www.coe.int/la cybercriminalité

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, le 13 juillet 2020
T-CY(2020)16FR_BC_Benefits_rep_Prov_1.docx

T-CY (2020)16

Comité de la Convention sur la cybercriminalité (T-CY)

La Convention de Budapest sur la cybercriminalité:

avantages et impact concrets

Table des matières

Résumé exécutif 3
1 Introduction 4
2 Législation nationale et utilisation pour les enquêtes et poursuites 5
2.1 Améliorations aux législations nationales et impact sur ces dernières 5
2.2 Enquêtes au niveau national 9
3 Coopération internationale 14
3.1 Exemples d'entraide dans la pratique 15
3.2 Utilisation des points de contact 24/7 21
3.3 Améliorations à la coopération du secteur privé du fait de l'adhésion à la Convention 24
4 Renforcement des capacités 28
4.1 Logique sous-jacente 28
4.2 Exemples d'activités de consolidation de capacités qui ont été menées 29
4.2.1 Afrique: Sénégal 30
4.2.2 Asie: Sri Lanka 34
4.2.3 Europe: Serbie 38
4.2.4 Amérique latine: République dominicaine 41
4.2.5 Pacifique: Tonga 44
4.3 Renforcement des capacités: les enseignements tirés 48
5 Conclusion 48
6 Annexe: Etats Parties, Signataires et Etats invités à adhérer à la Convention de Budapest (situation au 30 juin 2020) 50

Contact

Council of Europe
Secretariat of the Cybercrime Convention Committee
Strasbourg, France
Cybercrime@coe.int

Résumé exécutif

Le présent rapport a pour but d'illustrer les avantages que procure la Convention de Budapest sur la cybercriminalité et son impact afin de faciliter le dialogue avec les Etats et Parties intéressées par la coopération en matière de cybercriminalité. Il repose largement sur des informations émanant de praticiens dans les Etats parties au traité.

Le rapport cite des exemples de l'impact de la Convention de Budapest sur:

- les législations nationales des pays du monde entier en matière de cybercriminalité et de preuve électronique;
- les enquêtes nationales menées sur la base de ces législations nationales;
- la coopération internationale, y compris pour des affaires graves et organisées de cybercriminalité;
- coopération publique/privée;
- le renforcement des capacités de la justice pénale.

L'expérience pratique montre que la Convention de Budapest est davantage qu'un simple instrument juridique prévoyant l'incrimination de la cybercriminalité, des pouvoirs procéduraux pour recueillir et garantir les preuves électroniques et une base juridique pour la coopération internationale.

Renforcée par le Comité de la Convention sur la cybercriminalité (T-CY) et le Bureau des programmes spécialisé sur la cybercriminalité C–PROC pour la consolidation de capacités au niveau mondial, la Convention de Budapest est un cadre qui permet à des centaines de praticiens du monde entier de mettre en commun leur expérience et de nouer des relations favorisant la coopération dans des affaires spécifiques, notamment en situation d'urgence, au-delà des dispositions précises prévues dans cette Convention.

Tout pays peut bien entendu s'inspirer de la Convention dans son droit interne; toutefois, le fait de devenir Partie à ce traité procure des avantages supplémentaires:

- ce traité sert de fondement juridique pour la coopération internationale;
- les Etats Parties contribuent à faire évoluer la Convention par des notes d'orientation ou des protocoles additionnels;
- l'adhésion à la Convention entraîne l'adhésion à des réseaux de praticiens, en particulier les réseaux 24/7 de points de contact établis au titre de ce traité;
- les Etats Parties coopèrent mieux avec le secteur privé;
- les Etats parties et les Etats ayant demandé à adhérer à ce traité peuvent devenir des pays prioritaires et servir de point nodal pour la consolidation de capacités.

Etant donné que ce traité compte de plus en plus d'Etats membres, que les programmes de consolidation des capacités liés à cette Convention s'étoffent et que cette dernière évolue grâce au futur Deuxième protocole additionnel sur la coopération internationale renforcée et l'accès aux preuves dans le Cloud, le cadre de la Convention de Budapest devrait demeurer très pertinent et faire la différence partout dans le monde pour bien des années encore.

1 Introduction

La Convention sur la cybercriminalité, ouverte à la signature à Budapest, Hongrie, en novembre 2001, est considérée comme l'accord international le plus pertinent sur la cybercriminalité et la preuve électronique.

La Convention de Budapest prévoit (i) l'incrimination d'un certain nombre de comportements allant de l'accès illégal et l'atteinte à l'intégrité des données et des systèmes jusqu'à la fraude liée à l'informatique et à la pornographie enfantine; (ii) des outils de droit pénal pour enquêter dans des affaires de cybercriminalité et recueillir et sécuriser les preuves électroniques concernant tout crime; et (iii) une coopération internationale efficiente.

