COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Documents d'Information

SG/Inf(2020)32

12 novembre 2020

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

Rapport d'activité du C-PROC pour la période octobre 2019 – septembre 2020

Contenu

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, 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 2019 à septembre 2020.

Le C-PROC a soutenu environ 240 activités entre octobre 2019 et septembre 2020. Par le Bureau, le Conseil de l'Europe demeure un chef de file mondial en matière de renforcement des capacités dans le domaine de la cybercriminalité et des preuves électroniques.

En 2020, le Bureau a été affecté par la COVID-19 en ce notamment que la pandémie a entraîné une augmentation massive de la cybercriminalité, soulignant la pertinence de la Convention de Budapest et du renforcement nécessaire des capacités, mais aussi qu'elle a façonné la manière dont le Bureau a dû mener ses activités à partir de mars 2020. L'ensemble des 130 activités menées entre avril et septembre 2020, autres que les études documentaires, ont été déployées en ligne.

Le C-PROC, en dépit de la pandémie, a contribué de manière significative :

- Au renforcement des capacités en matière de justice pénale et de législation dans le domaine de la cybercriminalité et des preuves électroniques ;
- A de nouvelles adhésions à la Convention de Budapest et à sa mise en œuvre ;
- Aux travaux de préparation du 2ème Protocole Additionnel à la Convention de Budapest ;
- A la synergie avec les autres organisations et instruments pertinents.

En septembre 2020, le C-PROC constituait l'un des plus grands bureaux extérieurs du Conseil de l'Europe, avec un budget cumulé de plus de 38 millions d'euros pour des projets en cours et 35 employés.

Le Bureau s'est appuyé 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 États-Unis d'Amérique ont également mis à disposition des fonds importants. Les autres donateurs au cours de cette période ont été l'Estonie, le Royaume-Uni et le Japon. Le Bureau bénéficie en outredu soutien du gouvernement de la Roumanie, qui continue à fournir des espaces de bureaux à titre gracieux .

La formule de la Convention de Budapest comme norme commune, soutenue par le Comité de la Convention sur la cybercriminalité et le renforcement des capacité par le biais du C-PROC, a continué à générer un impact. Grâce au futur 2ème Protocole additionnel, le mécanisme de la Convention de Budapest devrait rester la norme internationale la plus pertinente pour les années à venir.

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) à Bucarest, Roumanie, pendant la période allant d'octobre 2019 à septembre 2020[1].

Le Bureau est opérationnel depuis avril 2014. Son ouverture 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 de renforcement des capacités en matière de cybercriminalité du Conseil de l'Europe, dans toutes les régions du monde[4].

Cette période a été marquée par la pandémie COVID-19 à partir de mars 2020 et le présent rapport montre de quelle façon le Bureau a continué à être productif dans ce contexte.

Le C-PROC et la pandémie COVID-19

Cybercriminalité liée à COVID-19

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, ainsi que pour la paix et la stabilité internationales, et elle a un impact social et économique important.

Si cela a été illustré ces dernières années par des attaques de logiciels de rançon, comme "WannaCry", qui ont notamment paralysé des hôpitaux, ou par des interférences électorales, la cybercriminalité liée à la COVID-19 a encore ampliphié ce phénomène. Cela a conduit certains à parler de « pandémie numérique ». La COVID-19 a forcé les sociétés à s'appuyer encore plus sur les systèmes informatiques pour communiquer, faire des achats, partager et recevoir des informations et atténuer l'impact de la distanciation sociale et des autres mesures prises pour contenir la pandémie. Le télétravail et les réunions virtuelles sont devenus la norme.

Cette dépendance a été, et est encore exploitée à grande échelle par des acteurs malveillants, pour des campagnes de hameçonnage (« phishing ») et la distribution de logiciels malveillants, attaques de rançons (« ransomware ») et autres contre les infrastructures d'information critiques, mécanismes de fraude et de la diffusion de désinformation. L'exploitation et les abus sexuels d'enfants en ligne ont également augmenté[5].

---

[1] La décision créant le C-PROC (voir ci-dessous) contenait une demande au/à la Secrétaire Général(e) de présenter de tels 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

[2] C-PROC est situé à la Maison des Nations Unies à Bucarest. Les bureaux sont alloués au Conseil de l'Europe et ne sont pas loués par le gouvernement roumain en vertu d'un protocole d'accord.

