par les tendances économiques actuelles (augmentation du coût des voyages, inflation, conséquences de l'agression russe contre l'Ukraine) ;
- le nombre d'États sollicitant les projets implémentés par le C-PROC a grandi et continuera de grandir de manière importante ;
- plusieurs projets arriveront à leur terme en 2023.

Des propositions d'éventuels projets sont formulées dans les « conclusions » ci-dessous.

Résultats

Capacités de la justice pénale

Durant la période d'octobre 2021 à décembre 2022, le C-PROC a contribué de manière significative au renforcement des capacités de la justice pénale, en particulier dans les 40 pays prioritaires actuels qui peuvent bénéficier d'un large éventail d'assistance. Plus de 90 autres pays ont participé à au moins une partie des activités.

Le soutien au renforcement des capacités généré par le Bureau est basé sur la Convention sur la cybercriminalité et renforce également le travail du T-CY. Les activités du projet se sont concentrées en particulier sur :

- la législation nationale sur la cybercriminalité et les preuves électroniques, ainsi que sur la protection des données, l'exploitation sexuelle des enfants et les abus sexuels en ligne ;
- les stratégies et politiques en matière de cybercriminalité, y compris la sensibilisation des décideurs politiques ;
- les capacités des services répressifs, notamment par le biais de procédures opérationnelles standard, d'outils de saisie des crypto-monnaies et autres ;
- l'intégration de 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 équipes d'intervention en cas d'urgence informatique) et les autorités de justice pénale ;
- la coopération internationale, notamment en ce qui concerne la rationalisation des procédures d'assistance mutuelle, les modèles de demande et autres outils, et le renforcement des points de contact 24/7.

Par nature, ces activités contribuent à la mise en œuvre de l'Agenda 2030 de l'ONU pour le développement durable, en particulier pour l'objectif de développement durable 16
(« Promouvoir l'avènement des 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 »).

Voici quelques exemples d'activités spécifiques :

- **CyberEast** : Les politiques relatives à la cybercriminalité dans tous les États du Partenariat oriental (à l'exception du Belarus) ont été renforcées par les résultats des enquêtes d'opinion publique (Cyber Baromètre). Le travail sur la législation avec les pays du projet s'est poursuivi compte tenu des exigences du Deuxième Protocole additionnel à la convention, avec la signature de la Moldavie et de l'Ukraine en novembre 2022 Le projet a permis de renforcer les capacités des autorités pénales et la coopération interinstitutionnelle par le biais de séries de formations sur les enquêtes financières, les preuves électroniques avancées et la criminalistique, ainsi que par des cyber-exercices régionaux en coopération, avec des sessions consacrées au signalement de la cybercriminalité et à l'accès aux données dans le secteur privé. Le soutien ciblé à l'Ukraine a consisté à garantir l'admissibilité des preuves, à soutenir les réformes juridiques, à développer des compétences pratiques en matière de lutte contre les *ransomwares* et à utiliser des renseignements de source ouverte pour les enquêtes. 72 activités ont été soutenues par ce projet au cours de cette période.

- **iPROCEEDS-2** : Les capacités des services répressifs ont été renforcées par des formations spécialisées sur les enquêtes relatives aux cyberattaques, aux *ransomwares*, aux monnaies virtuelles et au darknet, parallèlement à des exercices d'enquêtes financières. Des liens plus étroits entre les magistrats, les enquêteurs, la communauté de la cybersécurité et le secteur privé ont été réalisés en soutenant les réunions publiques/ privées au niveau national, en mettant l'accent sur la coopération entre les autorités de justice pénale et les fournisseurs de services. Les capacités des juges et des procureurs à traiter des affaires complexes de cybercriminalité ont été renforcées par une formation judiciaire durable sur la cybercriminalité, les preuves électroniques, la coopération internationale, les produits de la criminalité en ligne et la certification des compétences de formation. La troisième édition de la Conférence sur l'économie souterraine, en coopération avec l'équipe CYMRU, a rassemblé environ 500 représentants des services répressifs, de la communauté de la cybersécurité, de l'industrie privée et des universités du monde entier pour partager des études de cas et de nouveaux outils pour gérer les menaces de la cybercriminalité. Le projet a soutenu quelque 84 activités au cours de cette période.