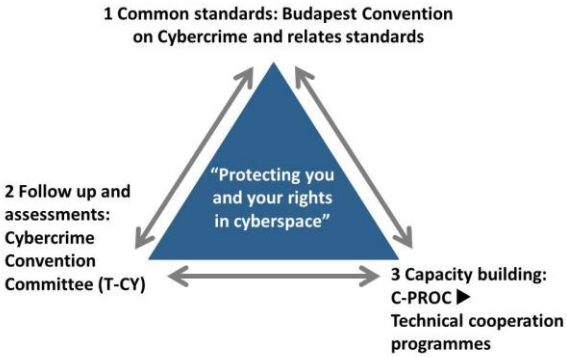
La Convention concilie la vision d'un Internet libre où les informations peuvent circuler, être accessibles et partagées librement, et la nécessité d'une réponse efficace de la justice pénale dans des affaires d'abus criminels de l'Internet. Les restrictions sont définies de manière étroite puisque seules certaines infractions spécifiques constitutives d'un crime passible de la justice pénale font l'objet d'enquêtes et poursuites et que les données spécifiées nécessaires comme preuves dans des procédures pénales spécifiques sont garanties sous réserve des protections liées aux droits de l'homme et à l'État de droit.

La Convention est complétée par un Protocole additionnel couvrant l'incrimination d'actes de nature raciste ou xénophobe commis au moyen de systèmes informatiques (STCE n° 189). Un deuxième Protocole additionnel sur la coopération internationale renforcée et l'accès aux preuves dans le Cloud est en cours de négociation.

Le traité a été négocié par des membres du Conseil de l'Europe mais aussi par le Canada, le Japon, l'Afrique du Sud et les États-Unis; il est toutefois ouvert à l'adhésion de tout État et un certain nombre de pays d'Afrique, des Amériques et de la région Asie-Pacifique utilisent cette possibilité dans l'intérêt d'une réponse efficace du système de justice pénale contre la cybercriminalité.

Les Etats Parties à la Convention sur la cybercriminalité, qui l'ont signée ou qui ont été invités à y adhérer participent en tant que membres ou observateurs (signataires ou invités) au Comité de la Convention sur la cybercriminalité (T-CY).Celui-ci, entre autres choses, évalue la mise en œuvre de la Convention par les Parties, adopte des notes d'orientation ou prépare des instruments juridiques supplémentaires.

La Convention est également étayée par des projets de consolidation de capacités – gérés par le Bureau des programmes spécialisé du Conseil de l'Europe (C–PROC) en Roumanie – qui aide les pays du monde entier à se doter des capacités nécessaires pour l'enquête, la poursuite et le jugement des infractions informatiques et des autres affaires impliquant les preuves électroniques, en conformité avec la Convention et avec les recommandations du T-CY.



La Convention de Budapest est donc bien davantage qu'un simple instrument juridique; elle est un cadre qui permet à des centaines de praticiens des Etats Parties de mettre en commun leur expérience et de nouer des relations favorisant la coopération dans des affaires spécifiques, notamment en situation d'urgence, au-delà des dispositions précises prévues dans cette Convention.
Le présent document a pour but d'illustrer les avantages et l'impact concrets de ce traité, afin de faciliter le dialogue avec les Etats et parties prenantes pour qui la Convention de Budapest présente un intérêt.

Préparé à la suite d'une décision prise par le T-CY en 2019, l'aperçu s'appuie principalement sur des informations transmises par des Parties pour juin 2020. Il n'a pas pour ambition de présenter une évaluation détaillée ou de remplacer des évaluations réalisées par le T-CY. Le rapport a été validé par le T-CY en juillet 2020.

2 Législation nationale et utilisation pour les enquêtes et poursuites

2.1 Améliorations aux législations nationales et impact sur ces dernières

La Convention de Budapest fait obligation aux Etats parties de veiller à ce que les infractions contre des systèmes informatiques et au moyen de systèmes informatiques, prévues aux articles 2 à 12, soient incriminées dans leur droit interne, et à ce que leurs autorités de justice pénale soient dotées des pouvoirs prescrits dans le droit procédural, non seulement pour enquêter dans des affaires de cybercriminalité mais aussi pour traiter toute infraction où la preuve se présente sous forme électronique. Un droit interne conforme à la Convention de Budapest facilite en outre la coopération internationale puisqu'il permet de répondre à l'exigence de double incrimination. A certains des pouvoirs procéduraux au niveau national prévus à la Convention correspond donc une disposition dans le pilier sur la coopération internationale.

Droit pénal matériel: infractions	Droit de procédure pour recueillir et sécuriser des preuves et pour mener des enquêtes	Coopération internationale
Art. 2 – Accès illégal Art. 3 – Interception illégale Art. 4 – Atteinte à l'intégrité des données Art. 5 – Atteinte à l'intégrité du système Art. 6 – Abus de dispositifs Art. 7 – Falsification informatique Art. 8 – Fraude informatique Art. 9 – Pornographie enfantine Art. 10 – Infractions liées à la propriété intellectuelle Art. 11 – Tentative et complicité Art. 12 – Responsabilité des personnes morales	Art. 14 – Portée d'application des mesures du droit de procédure Art. 15 – Conditions et sauvegarde Art. 16 – Conservation rapide Art. 17 –Conservation et divulgation partielle rapides de données relatives au trafic Art. 18 – Injonction de produire Art. 19 – Perquisition et saisie Art. 20 – Collecte en temps réel des données relatives au trafic Art. 21 – Interception de données relatives au contenu	Art. 23 – Principes généraux Art. 24 – Extradition Art. 25 – Principes généraux relatifs à l'entraide Art. 26 – Information spontanée Art. 27 – Entraide en l'absence d'accords internationaux Art. 28 – Confidentialité Art. 29 – Conservation rapide de données Art. 30 – Divulgation partielle de données relatives au trafic Art. 31 – Entraide concernant l'accès aux données Art. 32 – Accès transfrontière Art. 33 – Entraide pour la collecte en temps réel de données relatives au trafic Art. 34 – Entraide en matière d'interception de contenu Art. 35 – Réseau 24/7