[3] Decision CM/Del/Dec(2013)1180/10.4 du 9 octobre 2013, lors de sa 1180e réunion.

[4] Pour connaître l'approche du Conseil de l'Europe en matière de cybercriminalité, voir le sommaire dans l'Annexe.

[5] Cela a été confirmé par EUROPOL, INTERPOL et les rapports de nombreuses autres organisations des secteurs public et privé, y compris la COVID-19 Cyber Threat Coalition. Une ressource en ligne de C-PROC rend plus d'informations disponibles.

Les autorités de justice pénale doivent coopérer pleinement pour détecter, enquêter, attribuer et poursuivre les infractions susmentionnées et traduire en justice ceux qui exploitent la pandémie de COVID-19 à leurs propres fins criminelles. Avec la Convention de Budapest, 65 États disposent d'un cadre pour une coopération efficace avec les garanties nécessaires de l'État de droit.

Le C-PROC a notamment créé une ressource en ligne pour promouvoir cette coopération. Le futur 2ème protocole additionnel fournira des moyens supplémentaires de coopération efficace, y compris dans les situations d'urgence.

Impact de la COVID-19 sur le renforcement des capacités

La COVID-19 a non seulement entraîné une augmentation massive de la cybercriminalité, soulignant la pertinence de la Convention de Budapest et du renforcement des capacités qui y est lié par le C-PROC, mais elle a aussi fortement influencé la manière dont le Bureau a dû mener ses activités à partir de mars 2020 :

- Les 130 activités menées entre avril et septembre 2020, autres que les études documentaires, ont toutes été mises en œuvre en ligne. Ces activités allaient de webinaires ouverts ou restreints à des ateliers consultatifs sur la législation en matière de cybercriminalité, à des réunions par pays sur l'élaboration de procédures opérationnelles standard pour les preuves électroniques, des exercices sur table pour les décideurs politiques, des ateliers de formation des services répressifs et d'autres types d'activités[6]. Le Bureau a également soutenu des réunions virtuelles liées aux négociations du protocole du T-CY.

- D'autres ressources en ligne ont été développées ou améliorées, y inclus

  - la Communauté Octopus avec des "wikis pays", des "profils juridiques", des procédures de coopération internationale spécifiques à chaque pays, ainsi que des supports et guides de formation ;
  - un outil sur les webinaires ;
  - un portail sur la cybercriminalité liée à la COVID-19 ;
  - des ressources sur la cyberviolence.

- L'infrastructure du C-PROC a été améliorée afin de fournir la bande passante et la capacité technique nécessaires aux activités en ligne. Le personnel a été très polyvalent et adapté, ou a été formé à l'organisation d'activités virtuelles, et le Bureau a obtenu un accès administrateur aux plateformes nécessaires à ces activités.

- Le Bureau s'est engagé dans une coopération en ligne accrue avec une série de partenaires, dont l'Union européenne, INTERPOL, la CARICOM, le Groupe de travail anti-hameçonnage, les Nations Unies et bien d'autres.

[6] Voir la liste des activités en annexe ou des exemples dans la rubrique "news" sur www.coe.int/cybercrime.

Résumé des projets et des résultats pour la période octobre 2019 - septembre 2020

Aperçu des projets en cours

Entre octobre 2019 et septembre 2020, le C-PROC a soutenu environ 240 activités dans le cadre des projets énumérés ci-dessous.

Liste des projets (octobre 2019 - septembre 2020)			
Titre du projet	Durée	Budget	Financement
Cybercrime@Octopus	janvier 2014 - décembre 2020	EUR 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	mar 2016 - fév 2024	18,9 millions d'euros	UE/CoE JP (y inclus 10% budget ordinaire – BO - du Conseil de l'Europe)
Projet iPROCEEDS ciblant les produits du crime sur l'internet en Europe du Sud-Est et en Turquie	jan 2016 - déc 2019	5,56 millions d'euros	UE/CoE JP (10% BO)
Projet iPROCEEDS-2 visant les produits du crime sur 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 JP (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 pour l'élimination de la violence à l'égard des enfants
CyberSouth sur le renforcement des capacités dans le voisinage sud	juillet 2017 - déc 2021	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 - juin 2022	4,22 millions d'euros	UE/CoE JP (10% BO)

Un inventaire détaillé des activités soutenues ou accomplies, ainsi que d'autres informations sont disponibles en ligne.

