COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Documents d'information

SG/Inf(2021)32

15 novembre 2021

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

Rapport d'activité du C-PROC pour la période octobre 2020 – septembre 2021

Contenu

Sommaire exécutif 3
1. Cadre et objet du présent rapport 4
2. Contexte 4
Les défis de la cybercriminalité et des preuves électroniques 4
20 ans de la Convention de Budapest sur la cybercriminalité 6
(Projet de) Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques 6
Comité ad hoc de l'ONU sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles 7
Covid-19 et renforcement des capacités 8
3. Résumé des projets et des résultats pour la période octobre 2020 à septembre 2021 8
Projets en cours 8
Résultats 9
Capacités de la justice pénale 9
Guides et outils 11
Cybercriminalité et législation connexe 11
Synergies 11
4. Conclusions 12
Impact 12
Priorités 12

Annexe (en ligne)

Sommaire exécutif

Le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) 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, 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 2020 à septembre 2021.

Le C-PROC a fonctionné dans le contexte de (a) l'évolution des défis posés par la cybercriminalité et les preuves électroniques au regard des droits de l'homme, de la démocratie et de l'État de droit, (b) la portée et l'impact croissants de la Convention sur la cybercriminalité depuis son ouverture à la signature il y a vingt ans, (c) la finalisation du deuxième protocole additionnel à la Convention, (d) le début d'un processus des Nations Unies (ONU) chargé d'élaborer un nouveau traité sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles, et (e) la pandémie de COVID-19.

Le C-PROC a soutenu 395 activités impliquant plus de 120 pays entre octobre 2020 et septembre 2021 – la plupart d'entre elles menées en ligne en raison des restrictions liées à la COVID-19. Le Bureau a maintenu sa réputation de centre d'excellence en matière de renforcement des capacités en matière de cybercriminalité et de preuves électroniques.

C-PROC s'est concentré sur :

- le renforcement des capacités de justice pénale et de la législation sur la cybercriminalité et les preuves électroniques;
- l'élaboration de guides et d'outils sur les questions de cybercriminalité et leur mise en œuvre;
- l'augmentation des adhésions à, et la mise en œuvre de la Convention de Budapest;
- le processus d'élaboration du deuxième protocole additionnel à la Convention de Budapest;
- les synergies avec d'autres organisations et projets.

En septembre 2021, le C-PROC constituait l'un des plus grands bureaux extérieurs du Conseil de l'Europe, avec un budget cumulé d'environ 38 millions d'euros pour des projets en cours et 37 agent(e)s.

Le Bureau continue de s'appuyer dans une large mesure sur des financements externes. Plus de 90 % de son budget est financé par des contributions volontaires. L'Union européenne est restée le principal donateur grâce à des 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, le Royaume-Uni, le Canada et le Japon. Le Bureau bénéficie en outre du soutien du gouvernement de la Roumanie, qui continue à fournir des espaces de bureaux à titre gracieux.

La formule de la Convention de Budapest en tant que 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, a continué d'avoir à produire un impact. Avec le deuxième protocole additionnel à venir, la Convention de Budapest devrait rester le mécanisme international le plus pertinent pour les années à venir.

Les priorités pour l'année prochaine comprennent (a) le soutien à la mise en œuvre du deuxième protocole additionnel, (b) le renforcement des garanties en matière de droits de l'homme, d'État de droit et de protection des données, (c) l'amélioration des capacités pour la réalisation d'activités en ligne, (d) les synergies avec d'autres instruments et mécanismes du Conseil de l'Europe ainsi qu'avec d'autres organisations, et (e) l'extension des projets actuels et la conception de nouveaux projets afin de garantir le financement de futures activités de renforcement des capacités.

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 (C-PROC) entre octobre 2020 et septembre 2021[1].