Au mois de mai 2020, 76 Etats (39 %) étaient soit Parties (65 Etats), soit signataires (3) à la Convention de Budapest ou avaient été invités à y adhérer (8). Ainsi, le Guatemala et le Niger ont été invités en avril 2020 à devenir Parties à cette Convention, et sont en train de finaliser leurs procédures internes à cette

fin. Tous ces Etats soit ont déjà réformé leur droit interne, soit sont en train de le faire pour le mettre en conformité avec ce traité.

Toutefois, l'impact de la Convention de Budapest pour ce qui est de la législation n'est pas limité à ces Etats. Une étude récente sur la situation mondiale de la législation en matière de cybercriminalité a conclu qu'en février 2020:

- ces dernières années, quelque 177 États (92 %) dans le monde étaient en train de reformer leur législation ou l'avaient fait;

- les Parties ne sont pas les seules à s'être inspirées de la Convention de Budapest pour réformer leur droit : quelque 153 membres des Nations unies (79%) s'étaient inspirés de cette Convention en tant que lignes directrices et source pour leurs réformes;

- quelque 106 Etats (55 %) semblent avoir adopté des dispositions internes spécifiques correspondant en général aux articles de droit pénal matériel de la Convention de Budapest. Un tiers de plus des Etats a adopté au moins certaines dispositions spécifiques de droit pénal matériel dans l'esprit de ce traité. Au cours des sept dernières années, les progrès en ce sens ont été particulièrement forts en Afrique;

- quelque 82 Etats (42 %) se sont dotées de pouvoirs procéduraux spécifiques tandis que de nombreux Etats s'appuient encore sur des dispositions générales de droit pénal pour enquêter dans des affaires de cybercriminalité et recueillir et sécuriser des preuves électroniques. À l'évidence, reformer le droit procédural et attribuer de pouvoirs procéduraux spécifiques pour recueillir et sécuriser la preuve électronique qui sera ensuite utilisée dans des procédures pénales (correspondant aux articles 16 à 21 de la Convention de Budapest et sous réserve des protections prévues à l'article 15) est une entreprise plus complexe.

Cette performance est le résultat de la Convention de Budapest et des programmes de consolidation des capacités.

Étant donné l'impact considérable de la Convention de Budapest en tant que lignes directrices pour le droit interne dans le monde entier, nous nous bornerons à ne citer que quelques exemples.

- En 2017, le **Cabo-Verde** en 2017a adopté la Loi n°8/IX/2017, qui établit des procédures de droit pénal matériel et procédural ainsi que des dispositions de coopération internationale concernant la cybercriminalité et le recueil de la preuve électronique. Cette loi a été élaborée conformément à la Stratégie nationale sur la cybersécurité et aux dispositions de la Convention de Budapest.

- Le **Costa Rica** a passé en revue sa législation de manière exhaustive dans le processus d'adhésion à la Convention de Budapest, avec le soutien des experts du Conseil de l'Europe. En particulier, des représentants du Costa Rica ont analysé un nouveau projet de loi sur la lutte contre la cybercriminalité et fait des suggestions cet égard. Ce texte modifierait et réformerait certains articles du Code pénal et du Code de procédure pénale, et une troisième loi traiterait la procédure pénale et les mesures d'enquête. En outre, des représentants du Costa Rica ont mené un travail de fond pour incriminer l'exploitation sexuelle des enfants dans le droit fil de la Convention de Budapest et d'autres conventions internationales, ainsi que pour traiter de nombreuses autres formes d'exploitation sexuelle et de traite de personnes vulnérables.

- En 2013, la **Croatie** a mis sa loi sur le droit pénal matériel et procédural pleinement en conformité avec la Convention de Budapest, grâce à l'entrée en vigueur des nouveaux Codes pénal et de procédure pénale.

- La **République dominicaine** compte parmi le tout petit nombre de pays d'Amérique latine et des Caraïbes qui sont dotés d'une loi spécifique permettant d'enquêter, de poursuivre et de sanctionner la cybercriminalité, (la loi n° 53 – 07 sur les crimes et la criminalité high-tech), en vigueur depuis le 23 avril 2007, conjointement au Code pénal, au Code de procédure pénale et à d'autres dispositions législatives, forme le cadre juridique sur la cybercriminalité et la preuve électronique.

- La **Finlande** a modifié son Code pénal pour appliquer ses obligations vis-à-vis de la Convention de Budapest, et a introduit des pouvoirs procéduraux supplémentaires en lien avec ce traité par la Loi sur les mesures de coercition, adoptée en 2011 (en vigueur depuis 2014).

- La **France** a adopté de nombreux amendements à sa législation pour s'adapter à l'évolution de la cybercriminalité, grâce à la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui a permis par la suite la ratification de la Convention de Budapest sur la cybercriminalité.

- L'**Allemagne** a modifié son Code pénal en 2009 pour couvrir toutes les dispositions de droit matériel de la Convention de Budapest, les pouvoirs procéduraux étant prévus au Code de procédure pénale.