- **CyberSouth** : Les capacités judiciaires durables pour faire face à la cybercriminalité dans tous les pays prioritaires (Algérie, Jordanie, Liban, Maroc, Tunisie) ont été renforcées par la finalisation d'une série de formations sur la coopération internationale et les preuves électroniques et par l'organisation d'une formation de formateurs pour les magistrats, dans le but d'établir un pool d'experts nationaux qui peuvent être impliqués dans de futures activités éducatives sur la cybercriminalité. Un soutien a également été apporté aux institutions nationales de formation judiciaire afin qu'elles intègrent les programmes éducatifs sur la cybercriminalité et les preuves électroniques dans les cursus nationaux. La promotion de boîtes à outils nationales destinées aux premiers intervenants des services répressifs a contribué à améliorer la qualité et l'efficacité des enquêtes sur la cybercriminalité (Algérie, Jordanie, Liban, Maroc et Tunisie). Les approches stratégiques pour lutter contre la cybercriminalité ont continué à être soutenues par des discussions en ligne et des recommandations sur la collecte et l'analyse de données statistiques sur la cybercriminalité. Des conseils ont été fournis à la Jordanie en vue d'aligner davantage la législation nationale sur la Convention sur la cybercriminalité. Le projet a soutenu quelque 76 activités au cours de cette période.

- **GLACY+ :** Des réformes législatives et des examens de politiques ont été soutenus en Afrique, en Asie, en Amérique latine et dans le Pacifique sur la cybercriminalité et les preuves électroniques (Colombie, Equateur, Fidji, Nauru,

Panama, Philippines, Ouganda et Uruguay) et la protection des données (Chili, Equateur, Gambie, Vanuatu). Des séries de webinaires sur l'universalité et la mise en œuvre de la Convention sur la cybercriminalité (avec les parlementaires pour une action mondiale) et sur le Deuxième Protocole additionnel à la Convention (avec l'Association internationale des procureurs) ont permis de promouvoir la connaissance et l'utilisation de la Convention et de cimenter les partenariats du projet avec les organisations régionales et internationales. Des activités spécifiques en Colombie, au Brésil, au Bélize ou en Uruguay ont renforcé le dialogue entre les décideurs politiques et les praticiens. En continuant à mettre l'accent sur le renforcement des capacités techniques des autorités chargées de l'application de la loi, des ateliers consultatifs sur la recherche, la saisie et la confiscation des produits du crime en ligne, mis en œuvre par le partenaire du projet, INTERPOL, au Nigeria, au Ghana, au Chili, au Paraguay et aux Philippines, ont permis d'améliorer les connaissances des pays sur les enquêtes financières parallèles. La coopération internationale a été renforcée par une série d'événements annuels axés sur des exercices basés sur des scénarios concernant la préservation des données, l'entraide juridique, les enquêtes financières parallèles et d'autres mécanismes de coopération pour les régions Afrique
et Amérique latine. Deux nouvelles formations ont été mises à l'essai en Afrique et dans la région Amérique latine : la formation des formateurs pour le cours ECTEG pour les premiers intervenants et la formation FOSI, avec des projets d'étendre la prestation aux autres régions en 2023. Le projet GLACY+ a également mis l'accent sur la formation judiciaire en organisant des ateliers de formation nationaux au Bénin, au Cap-Vert, au Ghana, à Maurice, au Panama, au Paraguay, au Sénégal, en Sierra Leone et au Sri Lanka, ainsi qu'une série d'ateliers entre praticiens organisées dans le cadre du Réseau international de formateurs judiciaires nationaux du C-PROC. Deux événements majeurs ont eu lieu au Costa Rica en novembre 2022 en coopération avec le Projet Octopus, à savoir le Forum des Amériques sur la cybercriminalité et la Conférence internationale sur les femmes et la cybercriminalité. Quelque 180 activités ont été soutenues par le projet au cours de cette période.