Le Bureau est opérationnel depuis avril 2014. Son ouvertrue faisait 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 combine (a) la Convention de Budapest et les normes connexes, (b) des évaluations de suivi 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 – a évolué pour devenir une menace significative pour les droits fondamentaux, la démocratie et l'État de droit et elle a un impact social et économique important. Les menaces et tendances suivantes sont actuellement signalées en matière de cybercriminalité :

- La pandémie de Covid-19 a accru la dépendance aux technologies de l'information et de la communication et elle a accéléré la transformation numérique des sociétés. Cette dépendance est exploitée de manière criminelle sous la forme de campagnes d'hameçonnage et de distribution de logiciels malveillants, d'attaques par ransomware (y compris contre des établissements de santé), de systèmes de fraude, de désinformation ou d'une augmentation des violences sexuelles en ligne à l'encontre des enfants[4].

- Les *ransomwares*, qui empêchent l'accès ou l'utilisation de données, de systèmes ou de réseaux à moins que des paiements ne soient effectués, généralement en crypto-monnaie, sont actuellement considérés comme la menace la plus courante en matière de cybercriminalité. Les attaques par *ransomware* ont perturbé ou paralysé des organisations gouvernementales et privées, y compris des infrastructures critiques[5]. La fermeture de services hospitaliers par des *ransomwares* aurait entraîné des décès[6].

- Les attaques de chaînes d'approvisionnement où les réseaux ou systèmes sont attaqués, mais aussi les logiciels ou autres dispositifs qui y sont connectés via la chaîne d'approvisionnement, contournant ainsi les mesures de sécurité[7].

---

[1] La décision portant création du Bureau (voir ci-dessous) a demandé au Secrétaire général de présenter ces rapports annuels.
Pour le rapport couvrant la période d'avril 2014 à septembre 2015, voir ce rapport.
Pour la période d'octobre 2015 à septembre 2016, voir ce rapport.
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.
[2] C-PROC est situé à la Maison des Nations Unies à Bucarest. L'espace de bureau est alloué gratuitement 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 1180e réunion.
[4] Voir la ressource en ligne mise à disposition par C-PROC.
[5] Pour des exemples, voir https://www.blackfog.com/the-state-of-ransomware-in-2021/
[6] Voir par exemple : https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116
[7] Voir par exemple : https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

- Les processus démocratiques, y compris les élections, restent exposés au risque de cyberattaques et d'interférences. Si des mesures ont été prises dans de nombreux pays pour renforcer la sécurité des systèmes informatiques utilisés lors des élections, des tentatives de déstabilisation des élections par un accès illégal aux systèmes informatiques de parlements, partis et hommes politiques ou des campagnes électorales ont encore été signalées en 2020/2021.

- Le coût des cyberattaques (dommages ou vol de données ou d'argent, perte de productivité et perturbation des activités commerciales, vol de propriété intellectuelle, fraude, enquête médico-légale, récupération ou restauration de données ou de systèmes, atteinte à la réputation) aurait dépassé 1 000 milliards USD en 2020[8]. Par exemple, en août 2021, l'association allemande du secteur de l'Internet, BITKOM, a quantifié les dommages annuels des cyberattaques contre l'industrie allemande à plus de 220 milliards d'euros[9].

- L'exploitation et les abus sexuels en ligne des enfants sont encore exacerbés par la pandémie de Covid-19, sous la forme d'une augmentation des supports d'abus sexuels sur les enfants, de la prédation sexuelle en ligne, de communautés d'abus en ligne, de la prise de risque en ligne par les mineurs et de la diffusion en direct des abus[10]. En 2020, la CyberTipline gérée par le « National Centre for Missing and Exploited Children » a reçu 21,7 millions rapports d'abus d'enfants de la part de prestataires de services, avec plus de 65 millions de fichiers vidéo et d'images d'abus d'enfants. Le plus grand nombre de rapports, et de loin, a été reçu de Facebook (20,3 millions)[11]. Chaque mois, Facebook supprimerait quelque 250 000 comptes WhatsApp soupçonnés de partager des images d'abus d'enfants[12]. L'ampleur de ces abus et le nombre de délinquants et de victimes dans de multiples juridictions posent des défis majeurs aux enquêtes et aux poursuites.