- Le **Ghana** a adopté la loi sur les transactions électroniques (Electronic Transactions Act 772 – "ETA") en 2008. Ce texte très complet prévoit de nombreuses infractions liées à la cybercriminalité et des pouvoirs procéduraux pour le traitement de la preuve électronique conformes à la Convention de Budapest. D'autres textes législatifs tels que la loi sur la criminalité économique organisée, de 2010 (Economic and Organised Crime Act - "EOCA"), et la loi sur les services de sécurité et de renseignement, de 1996 (Security and Intelligence Agencies Act 526 - "SIAA"), prévoient également des pouvoirs procéduraux concernant les enquêtes liées à la cybercriminalité.

- L'**Italie** a procédé à plusieurs amendements dans son cadre pénal liés à la cybercriminalité et aux pouvoirs procéduraux y afférent. Des dispositions supplémentaires ont été introduites en 2008, dans le droit fil de la Convention de Budapest.

- L'**île Maurice** a adopté en 2003 la loi sur l'abus de systèmes informatiques et la cybercriminalité (Computer Misuse and Cybercrime Act), qui suit la Convention de Budapest. Cette loi prévoit des infractions pénales liées à la cybercriminalité et les règles correspondantes pour les actes d'enquête et de procédure. Elle couvre également des questions concernant les poursuites, la juridiction, les extraditions et les saisies.

- Le **Pérou** a adopté en 2013, puis actualisé en 2014, sa loi sur le droit pénal matériel en matière de cybercriminalité. Cette loi couvre maintenant des infractions contre des systèmes de données et d'information, notamment l'accès illégal et les atteintes à l'intégrité des données de systèmes; les infractions liées à l'exploitation des enfants; le trafic illégal de données et l'interception de données; la fraude électronique; et les infractions liées au vol d'identité et à l'abus de dispositifs. La loi couvre tant les atteintes aux systèmes informatiques que l'utilisation de ces derniers pour commettre des crimes. En lien avec ce texte législatif, des dispositions réglementaires ont été prises pour faciliter la signature et la ratification par le Pérou de traités multilatéraux qui

garantiraient la coopération et d'autres Etats dans les poursuites contre la cybercriminalité. Des dispositions réglementaires ultérieures ont établi que les définitions dans la loi de 2014 devaient être comprises comme conforme aux définitions de l'article 1 de la Convention de Budapest.

► Le **Portugal** a adopté sa loi sur la cyber-communication en 2009 (Law 109/2009). Cette loi suit de manière générale la structure de la Convention de Budapest et transpose intégralement dans le droit interne toutes les dispositions de cette dernière sur le droit pénal matériel, les pouvoirs procéduraux en matière pénale et la coopération internationale.

► La **Roumanie**, par la loi 161/2003 (Titre III – Prévention et lutte contre la cybercriminalité), a traduit entièrement la Convention de Budapest dans son droit interne. En 2004, elle a ratifié la Convention sur la cybercriminalité (loi 64/2004) et, en 2009, le protocole additionnel concernant l'incrimination d'actes de nature raciste ou xénophobe commis au moyen de systèmes informatiques. En 2012/2013, ces dispositions ont ensuite été intégrées aux nouveaux Code pénal et de procédure pénale, qui sont entrés en vigueur en 2014.

► En 2005, la **Slovaquie** a adopté deux lois modifiant son Code pénal et son Code de procédure pénale pour répondre aux exigences de la Convention de Budapest.

► L'**Espagne** a effectué plusieurs modifications du droit matériel sur la cybercriminalité et des pouvoirs procéduraux connexes afin de satisfaire les dispositions de la Convention de Budapest. En 2015, l'Espagne a adopté des amendements supplémentaires par le biais de ses lois organiques 1 et 2/2015 sur la définition des infractions informatiques et par la loi organique 13/2015 (Ley Orgánica 13/2015), entre autres pour prévoir la conservation rapide de données informatiques stockées, les injonctions de produire, ainsi que les perquisitions et saisies de données informatiques stockées. L'Espagne a signalé en particulier qu'elle utilise la Convention de Budapest comme ressource allant au-delà de simples modifications à ces dispositions législatives, elle base ses manuels et formations juridiques internes sur les contenus de la Convention de Budapest. Elle utilise à la fois le texte du traité et son rapport explicatif pour les études et formation destinées au personnel de justice pénale, y compris les forces de police (voir explications plus loin), ainsi que pour interpréter les crimes matériels et outils procéduraux dans le droit espagnol qui dérivent de la Convention de Budapest. Cette interprétation est diffusée sous la forme de circulaires du Bureau du Procureur général de l'Espagne établissant les critères à suivre par les procureurs pour comprendre et appliquer les normes juridiques. La Convention de Budapest et son rapport explicatif constituent des bases essentielles pour plusieurs de ces circulaires:

- Circulaire 1/2019 FGE sur les dispositions communes et mesures d'assurance pour les procédures de recherche technologique.
- Circulaire 2/2019 FGE sur l'interception de communications téléphoniques et télématiques.
- Circulaire 5/2019 FGE sur l'enregistrement de dispositifs et d'équipement informatiques.
- Circulaire 3/2017 sur la réforme du Code pénal concernant les infractions de découverte et divulgation de secrets et les infractions liées à l'endommagement de dispositifs informatiques.