- **Projet Octopus :** L'ouverture à la signature du Deuxième Protocole additionnel à la Convention sur la cybercriminalité soutenu par le Projet Octopus en coopération avec d'autres projets du C-PROC en mai 2022 a offert aux Parties à la Convention sur la cybercriminalité de nouvelles possibilités de coopération renforcée et de divulgation des preuves électroniques. Une série de webinaires dédiés, y compris des tables rondes multipartites en Amérique latine, ont permis de mieux faire connaître et accepter le protocole en vue de sa future adhésion par les États. L'amélioration du dialogue politique et des partenariats numériques sur la cybercriminalité a été encouragée par un échange de vues avec la communauté diplomatique, une série de webinaires parlementaires et d'autres activités soulignant l'importance de l'internet libre, ouvert et mondial et du respect des droits de l'homme et des exigences de l'État de droit. Les activités menées avec la Barbade, Nauru et d'autres pays des Caraïbes, d'Amérique latine et d'Asie ont porté sur la législation et les capacités des pays à relever le défi de la cybercriminalité et des preuves électroniques, de la cybercriminalité liée à la covid-19, de la cyberviolence (y compris l'exploitation et les abus sexuels des enfants en ligne et la cyberviolence fondée sur le sexe). Des supports de formation traduits ont été mis à disposition par le biais de la plate-forme Octopus et le cours HELP sur la cybercriminalité et les preuves électroniques, récemment lancé, est devenu un outil important permettant aux autorités de justice pénale et aux praticiens du droit du monde entier d'améliorer leurs connaissances sur le sujet. Une plateforme de formation en ligne spécialisée, qui devrait être pleinement opérationnelle début 2023, est destinée à compléter la panoplie d'outils dont disposent les pays du monde entier. Le dialogue a été encouragé au sein de la

communauté de la Convention sur la cybercriminalité : le soutien aux plénières du T-CY, au groupe de travail sur les enquêtes sous couverture et l'extension du champ des perquisitions, la célébration du 20ème anniversaire de la Convention sur la cybercriminalité et la conférence Octopus ont permis de renforcer l'adhésion, la portée et l'impact de ce traité. 112 activités ont été soutenues par ce projet au cours de cette période.

Guides pour les praticiens

Le C-PROC, également en partenariat avec d'autres organisations internationales, a élaboré un certain nombre de guides et des outils sur des questions liées à la cybercriminalité et aux preuves électroniques. Ces guides fournissent aux praticiens des outils pratiques pour les enquêtes et les poursuites en matière de cybercriminalité et pour le traitement des preuves électroniques, sur la base des bonnes pratiques internationales. Ils permettent également au C-PROC de fournir un soutien plus cohérent aux autorités de justice pénale dans différents pays. Entre octobre 2021 et décembre 2022, les guides additionnels suivants ont été élaborés dans le cadre de projets du C-PROC :

- La version 3.0 du Guide des preuves électroniques du Conseil de l'Europe (en anglais uniquement) fournit des conseils aux professionnels de la justice pénale sur la manière d'identifier, de traiter, de saisir et de sécuriser les preuves électroniques, avec une mise à jour sur les nouvelles technologies et les nouveaux dispositifs tels que les drones et les crypto-monnaies.

- Le C-PROC a publié le Guide sur les stratégies de formation des forces de l'ordre en matière de cybercriminalité et de preuves électroniques (en anglais uniquement), préparé en coopération avec INTERPOL.

- Un guide pour les enquêtes sur les infractions liées aux *ransomwares* a été finalisé en novembre 2022.

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

Avant la pandémie de covid-19, la majorité des efforts de renforcement des capacités soutenus par le C-PROC impliquait des activités classiques sur place. Après le début de la pandémie, le C-PROC s'est tourné vers l'offre d'activités en ligne. Il est devenu évident que, même avec la levée des restrictions liées à covid-19 et le retour aux activités sur site, les formats d'apprentissage numériques se maintiendront dans le temps.

Le C-PROC prépare donc une plateforme de formation en ligne sur la cybercriminalité et les preuves électroniques qui devrait être lancée au début de l'année 2023, afin de servir de centre virtuel de formation pour tout pays coopérant avec le Bureau, ainsi que de dépôt de matériel de formation et de cours sur le sujet.

Cybercriminalité et législation connexe

Le renforcement de la législation nationale sur la cybercriminalité et les preuves électroniques est un élément important de tous les projets. Des exemples de ce soutien au cours des dernières années ont été cités précédemment.

Le C-PROC tient à jour des informations sur l'évolution de la législation dans des « wikis pays » et des « profils juridiques » sur la plate-forme Octopus et réalise régulièrement des enquêtes sur l'état mondial de la législation en matière de

cybercriminalité.[20]

Par exemple, en janvier 2022, 128 États (soit deux tiers des membres de l'ONU) avaient mis en place des dispositions de droit pénal substantiel correspondant largement à celles de la Convention sur la cybercriminalité. Cela représente une augmentation de 22 États en deux ans (c'est-à-dire depuis février 2020).