- En outre, le darkweb offre des places de marché illicites pour tout type d'activité criminelle, y compris des outils et des services permettant de commettre d'autres crimes (« crime-as-a-service »)[13]. La cybercriminalité facilite ou finance d'autres formes de criminalité, notamment le crime organisé et le terrorisme.

- Tous les types de criminalité, pas seulement la cybercriminalité, peuvent engendrer des preuves sur des systèmes informatiques. Cela signifie que l'efficacité de nombreux instruments du Conseil de l'Europe relatifs aux questions pénales sera considérablement renforcée si les Parties respectives disposent également des outils de procédure et de coopération internationale de la Convention de Budapest et de son deuxième protocole additionnel à venir. Les exemples vont de la Convention pénale sur la corruption (STCE 173) aux conventions et/ou protocoles sur le blanchiment d'argent et le financement du terrorisme (STCE 198), la traite des êtres humains (STCE 197), le terrorisme (STE 190, STCE 196, STCE 217), la protection des enfants contre l'exploitation et les abus sexuels (STCE 201), la violence à l'égard des femmes et la violence domestique (STCE 210), la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique (STCE 211), la manipulation de compétitions sportives (STCE 215), le trafic d'organes humains (STCE 216), entre autres.

---

[8] https://www.business-standard.com/article/technology/mcafee-report-says-cybercrime-to-cost-world-economy-over-1-trillion-1201207002491.html

[9] https://www.bitkom-research.de/de/pressemitteilung/angriffsziel-deutsche-wirtschaft-mehr-als-220-milliarden-euro-schaden-pro-jahr

[10] Voir par exemple : https://www.end-violence.org/sites/default/files/paragraphs/download/esafety%20OCSE%20report%20-%20salter%20and%20wong.pdf

[11] Source : https://www.missingkids.org/content/ncmec/en/ourwork/impact.html et https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf

[12] https://www.theguardian.com/global-development/2021/feb/09/exclusive-rise-in-child-abuse-images-online-threatens-to-overwhelm-uk-police-officers-warn

[13] Voir, par exemple, https://securityintelligence.com/news/darkmarket-dark-web-marketplace-taken-down/ et https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

20 ans de la Convention de Budapest sur la cybercriminalité

La Convention sur la cybercriminalité a été ouverte à la signature à Budapest, en Hongrie, le 23 novembre 2001. En vingt ans, l'impact de cet instrument est devenu mondial. Par exemple:

- En septembre 2021, 66 États, dont 21 États non membres du Conseil de l'Europe, étaient parties à la Convention. 11 l'avaient signée ou avaient été invités à y adhérer et plusieurs demandes d'adhésion étaient en cours de traitement, conformément à l'article 37 de la Convention. Avec chaque nouvelle Partie, la valeur de la Convention en tant que cadre de coopération internationale en matière de cybercriminalité et de preuve électronique s'est accrue. Un exemple en est le réseau de points de contact 24/7, en vertu de l'article 35.

- Plus de 120 États disposaient dans leur droit interne de dispositions pénales de fond correspondant largement à celles de la Convention. Plus de 90 États disposaient également de pouvoirs procéduraux pour enquêter sur la cybercriminalité et recueillir des preuves électroniques. Et plus de 150 États l'ont utilisée comme ligne directrice ou du moins comme source d'inspiration lors de la réforme de leur législation nationale[14].

- La Convention a ainsi eu une influence claire sur les enquêtes et les poursuites dans les États qui ont réformé leur droit interne sur la base de ce traité. Elle a également eu un impact sur l'État de droit grâce à la mise en œuvre des garanties de la Convention (telles que le contrôle judiciaire prévu à l'article 15) visant à empêcher l'utilisation abusive des pouvoirs d'enquête. Et dans un certain nombre d'États, la réforme de la législation pénale s'accompagne de réformes de la législation sur la protection des données, souvent avec le soutien du Conseil de l'Europe et conformément aux Conventions 108 et désormais « 108+ ».