► En 2007, le **Sri Lanka** a adopté la loi sur les crimes informatiques 24/2007, largement basée sur la Convention de Budapest. De plus, la loi sur les fraudes aux dispositifs de paiement 30/2006, la loi sur la propriété intellectuelle 36/2003 et un certain nombre d'articles de portée générale du Code pénal et d'amendements s'appliquent aux infractions liées à la cybercriminalité. Le Code pénal, amendé par les lois d'amendement 22/2005, 16/2006 et 10/2018 contient des dispositions

pour traiter certaines problématiques liées aux images indécentes d'enfants. En outre, le Sri Lanka a adopté en 2018 des amendements à la loi sur l'assistance mutuelle en matière pénale (24/2018) qui compte désormais des dispositions spécifiques relatives a l'entraide judiciaire dans les affaires liées aux infractions informatiques et preuves électroniques, y compris la conservation rapide des données, en conformité avec la Convention de Budapest.

Ces quelques exemples d'Etats qui sont Parties à la Convention de Budapest ne sont qu'un échantillon parmi les nombreux autres qui ont adapté leur droit interne dans l'esprit de la Convention de Budapest ou qui sont en train de le faire – souvent avec l'assistance technique du Conseil de l'Europe – ; tel est le cas du Belize, du Bénin, de la Côte d'Ivoire, du Burkina Faso, de la Gambie, du Guatemala, des Fidji, du Kenya, du Niger ou du Nigéria notamment.

2.2 Enquêtes au niveau national

Lorsqu'on cite des exemples de l'utilisation de la Convention de Budapest dans des enquêtes et des poursuites nationales via les dispositions de droit interne, il importe de tenir compte des éléments suivants:

- Dans des Etats qui ont adopté des textes législatifs reposant sur la Convention de Budapest, toute enquête utilisant ces dispositions peut être reliée à ce traité. Cependant, les poursuites et les décisions de justice renverront aux articles du droit interne et non à la Convention de Budapest, sauf dans des cas où la preuve est obtenue au moyen des dispositions relatives à la coopération internationale.
- Les pouvoirs publics ne peuvent divulguer que des informations limitées, les détails pouvant être confidentiels ou les enquêtes en cours.

Toutefois, nous pouvons citer quelques exemples qui ont été mentionnés par des Etats Parties:

► Le Bureau du Procureur de la **Bosnie-Herzégovine** a signalé que:

- Dans au moins trois affaires, il s'est servi des mécanismes prévus aux articles 29 et 30 de la Convention de Budapest pour demander la conservation de données à des fournisseurs étrangers. Dans deux autres affaires, des demandes ont été envoyées pour des données concernant les abonnés en vertu de l'article 31 de la Convention.
- En 2013, le Bureau du Procureur du District de Brčko a mis en accusation une personne pour utilisation illégale du compte d'une autre personne en vue d'accéder à une page Internet privée et de changer les mots de passe ainsi que le code source de la page. Ceci a abouti à l'effacement automatique de toutes les données, constitutif de l'infraction d'atteinte à l'intégrité de données et programmes informatiques.
- Dans une autre affaire, l'accusé avait acheté à plusieurs reprises des biens et services sur Internet, procédé à une surveillance non autorisée des activités informatiques de tiers, et créé de faux documents au moyen de systèmes informatiques. L'accusé a été condamné pour fraude informatique et autres cyber infractions et pour avoir à l'aide de ces fraudes porté atteinte à des personnes et des entreprises; il s'est vu condamner à une peine de prison assortie d'une amende.
- Des changements procéduraux découlant de l'intégration de la Convention de Budapest (article 26, Information spontanée) dans la législation nationale ont aidé la Republika Srpska dans une enquête en 2019. Les accusés s'étaient vus reprocher la violation du droit de propriété (la création non autorisée d'un site Web Internet pour diffuser du contenu d'œuvres cinématographiques). Les mécanismes d'investigation basés sur les articles 29 et 32 de la Convention ont également été utilisés dans cette affaire.

- Une autre affaire en 2019 a permis d'utiliser d'autres mécanismes reposant sur la Convention de Budapest- des enquêteurs avaient reçu des informations d'un fournisseur américain de services sur Internet (ISP) concernant la diffusion de pornographie enfantine à partir de la Republika Srpska. L'enquête a identifié un auteur à Banja Luka et a permis la confiscation de 1000 éléments de médias pour le stockage, 42 disques durs, ordinateurs, téléphones mobiles et d'autres équipements utilisés pour stocker de la pornographie enfantine.
- Dans une affaire en 2018/2019, il a été fait usage des mécanismes de la Convention de Budapest prévus pour la coopération avec des fournisseurs étrangers de services sur Internet (ISP) en vue de la conservation et de la divulgation de données identifiant certains utilisateurs de réseaux sociaux. Enfin, ces méthodes ont été utilisées en 2019 pour des enquêtés liées à la mise en danger de la sécurité de personnalités en Républika Srpska. Dans cette affaire, un fournisseur américain de services sur Internet a fourni les données permettant d'identifier une cible.