En septembre 2020, le budget combiné des projets en cours s'élevait à quelque 38 millions d'euros. Cela représente une nouvelle augmentation par rapport aux années précédentes[7].

[7] 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.

Le Bureau s'appuie 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 États-Unis d'Amérique ont également mis à disposition des fonds importants. Les autres donateurs durant cette période ont été l'Estonie, le Royaume-Uni et le Japon. Le Bureau bénéficie en outredu soutien du gouvernement de la Roumanie, qui continue à fournir des espaces de bureaux à titre gracieux.

Alors que Cybercrime@Octopus et EndOCSEA@EUROPE sont 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

D'octobre 2019 à septembre 2020, le C-PROC a contribué de manière significative au renforcement des capacités de la justice pénale, dans des pays du monde entier. Outre les 45 pays prioritaires éligibles à l'ensemble des aides - allant des réformes législatives aux programmes de formation durables pour les praticiens de la justice pénale, en passant par les exercices pratiques et les procédures de coopération interinstitutionnelle, publique/privée et internationale - environ 80 autres pays ont participé à certaines des activités[8].

Exemples d'activités :

- CyberEast: 14 sessions de formation et ateliers sur les enquêtes en cybercriminalité et l'investigation numérique, la coopération avec les fournisseurs de services et les produits de la criminalité en ligne ont été organisés en étroite collaboration avec les académies nationales de formation ;
- CyberSouth: soutien aux procédures d'exploitation normalisées et boîtes à outils pour les premiers intervenants en cybercriminalité et preuves électroniques en Jordanie et au Maroc ; soutien aux groupes de travail sur le matériel de formation judiciaire au Liban et en Tunisie ;
- EndOCSEA@EUROPE: examen des stratégies de formation pour les forces de l'ordre en Arménie, Azerbaïdjan et Ukraine ; programme de formation sur l'Exploitation et aux Abus Sexuels des Enfants en Ligne (OCSEA) pour les forces de l'ordre, les juges et les procureurs ;
- GLACY+: prestation à distance d'activités dans le pays ou la région, tel que la formation « Premiers intervenants » ; ou apprentissage en ligne tel que le E-Evidence Boot Camp, le E-FIRST Course ;
- iPROCEEDS-2: participation des praticiens de la justice pénale des pays et des zones de projet au programme de Master à distance sur l'investigation informatique et les enquêtes en cybercriminalité de l'University College Dublin.

Le rapport du T-CY sur la "Convention de Budapest sur la cybercriminalité : avantages et impact dans la pratique" (juillet 2020) confirmé une fois de plus la valeur de l'approche spécifique du Conseil de l'Europe par laquelle, dans un processus dynamique, les normes de la Convention de Budapest et le suivi par le Comité de la Convention sur la cybercriminalité sont constamment soutenus par le renforcement des capacités du C-PROC.

[8] Pour des exemples spécifiques, voir l'Annexe.

Ce triangle génère un impact sur :

- la législation nationale sur la cybercriminalité et les preuves électroniques;
- les enquêtes nationales fondées sur cette législation ;
- la coopération internationale, y compris pour les cas graves et organisés de cybercriminalité ;
- la coopération public/privé ;
- le renforcement des capacités de la justice pénale.

Cela a contribué à son tour à la mise en œuvre de l'Agenda 2030 des Nations unies pour le développement durable, en particulier l'objectif 16 ("Promouvoir des sociétés pacifiques et inclusives pour le développement durable, assurer à tous l'accès à la justice et mettre en place des institutions efficaces, responsables et inclusives à tous les niveaux").

La législation sur la cybercriminalité

L'aide au renforcement de la législation nationale sur la cybercriminalité et les preuves électroniques est un élément majeur de tous les projets. Ainsi, de nombreux pays ont soit adopté une telle législation, soit avancé dans leurs réformes entre octobre 2019 et 2020.

Le C-PROC suit de près les développements à cet égard. La mise à jour de l'"État mondial de la législation sur la cybercriminalité" (publiée en mars 2020) montre une augmentation du nombre d'États ayant adopté une législation pénale de fond conforme à la Convention de Budapest. En février 2020, 106 États (soit 55 % des membres des Nations unies) avaient mis en place une telle législation. D'autres pays ont suivi leur exemple entre mars et septembre 2020. Nombre d'entre eux ont bénéficié de l'assistance du C-PROC, souvent non seulement en matière de cybercriminalité mais aussi de législation sur la protection des données conformément à la « Convention 108+ » (Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE 223).