- La Convention est un catalyseur pour le renforcement des capacités qui, à son tour, est un facteur primordial pour une augmentation des adhésions à la Convention de Budapest. La raison d'être des programmes de coopération mis en œuvre par le C-PROC est que, si tout pays peut être aidé à réformer sa législation nationale conformément à la Convention de Budapest, un État qui est allé plus loin et a demandé l'adhésion ou est devenu partie peut devenir un « pays prioritaire » pouvant bénéficier de toute la gamme des activités de formation et d'assistance technique afin de permettre la mise en œuvre de la Convention.

Ce dernier point contribue à expliquer les raisons de l'impact mondial de la Convention. Outre le fait qu'elle fournit un cadre pour une réponse de la justice pénale qui répond aux exigences des droits de l'homme et de l'État de droit, la Convention est soutenue par le Comité de la Convention sur la cybercriminalité (T-CY) pour les évaluations et le suivi, et par les activités de renforcement des capacités du C-PROC[15]. Ces éléments permettent une coopération, une sensibilisation et une réforme continues, conformément à ce traité.

(Projet de) Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques

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 fournir les moyens de protéger les droits des individus contre la criminalité.

[14] Voir les études préparées par C-PROC sur l'état mondial de la législation en matière de cybercriminalité.
[15] Voir le rapport T-CY sur "La Convention de Budapest sur la cybercriminalité. Avantages et impact dans la pratique".

Par conséquent, après presque quatre ans de consultation, le 28 mai 2021, le Comité de la Convention sur la cybercriminalité a achevé les négociations et approuvé le projet de deuxième protocole additionnel relatif au renforcement de la coopération en matière de cybercriminalité et de preuves électroniques. Le projet de protocole est le résultat d'un processus inclusif, impliquant plus de 600 experts de 75 pays, 91 sessions de négociation et six cycles de consultations des parties prenantes.

Le protocole aura une valeur opérationnelle pour les praticiens en ce qu'il prévoit :

- 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" ;
- des outils d'entraide (« vidéoconférence », « ECE ») ;
- des garanties en matière de protection des données pour permettre le flux de données à caractère personnel en vertu du protocole.

Il aura également une valeur politique dans la mesure où, grâce à ce protocole, la Convention sur la cybercriminalité restera pertinente et efficace, puisqu'il démontre qu'une coopération efficace dans le respect de l'État de droit et des 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.

Une fois adopté par le Comité des ministres, il pourrait être ouvert à la signature en mars 2022.

Le C-PROC a facilité ce travail dans le cadre des projets Cybercrime@Octopus et Octopus et a soutenu les réunions plénières de rédaction du protocole et les réunions du groupe de rédaction et des sous-groupes.

Des informations sur le futur protocole ont déjà été fournies dans le cadre d'un certain nombre d'activités du C-PROC. Lorsque le protocole sera ouvert à la signature, il faudra renforcer les capacités pour soutenir sa mise en œuvre. Ce soutien pourra être fourni sans délai, car il est déjà prévu dans les projets C-PROC actuels.

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

En décembre 2019, par la résolution 74/247, l'Assemblée générale des Nations unies a décidé de créer un « 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 ». Le comité ad hoc devra notamment prendre « pleinement en considération les instruments internationaux existants ».

En mai 2021, l'Assemblée générale a adopté la résolution 75/282, intitulée « Lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles » concernant les modalités du processus d'élaboration du traité. La première session de fond est prévue du 17 au 28 janvier 2022 à New York.

L'achèvement du deuxième protocole additionnel à la Convention sur la cybercriminalité en 2021 fournira aux États parties à la Convention de Budapest des repères concernant tant la substance que les garanties nécessaires en matière de droits de l'homme, d'État de droit et de protection des données, au respect desquels il conviendra de veiller dans le cadre d'un futur traité des Nations unies.

Le C-PROC pourra être amené à soutenir la participation d'experts des pays prioritaires du projet aux réunions de l'ONU liées à ce processus.