► Le **Costa Rica** est devenu Partie à la Convention de Budapest en janvier 2018. En cinq ans (de 2014 à 2018), plus de 7000 affaires de cybercriminalité ont été enregistrées, dont la très grande majorité (6342) étaient liées à des fraudes. 94 de ces affaires de fraude ont abouti à des poursuites pénales. À la suite de son adhésion à la Convention de Budapest, le Costa Rica a établi un Service de lutte contre la cybercriminalité au sein du Bureau du Procureur public, qui s'appelle désormais le «Bureau du procureur délégué pour la fraude et la cybercriminalité» et coopère étroitement avec la police judiciaire dans les enquêtes pour des affaires de cybercriminalité. De ce fait, des groupes criminels organisés montant des fraudes au moyen de l'informatique ont été démantelés et des perquisitions et saisies menées. Les groupes criminels avaient une organisation complexe avec un service qui ciblait des victimes par la technique du phishing, de pharming et d'autres techniques d'ingénierie sociale, un autre service chargé de recruter des passeurs d'argent (mules), un troisième qui organisait les transferts de produits du crime et un quatrième qui collectait des informations sur les victimes potentielles.

► **La Finlande** a réalisé une perquisition à distance sur la base des dispositions de la Convention de Budapest dans une affaire impliquant des attaques multiples et graves par refus de service distribué (DDoS) à l'encontre de plusieurs services d'autorités finlandaises en 2017 et 2018. Le suspect s'était servi d'un dispositif mobile pour lancer les attaques de DDoS grâce à des services de crime commercial (*crime as a service*) Stresser pour automatiser les attaques par des botnets. La police a procédé à une perquisition à distance du site de messagerie du suspect et de ses comptes Stresser pour trouver des preuves que celui-ci s'était servi de ces services via un certain dispositif les jours où s'étaient produites les attaques. Les résultats des perquisitions à distance étaient cruciaux, car il n'y avait essentiellement pas d'autres moyens d'obtenir des preuves suffisantes que le suspect était à l'origine des attaques.

► La **France** a déclaré que ses services de lutte contre la cybercriminalité utilisent régulièrement le cadre de la Convention de Budapest comme outil d'investigation des attaques informatiques et a cité trois exemples d'affaires nationales basées sur des dispositions législatives liées à la Convention de Budapest:

- Dans la première affaire, les autorités de santé publique à Marseille ont mené une enquête sur l'importation et la vente d'un produit contenant du glyphosate non autorisé à la vente, qui était diffusé sous les marques de contrefaçonGALLUP360 et LUTESATE 360 et présentait des risques pour la consommation humaine. Les quatre accusés se sont vus infliger des peines de prison avec sursis et des amendes.

- Dans la deuxième affaire, les mêmes autorités ont enquêté sur un réseau de production de contrefaçons pour les médicaments PLAVIX et ZYPREXA, également impropres à l consommation humaine. L'enquête préliminaire a démarré avec la saisie de 40 000 conteneurs de médicaments, qui apparemment provenaient de Singapour et étaient commercialisés essentiellement en Europe (au Royaume-Uni, en France et en Suisse). Les trois accusés ont été condamnés en 2017 pour pratique illégale de la pharmacie, fraude impliquant un produit présentant un risque pour les personnes ou les animaux, et importation de produits contrefaits dangereux pour la santé humaine. Les deux accusés, qui étaient des personnes physiques, se sont vus infliger des peines de prison de diverses durées et une confiscation de leurs biens ou une amende financière. L'un d'entre eux a été interdit pendant cinq ans de gérer une activité commerciale. La personne morale s'est vue infliger une amende de 15 000 euros.
- Dans la dernière affaire, une enquête préliminaire avait abouti à la saisie de 6 000 cartons de cigarettes de contrebande MAYFAIR, d'une valeur de 387 000 euros. Elles avaient été apparemment importées d'Espagne et il était prévu de les vendre en Italie. Le danger pour la santé des consommateurs provenait de l'ignorance complète où l'on était quant à l'origine des cigarettes et à leur procédé de fabrication. L'accusé a été condamné en 2018 pour plusieurs chefs d'inculpation liés à la possession et distribution illégale de produits insuffisamment documentés et pour infraction liée au crime organisé. Il s'est vu infliger une peine de prison avec sursis et une amende de 300 000 euros.

► La **Hongrie** a cité un certain nombre d'exemples d'enquêtes nationales facilitées par les changements dans la procédure pénale sur la base de l'article 32 de la Convention de Budapest. L'article 32 (a) permet à une Partie d'accéder à des données informatiques stockées sur un système et accessibles publiquement (source ouverte) sans l'autorisation d'une autre Partie, quel que soit l'endroit géographique où les données sont stockées. L'article 32 (b) permet l'accès transfrontière à des données informatiques stockées – dans des circonstances soigneusement délimitées – avec le consentement licite et volontaire de quelqu'un qui a l'autorité pour divulguer ces données:

- Dans la première affaire, deux criminels, ensemble avec la victime, mineure, avaient pris place à bord d'un car qui se dirigeait vers la ville de X. Visiblement sous l'influence de produits stupéfiants et d'alcool, elle/il avait demandé aux criminels une cigarette. Ceux-ci lui avaient dits qu'ils la lui donneraient si elle/il descendait du car avec eux une fois arrivés à la ville de X. La victime est descendue du car et s'est rendue à la banque de X où les auteurs de l'infraction lui ont donné une cigarette. Après l'avoir fumée, la victime s'est sentie totalement désorientée, tandis que les auteurs, tirant avantage de la situation, l'ont agressé(e) sexuellement. L'autorité chargée de l'enquête a saisi et analysé les images de la caméra de surveillance installée dans le car, ce qui a permis d'établir l'identité des auteurs. Les enquêteurs ont également analysé des données publiques, des photos et des relations sur Facebook, conformément à l'article 32 (a) la Convention.
- Dans la deuxième affaire, l'accusé avait étouffé sa mère avec un oreiller au domicile de cette dernière, avait emballé le corps dans une couverture, l'avait tiré hors du domicile et jeté dans une fosse septique située dans le jardin derrière la maison. L'autorité chargée de l'enquête a saisi le téléphone iPhone V et la montre connectée iWatch3 de l'accusé. Pour que l'enquête puisse aboutir, il était nécessaire d'obtenir les données stockées par un fournisseur de services basés aux États-Unis (Apple Inc.). Durant les interrogatoires, l'autorité chargée de l'enquête a demandé le consentement de l'accusé pour accéder aux données de son compte à distance, puisque celles-ci étaient stockées en dehors de la Hongrie. L'accusé y a consenti, s'est connecté à son compte et a donné le mot de passe aux autorités. Pour cette affaire, la Hongrie a relevé que sans la possibilité prévue à

l'article 32 (b) de la Convention de Budapest, les données n'auraient pu être obtenues que via une procédure d'entraide judiciaire très longue.

Plus généralement, la Hongrie a observé que sans le recours à la Convention de Budapest, il fallait envoyer une demande d'entraide aux fournisseurs de service dans le cadre de la coopération judiciaire pour accéder à des données stockées sur un serveur situé dans un autre pays. Cette procédure est longue et administrativement lourde, en particulier pour des données stockées sur le territoire américain. Avec le consentement volontaire, les données stockées à l'étranger sont accessibles, peuvent être enregistrées par les autorités chargées de l'enquête et deviennent donc un élément de preuve.

► Au **Japon**, de multiples accusés géraient un site dit sangsue qui recueillait des liens vers des sites internet contenant des données de manga et autres ouvrages qui avaient été téléchargées illégalement. Les accusés ont été condamnés pour violation de la Loi sur la propriété intellectuelle. Dans une autre affaire, l'accusé avait créé un programme de minage et l'avait téléchargé sur Internet en le faisant passer pour un programme de jeu en ligne. L'accusé était récompensé chaque fois que le programme était installé sur l'appareil d'un internaute qui le téléchargeait sans savoir qu'en fait, il s'agissait d'un programme de minage. Le parquet a obtenu des preuves en recourant aux dispositions relatives à la perquisition et à la saisie et extraction de preuves sur des ordinateurs saisis. L'accusé a été condamné pour utilisation d'un enregistrement électromagnétique exécutant une commande non autorisée.

► La République de Moldova a adopté son Loi sur la cybercriminalité 20/2009, ce qui lui a permis de devenir partie cette année-là. La loi a été appliquée dans de nombreuses affaires, parmi lesquelles:

- Dans une affaire, l'accusé est allé à l'étranger pour se procurer un skimmer afin d'obtenir illégalement des informations des cartes de paiement. L'accusé a été condamné pour être l'initiateur d'une tentative de rendre disponibles les moyens dans le but de commettre l'infraction prévue aux articles 259, 26, 42 para. (2), 259 para. (2) lit. b) et e) du Code pénal de la République de Moldova, et pour être l'auteur de la préparation de l'accès illégal aux données informatiques, infraction commise par deux ou plusieurs personnes a l'aide des moyens techniques.
- Dans une autre affaire, l'accusé est entré sur le territoire de la République de Moldova pour installer à Chisinau, avec l'aide d'autres personnes, des skimmers aux guichets automatiques (MTA) ayant pour but l'accès illégal et le vol des renseignements des cartes de paiement. Ces actes constituent des infractions pénales en vertu des articles 237 et 259 du Code pénale.

► En **Roumanie**, la cybercriminalité a évolué au cours des 17 dernières années, passant d'infractions commises à titre individuel par des criminels pointus en informatique à un modus operandi plus sophistiqué où interviennent des groupes criminels organisés qui commettent des fraudes sous diverses formes sur internet ou se livrent à des activités illégales en lien avec des instruments de paiement électronique.

- Une décision de la Haute Cour de Cassation de justice, rendue en 2013, a conclu que l'article 6 de la Convention de Budapest (« Utilisation abusive de dispositif ») est applicable lorsqu'un lorsque l'auteur d'une infraction monte un dispositif de lecture/écriture sur un DAB dans le but de collecter des informations sensibles à partir d'un instrument de paiement électronique. La décision a également conclu que l'utilisation illégale sur un DAB