La Communauté Octopus propose des informations spécifiques à chaque pays sous forme de « wiki pays » et de « profils juridiques ».

Adhésion à, et mise en oeuvre de la Convention de Budapest

La raison d'être du renforcement des capacités est de soutenir les gouvernements dans un processus de changement pour atteindre des objectifs définis. Si ces objectifs sont liés à une réponse efficace de la justice pénale à la cybercriminalité, conformément à la Convention de Budapest, ce processus est soutenu par le C-PROC.

Le renforcement des capacités reste un facteur essentiel pour l'augmentation du nombre de membres de la Convention de Budapest. Il incite de nombreux pays à demander l'adhésion et aide les pays se préparant à devenir parties à remplir les obligations de la Convention et à s'engager dans une coopération internationale efficace.

Entre octobre 2019 et septembre 2020, la Colombie et le Pérou sont devenus parties. Le Brésil, le Burkina Faso, le Guatemala, le Niger et la Nouvelle-Zélande ont été invités à adhérer à la Convention de Budapest. Le C-PROC aide de nombreux autres pays à réformer leur législation nationale avant de faire une demande d'adhésion.

2ème Protocole additionnel à la Convention de Budapest

La préparation du 2ème Protocole a commencé en septembre 2017 et se poursuit dans le cadre du Comité de la Convention sur la cybercriminalité (T-CY). Ce nouveau Protocole doit permettre une coopération plus efficace en matière de cybercriminalité et de preuves électroniques, notamment :

- Dispositions pour une assistance mutuelle plus efficace ;
- Coopération accélérée dans les situations d'urgence ;
- Coopération directe avec les prestataires de services et les bureaux d'enregistrement des autres parties ;
- Garanties de protection des données.

Si un accord peut être trouvé sur ces dispositions, le protocole sera d'une grande valeur opérationnelle pour les praticiens, établira des normes internationales pour une coopération efficace avec des garanties appropriées et garantira la pertinence continue de la Convention de Budapest.

Le Bureau facilite ce travail grâce à son projet Cybercrime@Octopus, financé par des contributions volontaires. Le soutien apporté à plusieurs plénières de rédaction de protocole et à de nombreuses réunions de groupes et de sous-groupes de rédaction a permis de faire avancer les négociations de manière significative. La Conférence Octopus de novembre 2019 a offert une plateforme pour des consultations multipartites sur des projets de dispositions du Protocole.

La perspective de ce protocole renforce l'intérêt pour la Convention de Budapest et crée une demande accrue de renforcement des capacités. Les nouveaux projets C-PROC prévoient déjà la possibilité de soutenir la mise en œuvre du protocole dans différentes régions du monde dès qu'il sera disponible.

Synergies

Le renforcement des capacités crée des synergies. Comme les années précédentes, les activités de renforcement des capacités C-PROC ont été menées en partenariat avec de multiples organisations, parmi lesquelles l'Union européenne, EUROJUST, EUROPOL, l'Institut d'études de sécurité de l'UE, la Commission de l'Union africaine, la CARICOM, la Communauté des pays de langue portugaise (CPLP), la CEDEAO, le FOPREL, le Global Forum for Cyber Expertise (GFCE), l'Association internationale des procureurs, 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. La Conférence Octopus a réuni un grand nombre de ces parties prenantes de plus de 115 pays au Conseil de l'Europe à Strasbourg en novembre 2019. En juin et juillet 2020, une série de webinaires conjoints de l'Union européenne et du Conseil de l'Europe a été offerte pour faciliter le partage d'expérience entre praticiens pour l'élaboration des poltiques internationales 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.

Des synergies sont également créées avec d'autres instruments du Conseil de l'Europe. GLACY+ a assisté plusieurs pays dans la mise en œuvre de la « Convention 108+ » sur la protection des données.

Le projet EndOCSEA@Europe est mis en œuvre par la division des droits de l'enfant avec le soutien de C-PROC et illustre les synergies entre les Conventions de Budapest et de Lanzarote.