Covid-19 et renforcement des capacités

La pandémie de Covid-19 a entraîné une augmentation massive de la cybercriminalité, soulignant la pertinence de la Convention de Budapest et du renforcement des capacités connexes par le C-PROC. Cependant, elle a également continué à façonner la manière dont le C-PROC a mené ses activités de renforcement des capacités. La quasi-totalité des 395 activités - à l'exception des recherches et des études documentaires - se sont déroulées en ligne, sous la forme de webinaires ouverts ou restreints, d'ateliers consultatifs sur la législation en matière de cybercriminalité, de réunions par pays pour l'élaboration de procédures opérationnelles standard pour les preuves électroniques, d'exercices sur table pour les décideurs, d'ateliers de formation des services répressifs ou d'autres types d'activités.

Un certain nombre d'outils en ligne ont été développés ou améliorés, tels que les « wikis pays » et les « profils juridiques » sur la plate-forme Octopus, la plateforme dédiée à la cyberviolence ou celle à la cybercriminalité et Covid-19.

Le personnel du C-PROC a acquis des compétences supplémentaires pour la réalisation d'activités en ligne, et l'infrastructure technique du Bureau a encore été améliorée.

Anticipant la poursuite des événements en ligne après la Covid, une nouvelle plateforme C-PROC pour l'apprentissage en ligne et la fourniture de formations judiciaires en ligne est en cours de développement dans le cadre du projet Octopus et devrait être opérationnelle en 2022.

3. Résumé des projets et des résultats pour la période octobre 2020 à septembre 2021

Projets en cours

Entre octobre 2020 et septembre 2021, le C-PROC a soutenu environ 395 activités dans le cadre des projets énumérés ci-dessous :

Liste des projets (octobre 2020 - septembre 2021)			
Titre du projet	**Durée**	**Budget**	**Financement**
Cybercriminalité@Octopus	janvier 2014 - décembre 2020	4 millions d'euros	Contributions volontaires (Estonie, Hongrie, Monaco, Pays-Bas, Roumanie, Slovaquie, Royaume-Uni, Japon, États-Unis et Microsoft)
Extension du projet GLACY+ sur l'action mondiale contre la cybercriminalité	mars 2016 - février 2024	18,9 millions d'euros	PC 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 (Hongrie, Royaume-Uni, Canada, Japon et États-Unis)
Projet iPROCEEDS-2 visant les produits du crime sur l'internet et la sécurisation des preuves électroniques en Europe du Sud-Est et en Turquie	janvier 2020 - juin 2023	4,95 millions d'euros	UE/CoE PC (10% BO)
Projet EndOCSEA@EUROPE contre l'exploitation et les abus sexuels des enfants en ligne	juillet 2018 - juin 2021	0,97 million d'euros	Fonds de lutte contre la violence à l'égard des enfants
CyberSouth sur le renforcement des capacités dans le voisinage sud	juillet 2017 - décembre 2021	5 millions d'euros	UE/CoE PC (10% BO)
Projet CyberEast sur l'action contre la cybercriminalité pour la résilience cybernétique dans la région du partenariat oriental	juin 2019 - juin 2022	4,22 millions d'euros	UE/CoE PC (10% BO)

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

En septembre 2021, le budget combiné des projets en cours s'élevait à quelque 38 millions d'euros [16].

Le Bureau s'appuie dans une large mesure sur un financement externe. Au cours de l'année écoulée, plus de 90 % de son budget a été financé par des contributions volontaires. L'Union européenne est restée le principal donateur grâce à des programmes conjoints cofinancés par le Conseil de l'Europe. Les Etats-Unis d'Amérique ont également mis à disposition des fonds importants et la Hongrie, le Royaume-Uni, la Canada et le Japon ont également contribué. Le Bureau bénéficie en outre du soutien du gouvernement de la Roumanie, qui continue à fournir des espaces de bureaux à titre gracieux.

Alors que Cybercrime@Octopus, le projet Octopus et EndOCSEA@EUROPE sont ou ont été entièrement financés par des contributions volontaires, les programmes conjoints avec l'Union européenne comprennent un cofinancement de 10% du budget du Conseil de l'Europe.