Partenariats et synergies

Le renforcement des capacités crée des synergies et les activités du C-PROC ont continué à être menées en partenariat avec de nombreuses organisations, parmi lesquelles la Commission européenne, l'Agence européenne de coopération en matière de justice pénale (EUROJUST), l'Agence européenne de coopération policière (EUROPOL), l'Agence européenne pour la formation des forces de l'ordre (CEPOL), l'Institut d'études de sécurité de l'UE, la Commission de l'Union africaine, le Groupe européen d'éducation et de formation en matière de 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 d'Amérique centrale et des Caraïbes (FOPREL), le Forum mondial de la cyber-expertise (GFCE), l'Association internationale des procureurs (AIP), INTERPOL[21], les Parlementaires pour l'action mondiale (PGA), l'Organisation des États américains (OAS), le Pacific Island Law Officers Network (PILON), les Nations unies, le ministère de la Justice des États-Unis, le département d'État 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, El PAcCTO, SIRIUS, OCWAR_C) qui comptent la cybercriminalité et les preuves électroniques parmi leurs thèmes afin d'assurer la promotion de politiques internationales similaires en matière de cybercriminalité. Tout cela montre que le C-PROC est bien relié à de vastes réseaux d'experts et d'institutions dans toutes les régions du monde et 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 les activités de renforcement des capacités en matière de protection des données conformément à la Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel[22] (ci-après dénommée « Convention 108+ ») ou en matière de protection des enfants contre l'exploitation et les abus sexuels conformément à la Convention de Lanzarote, la création de la ressource en ligne sur la cyberviolence, ou le soutien aux études typologiques sur le blanchiment d'argent.

4. Conclusions

Impact

Le Bureau de programme sur la cybercriminalité du Conseil de l'Europe a de nouveau exercé, entre octobre 2021 et décembre 2022, un impact important sur les capacités de la justice pénale et sur la législation en matière de cybercriminalité et de preuve électronique basées sur la Convention sur la cybercriminalité, dans toutes les régions du monde, grâce à quelque 420 activités impliquant plus de 130 pays. Avec le travail du

[20] https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan2022-p/1680a564bb
https://www.coe.int/en/web/octopus/home
Le Complexe mondial INTERPOL pour l'innovation (CMII) à Singapour est un partenaire du projet GLACY+. Dans le cadre d'un accord de subvention, INTERPOL est responsable de la composante répressive de ce projet.
[22] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE nº 223).

C-PROC, le Conseil de l'Europe reste un leader mondial en matière de renforcement des capacités dans ce domaine.

Le partenariat et les synergies avec d'autres parties prenantes et le recours aux normes connexes du Conseil de l'Europe (par exemple sur la protection des données ou la protection des enfants) ont contribué à multiplier l'impact.

Bien que les projets C-PROC soient clairement axés sur une réponse efficace de la justice pénale fondée sur la Convention sur la cybercriminalité et ses protocoles et avec les garanties nécessaires en matière de droits de l'homme, d'État de droit et de protection des données, l'approche s'est avérée suffisamment pragmatique et flexible pour répondre aux nouveaux défis. Au cours de l'année écoulée, il s'est agi, par exemple, de soutenir l'Ukraine, de faire face aux attaques par ransomware ou de renforcer les liens entre la cybersécurité et les réponses de la justice pénale.

Le nombre de pays alignant leur législation nationale sur la Convention sur la cybercriminalité et cherchant à y adhérer n'a cessé d'augmenter au cours de cette période.

En assurant la participation d'experts des Parties à la Convention sur la cybercriminalité dans le processus des traités de l'ONU, davantage d'États membres de l'ONU ont pris conscience des avantages de la Convention, suscitant ainsi un plus grand intérêt pour celle-ci.

L'ouverture à la signature du Deuxième Protocole additionnel sur le renforcement de la coopération et de la divulgation des preuves électroniques a encore renforcé l'attrait de la Convention sur la cybercriminalité. Avec ce nouvel instrument, la Convention restera l'accord international le plus pertinent en matière de cybercriminalité dans un avenir prévisible. La Convention, ses protocoles, ses rapports explicatifs et ses notes d'orientation sont disponibles en une seule compilation. En outre, des éditions spéciales (en anglais uniquement) ont été préparées pour documenter le processus de négociation de la Convention sur la cybercriminalité, et du Deuxième Protocole additionnel.