Les ressources en ligne sur la “cyberviolence” sont un autre exemple de synergies entre les Conventions de Budapest, de Lanzarote et d’Istanbul.

Conclusions

Impact

Le Bureau de programme sur la cybercriminalité, entre octobre 2019 et septembre 2020 – et en dépit de la pandémie COVID-19 – a contribué de manière significative au renforcement des capacités en matière de justice pénale et de législation dans le domaine de la cybercriminalité et des preuves électroniques, mais également à ma mise en œuvre de la Convention de Budapest et aux synergies avec les autres organisations et instruments pertinents.

A travers le C-PROC, le Conseil de l'Europe reste un chef de file mondial en matière de renforcement des capacités dans le domaine de la cybercriminalité et des preuves électroniques.

La formule de la Convention de Budapest comme norme commune, soutenue par le Comité de la Convention sur la cybercriminalité et le renforcement des capacité par le biais du C-PROC, ont continué à générer un impact. Grâce au futur 2ème Protocole additionnel, le mécanisme de la Convention de Budapest devrait rester la norme internationale la plus pertinente pour les années à venir.

Priorités

Le Bureau continuera à suivre la voie qui a fait ses preuves en matière de résultats et d'impact, en partenariat avec d'autres organisations. Les priorités spécifiques pour les douze prochains mois sont les suivantes :

- Accroître encore la capacité à fournir en ligne des activités de renforcement des capacités des ressources en ligne. Bien qu'il soit difficile de prévoir l'évolution de la pandémie et des restrictions qui y sont liées, il est presque certain que les activités en ligne resteront une caractéristique importante à l'avenir. Une combinaison bien conçue d'activités physiques et virtuelles peut contribuer à produire un impact plus important à moindre coût. En plus de la gamme d'activités virtuelles déjà réalisées par C-PROC, cela pourrait inclure dans les prochains mois :

  - la création de réseaux virtuels de praticiens dans et entre les différentes régions du monde ;
  - l'offre à d'autres organisations et initiatives d'une plate-forme pour la réalisation d'activités communes ;
  - la mise en place d'une plate-forme d'apprentissage et de formation en ligne
  - la poursuite du développement des ressources en ligne (nouveaux cours de formation judiciaire, guide des preuves électroniques, guide des statistiques sur la cybercriminalité, wikis nationaux et profils juridiques sur l'exploitation et les abus sexuels des enfants en ligne, etc.)

- Promouvoir de nouvelles synergies entre la Convention de Budapest et les normes connexes du Conseil de l'Europe, notamment son 1er 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).

- Soutenir la finalisation du 2ème protocole additionnel à la Convention de Budapest sur la cybercriminalité.

- Préparer de nouveaux projets et mobiliser des ressources. Le portefeuille actuel de projets couvre des régions prioritaires en Europe (région du partenariat oriental, et Europe du Sud-Est et Turquie) ainsi que des pays d'autres régions du monde qui se sont engagés à mettre en œuvre la Convention de Budapest. Certains projets prendront fin dans un avenir proche, et un suivi sera nécessaire :

  - Le projet Cybercrime@Octopus prendra fin en décembre 2020. Il sera suivi par le nouveau projet Octopus, doté d'un budget pouvant atteindre 5 millions d'euros et d'une durée de quatre ans, de janvier 2021 à décembre 2024. Une récente contribution américaine de 1,5 million de dollars US assure le financement initial. Des discussions avec d'autres donateurs sont en cours.
  - Le projet End-OCSEA@Europe sur la maltraitance des enfants en ligne doit prendre fin en juin 2021. Un projet de suivi serait nécessaire.
  - Le projet CyberSouth doit s'achever en décembre 2021 et les réflexions sur un éventuel suivi devraient commencer bientôt.

  Dans l'ensemble, le C-PROC est bien doté en ressources à ce stade. La nécessité, liée à la COVID-19, de mettre toutes les activités en ligne devrait permettre de réaliser d'importantes économies dans le cadre des projets. Une nouvelle budgétisation et une nouvelle planification avec une éventuelle extension des projets pourraient devoir être entreprises en consultation avec les donateurs dans un avenir proche.

Le C-PROC est bien préparé pour continuer à évoluer en termes de qualité, d'expertise, d'impact et de synergies pour une coopération mondiale sur la cybercriminalité et la preuve électronique.