Résultats

Capacités de la justice pénale

Durant la période de référence couverte par ce rappprt, le C-PROC a mené des activités tendant au renforcement des capacités de la justice pénale en particulier dans les 35 pays actuellement prioritaires qui peuvent bénéficier d'un large éventail d'assistance. Plus de 80 autres pays ont participé à au moins une partie des activités.

Ces activités se sont concentrées en particulier sur :

- la législation nationale sur la cybercriminalité et les preuves électroniques ainsi que sur la protection des données ;
- 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 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 oeuvre de l'Agenda 2030 des Nations unies pour le développement durable, en particulier 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 :

[16] 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.

- **CyberEst:** L'élaboration de politiques et de réformes législatives a occupé une place importante dans tous les États du partenariat oriental (à l'exception du Belarus). Ceci est complété par le lancement d'enquêtes d'opinion publique sur la cybercriminalité et la cybersécurité. Le projet a permis de renforcer les capacités des autorités pénales et la coopération interinstitutionnelle grâce à une série de discussions en ligne sur la protection des données, à l'élaboration de procédures opérationnelles standard, à de nombreuses sessions de formation et à des exercices pratiques. Quelque 68 activités ont été soutenues par ce projet au cours de l'année écoulée.

- **CyberSouth:** Les cadres juridiques pour la protection des données personnelles dans les pays prioritaires (Algérie, Jordanie, Liban, Maroc et Tunisie) ont été évalués et des recommandations ont été préparées avec le soutien du projet. Des matériels de formation judiciaire ont été développés en Algérie, au Liban et en Tunisie. Les capacités de coopération policière et judiciaire en matière de cybercriminalité et de preuves électroniques ont été renforcées et le développement de stratégies contre la cybercriminalité a été encouragé dans les pays prioritaires. Quelque 62 activités ont été soutenues par ce projet au cours de l'année écoulée.

- **GLACY+:** Des réformes législatives et des révisions de politiques sur la cybercriminalité, les preuves électroniques et la protection des données ont été soutenues, en particulier dans les pays d'Afrique, d'Asie, du Pacifique et des Caraïbes (par exemple, Belize, Botswana, Burkina Faso, Côte d'Ivoire, Gambie, Fidji, Kiribati, Maldives, Ile Maurice, Mozambique, Namibie, Nigeria, Papouasie-Nouvelle-Guinée, Sierra Leone, Soudan et Tonga). La coopération régionale en Afrique a été renforcée par l'organisation du deuxième Forum africain. Ce forum a également encouragé l'utilisation de la Convention de Budapest en Afrique. GLACY+ a contribué de manière significative à la consolidation de la communauté des formateurs judiciaires et à la création d'un réseau international de formateurs judiciaires sur la cybercriminalité et les preuves électroniques. Quelque 128 activités ont été soutenues par ce projet au cours de l'année écoulée.

- **iPROCEEDS-2:** un guide sur la saisie des crypto-monnaies a été produit et est rapidement devenu une "boîte à outils" pour les enquêteurs au niveau international. Les connaissances des magistrats sur les enquêtes relatives à l'exploitation sexuelle des enfants en ligne ont été améliorées grâce à des cours de formation en ligne. Le processus d'entraide judiciaire a été amélioré grâce à un cours régional de formation judiciaire spécialisée sur la coopération internationale et le suivi par des ateliers régionaux et nationaux. Le projet a soutenu plus de 90 activités au cours de l'année écoulée.

- **EndOCSEA@Europe:** Les connaissances et les capacités des autorités de justice pénale ont été renforcées grâce à une formation pilote sur l'exploitation et l'abus sexuel des enfants en ligne destinée aux juges, aux procureurs et à la police nationale de la République de Moldavie. La conférence régionale sur l'amélioration des capacités opérationnelles pour lutter contre l'exploitation et l'abus sexuels des enfants en ligne (OCSEA) a présenté le module de formation pour les forces de l'ordre, les juges et les procureurs; il a été traduit en 11 langues et est disponible sur demande. Quelque 25 activités ont été soutenues par ce projet au cours de l'année écoulée. Le projet s'est terminé en juin 2021.