La formule de la Convention sur la cybercriminalité comme norme commune, soutenue par le Comité de la Convention sur la cybercriminalité (T-CY) et le renforcement des capacités par le biais du C-PROC, demeure efficace pour garantir impact et innovation.

Les demandes de renforcement des capacités du C-PROC ne cessent d'augmenter :

- Le nombre croissant de pays demandant à adhérer à la Convention sur la cybercriminalité signifie que davantage de pays auront besoin de soutien pour s'assurer que leur législation répond aux exigences de la Convention (y compris les sauvegardes), qu'ils ont la capacité d'appliquer cette législation et qu'ils sont en mesure de coopérer avec les autres Parties.

- L'ouverture à la signature du Deuxième Protocole additionnel signifie que les signataires doivent être soutenus dans la mise en œuvre de cet instrument en termes de législation et de capacités.

- Un soutien est nécessaire pour relever les défis émergents (par exemple, ceux liés aux *ransomwares*, aux monnaies virtuelles, à la cyberviolence, aux crimes de guerre et à la cybersécurité).

Le retour aux activités en présentiel (en combinaison avec les formats en ligne et hybrides) signifie que le coût des activités augmente. Cette situation est encore aggravée par les tendances économiques actuelles.

Dans le même temps, il est prévu que trois projets se terminent en 2023 (les projets iPROCEEDS-2, CyberSouth et CyberEast). Des ressources supplémentaires doivent être obtenues pour maintenir l'approche actuelle.

Priorités

Les priorités spécifiques pour les douze mois à venir sont les suivantes :

- S'assurer que les pays invités à adhérer à la Convention sur la cybercriminalité disposent de la législation et des capacités nécessaires, conformément aux dispositions de ce traité, avant l'adhésion effective.

- Soutenir l'ouverture à la signature, la ratification et la mise en œuvre du Deuxième Protocole additionnel à la Convention sur la cybercriminalité.

- Promouvoir le Premier Protocole additionnel à la Convention sur la cybercriminalité sur la xénophobie et le racisme commis par le biais de systèmes informatiques. Son 20ème anniversaire en janvier 2023 en sera l'occasion.

- Aider les autorités de justice pénale à relever les défis actuels liés aux attaques par *ransomware*, aux crypto-monnaies, à l'utilisation du renseignement de source ouverte et des preuves électroniques dans les procédures liées aux crimes de guerre (Ukraine) et renforcer leur coopération avec les organismes chargés de la cybersécurité.

- Soutenir le renforcement des droits de l'homme, de l'État de droit et des garanties de protection des données dans les pays participant aux activités du projet. Cela inclut notamment un soutien à la mise en oeuvre de la "Convention 108+".

- Promouvoir davantage les synergies de la Convention sur la cybercriminalité avec les instruments pertinents du Conseil de l'Europe, notamment son Premier Protocole additionnel à la Convention sur la xénophobie et le racisme commis par le biais de systèmes informatiques,ainsi que les Conventions sur la protection des données [23], de Lanzarote[24] et d'Istanbul[25], la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme[26] et MONEYVAL (concernant les crypto-monnaies). D'autres partenariats et synergies avec d'autres organisations seront également recherchés.

- Préparer de nouveaux projets ou l'extension des projets en cours et mobiliser des ressources supplémentaires. Le portefeuille actuel de projets couvre des régions prioritaires en Europe ainsi que des pays engagés dans la mise en œuvre de la Convention sur la cybercriminalité dans d'autres parties du monde. Certains projets arriveront à terme dans un avenir proche, et un suivi sera nécessaire pour garantir un impact au-delà de 2023 :

  - Plusieurs lancements en janvier 2024 :

    - un nouveau projet sur la cybercriminalité, les enquêtes financières et le Deuxième Protocole additionnel couvrant l'Europe du Sud-Est et la

[23] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE nº 223).
[24] Convention pour la protection des enfants contre l'exploitation et les abus sexuels (STCE nº 201).
[25] 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 nº 210).
[26] Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE nº 198).

Türkiye (dans le prolongement d'iPROCEEDS-2 ou sous la forme d'une extension des coûts de ce projet) ;
- un nouveau projet CyberEast (ou son extension) couvrant l'Arménie, l'Azerbaïdjan, la Géorgie, la Moldavie et l'Ukraine (dans le prolongement du projet CyberEast actuel) ;
- un nouveau projet faisant suite au projet CyberSouth (qui couvre actuellement l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie).

– L'expansion du projet Octopus et la mobilisation de ressources supplémentaires.