- **Cybercrime@Octopus** et sa continuation, le **projet Octopus :** ils ont permis d'étendre les activités de renforcement des capacités et les modifications législatives à la région des Caraïbes (Barbade, Guyane, Montserrat, Jamaïque, Sainte-Lucie, Suriname et Trinité-et-Tobago), ainsi qu'à d'autres pays d'Afrique et d'Asie. Une série de webinaires a été lancée ainsi que d'autres activités sur la cybercriminalité liée au COVID-19 en Asie. La lutte contre l'exploitation et les abus sexuels des enfants en ligne a été encouragée par la préparation de profils nationaux et un atelier régional pour l'Asie. Une attention particulière a été accordée à la sensibilisation des décideurs politiques aux menaces de la cybercriminalité par le biais d'activités conjointes avec d'autres partenaires (webinaires parlementaires). Quelque 72 activités ont été soutenues par ces projets au cours de l'année écoulée.

Guides et outils

Le C-PROC, également en partenariat avec d'autres organisations internationales (par exemple INTERPOL), a élaboré un certain nombre de guides et d'outils sur des questions liées à la cybercriminalité et aux preuves électroniques (parmi les exemples récents, citons un « guide sur les statistiques de la justice pénale en matière de cybercriminalité », le « guide sur les crypto-monnaies » susmentionné et un « guide pour les premiers intervenants dans les enquêtes sur la cybercriminalité »). Ces guides ont ensuite été utilisés dans des ateliers nationaux ou comme documents de référence, par exemple lors de l'élaboration de procédures opérationnelles standard nationales.

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.

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. En conséquence, de nombreux pays ont soit adopté une telle législation, soit avancé dans leurs réformes entre octobre 2020 et septembre 2021. Le C-PROC tient à jour une base de données sur la législation relative à la cybercriminalité dans les pays du monde entier. Par exemple, le dernier aperçu rapide de « l'état mondial de la législation sur la cybercriminalité » montre qu'en juin 2021, 124 États (soit 64 % des membres de l'ONU) avaient mis en place des dispositions de droit pénal substantiel correspondant largement à celles de la Convention de Budapest. Cela représente une augmentation de 18 États depuis février 2020. Citons par exemple l'Afrique du Sud, le Belize, le Congo, les Fidji, le Mozambique, le Vanuatu ou la Zambie. La plupart d'entre eux avaient bénéficié de l'assistance du C-PROC.

Des informations spécifiques à chaque pays, sous forme de « wikis » et de « profils juridiques », sont disponibles sur la Communauté Octopus.

En outre, le C-PROC, en coopération avec l'Unité de protection des données du Conseil de l'Europe, a soutenu les réformes de la législation sur la protection des données conformément à la Convention 108+ » dans un certain nombre de pays (voir ci-dessous).

Synergies

Le renforcement des capacités crée des synergies et les activités du C-PROC ont continué à être menées en partenariat avec de multiples organisations, parmi lesquelles l'Union européenne, EUROJUST, EUROPOL, le Groupe européen d'éducation et de formation en matière de cybercriminalité (ECTEG), l'Institut d'études de sécurité de l'UE, la Commission de l'Union africaine, CARICOM, la Communauté des pays de langue portugaise (CPLP), la CEDEAO, le FOPREL, le Forum mondial pour la cyber-expertise (GFCE), l'Association internationale des procureurs (IAP), INTERPOL, l'Organisation des États américains, le Pacific Island Law Officers Network (PILON), les Nations unies, le ministère de la Justice et 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'Union européenne (ElPAcCTO, SIRIUS, OCWAR_C) qui ont la cybercriminalité et la preuve électronique parmi leurs thèmes pour assurer la promotion des politiques internationales similaires sur la 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 du Conseil de l'Europe. GLACY+, CyberEast et CyberSouth ont assisté plusieurs pays dans la mise en œuvre des activités de renforcement des capacités en matière de protection des données conformément à la Convention “108+”, notamment en Arménie, Géorgie et Moldova, et en Algérie, Colombie, Éthiopie, Gambie, Jordanie, au Liban, au Maroc, en Namibie, au Pérou, en Thaïlande et en Tunisie.

EndOCSEA@Europe a été mis en œuvre par la Division des droits de l'enfant avec le soutien de C-PROC et est une illustration des synergies entre les Conventions de Budapest et de Lanzarote. La ressource en ligne sur la « cyberviolence » est un exemple des synergies entre les Conventions de Budapest, de Lanzarote et d'Istanbul.

4. Conclusions

Impact

Le Bureau de programme sur la cybercriminalité du Conseil de l'Europe a continué, entre octobre 2020 et septembre 2021, à produire un impact sur les capacités de la justice pénale et la législation sur la cybercriminalité et les preuves électroniques basées sur la Convention de Budapest, dans des pays de toutes les régions du monde.

Le C-PROC a répondu aux restrictions liées au Covid-19 en améliorant ses ressources techniques et humaines, ainsi que ses compétences pour la réalisation d'activités en ligne, et a ainsi pu mettre en œuvre près de 400 activités au cours de cette période.

Par l'intermédiaire du Bureau de programme sur la cybercriminalité, le Conseil de l'Europe continue à jouer un rôle de premier plan en termes de renforcement des capacités sur la cybercriminalité et les preuves électroniques. Les synergies avec les organisations et projets pertinents ont encore augmenté au cours des douze derniers mois.

De nombreuses activités ont porté sur le renforcement de la législation et des systèmes de protection des données afin de garantir que les réponses efficaces à la cybercriminalité s'accompagnent de garanties en matière de droits de l'homme et d'État de droit.

La formule de la Convention de Budapest 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. Avec le deuxième protocole additionnel à venir, la Convention de Budapest devrait rester la norme internationale la plus pertinente en matière de cybercriminalité pour les années à venir. Le renforcement des capacités a été et restera un facteur majeur d'augmentation du nombre d'adhésions à la Convention et à ses Protocoles.

Priorités

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

- Soutenir l'ouverture à la signature et la mise en œuvre ultérieure du deuxième protocole additionnel à la Convention sur la cybercriminalité. Une conférence sur le « renforcement de la coopération en matière de cybercriminalité et de preuves électroniques » doit être organisée dans le cadre du projet Octopus à Strasbourg les 29 et 30 mars 2022. Elle permettrait l'ouverture à la signature du protocole.

- 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 œuvre de la Convention “108+”.

- Améliorer encore les capacités de mise en œuvre d'activités en ligne. Les priorités pour 2022 comprennent le lancement de la plateforme C-PROC pour l'apprentissage en ligne et la fourniture d'une formation judiciaire en ligne.

- Promouvoir davantage les synergies de la Convention de Budapest avec les instruments pertinents du Conseil de l'Europe, notamment son premier Protocole sur la xénophobie et le racisme (STCE 189) ainsi que les Conventions sur la protection des données (STCE 223), de Lanzarote (STCE 201) et d'Istanbul (STCE 210), la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE 198) et MONEYVAL concernant les crypto-monnaies. D'autres synergies avec d'autres organisations seront également recherchées.

- Préparer l'extension des projets actuels 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 de Budapest dans d'autres parties du monde. Certains projets arriveront à leur terme dans un avenir proche, et un suivi sera nécessaire :

  - la prolongation du projet GLACY+ de 42 mois avec un complément de 5,5 millions d'euros est en préparation ;
  - la prolongation du projet CyberEast de 18 mois avec un complément de 1,08 million d'euros a été préparée et devrait être approuvée prochainement ;
  - le projet CyberSouth devait s'achever en décembre 2021 mais une mais une prolongation sans frais de 24 mois a été convenue en principe ;
  - de nouvelles propositions de projets seront élaborées dans le courant de l'année 2022.