d'un instrument légitime ou contrefait de paiement électronique dans le but de retirer des espèces est incriminée en vertu de l'article 2 (Accès illégal) en conjonction avec les dispositions spéciales sur les opérations frauduleuses avec des instruments de paiement électronique. De plus, la Roumanie a été victime de diverses attaques contre des systèmes ou réseaux informatiques visant le système financier qui ont pris la forme de différents montages de « jackpots », incriminés en vertu de dispositions législatives nationales qui appliquent les dispositions de la Convention de Budapest. En 2016, dans une affaire, un programme de "jackpot" qui avait compromis plus d'une vingtaine de DAB en moins de 90 minutes avait permis des retraits frauduleux à hauteur de 800 000 euros. Un des accusés a été pris la main dans le sac avec 17 000 euros d'espèces qu'il avait retirées et condamné à quatre ans de prison pour fraude informatique (article 8 de la Convention de Budapest) et participation à un groupe criminel organisé. Malheureusement, la complexité du montage qui prévoyait le déploiement d'une attaque de phishing ayant compromis la messagerie d'un fonctionnaire, l'intrusion (article 2 de la Convention de Budapest) et les altérations faites au fichier système des DAB qui ont permis de contourner les commandes des systèmes (articles 4 et 5 de la Convention de Budapest) n'ont pas été sanctionnées.

► L'**Espagne** a cité quelques exemples dans lesquels la Convention elle-même a été mentionnée dans des affaires espagnoles entre 2015 et 2019:

- Dans de nombreuses affaires entre 2015 et 2019, la Convention de Budapest (mais aussi la Convention de Lanzarote) ont été citées pour l'incrimination de pornographie enfantine et d'infractions de cyber-séduction à l'encontre d'enfants. Elles ont également été utilisées pour identifier les faits nécessaires à la preuve d'infractions de pornographie enfantine ou pour définir les concepts de pornographie enfantine et de matériel pornographique. D'autres jugements ont cité les Conventions de Budapest et de Lanzarote ainsi que leurs rapports explicatifs respectifs pour évaluer le crime de possession de pornographie enfantine et pour interpréter ce qui constitue du matériel à caractère pornographique ou un comportement sexuellement explicite.
- Dans une affaire impliquant l'accès illégal à des systèmes informatiques, un jugement de 2015 s'est appuyé sur la Convention de Budapest pour interpréter et appliquer la définition de l'incrimination d'accès illégal à des systèmes informatiques. Cette affaire a été tranchée avant que la disposition pénale espagnole pertinente n'ait été amendée. La décision analyse donc ainsi le concept pré-amendement par rapport à l'article de la Convention.
- Et dans des affaires impliquant des atteintes à l'intégrité de données et de systèmes, deux arrêts se sont appuyés sur la Convention de Budapest. Dans le premier, le tribunal qui a condamné l'auteur de dommages informatiques a cité expressément l'article 1 de la Convention pour définir le concept. Dans le second, toujours pour des poursuites liées à des dommages informatiques, la cour a cité les articles 2 à 6 de la Convention de Budapest dans son interprétation des articles pertinents du Code pénal espagnol.
- Enfin, dans une affaire impliquant le retrait physique d'équipement informatique, un arrêt de 2015 de la Cour provinciale de Madrid a fait référence au concept de données informatiques visées à l'article 1 de la Convention de Budapest.

L'Espagne a en outre indiqué que la conservation rapide de données stockées sur un système informatique conformément à l'article 16 de la Convention (du reste prévu en droit espagnol) sert très fréquemment dans pratiquement toutes les enquêtes liées aux technologies, que ce soit lorsque l'information qui doit être conservée est détenue par des fournisseurs nationaux ou à l'étranger. L'Espagne a également proposé un exemple d'utilisation de plusieurs outils de procédure pénale prévus dans la Convention de Budapest. En juin 2019, une plainte a été déposée par le Bureau du Procureur après l'enquête concernant une attaque informatique avec

accès au réseau interne d'une importante institution espagnole, qui a eu des conséquences sur les systèmes et appareils situés dans différents endroits en Espagne et dans d'autres pays. La plainte du procureur général visait l'accès illégal à des systèmes et l'atteinte à des ordinateurs (sur la base des articles du Code espagnol qui dérivent de la Convention de Budapest). Cette enquête en cours implique de nombreuses actions transnationales et l'utilisation des outils d'enquête prévus par la Convention de Budapest concernant la conservation de données, les injonctions de produire ainsi que la perquisition et la saisie de dispositifs informatiques.

3 Coopération internationale

En ce qui concerne la coopération internationale, les avantages que procure la Convention de Budapest sont issues de plusieurs sources:

Coopération internationale

Art. 23 – Principes généraux
Art. 24 – Extradition
Art. 25 – Principes généraux relatifs à l'entraide
Art. 26 – Information spontanée
Art. 27 – Entraide en l'absence d'accords internationaux
Art. 28 – Confidentialité
Art. 29 – Conservation rapide de données
Art. 30 – Divulgation partielle de données relatives au trafic
Art. 31 – Entraide concernant l'accès aux données
Art. 32 – Accès transfrontière
Art. 33 – Entraide pour la collecte en temps réel de données relatives au trafic
Art. 34 – Entraide en matière d'interception de contenu
Art. 35 – Réseau 24/7

- le fait qu'elle représente un cadre juridique pour la coopération en matière de justice pénale concernant la cybercriminalité et toute autre infraction dont les preuves sont sur informatique. La section sur la coopération internationale contient des dispositions générales sur la coopération internationale qui peuvent également se trouver dans d'autres traités sur la coopération en matière pénale, ainsi que des dispositions qui sont spécifiques au recueil et à la collecte de preuves électroniques. Le deuxième protocole additionnel qui est actuellement en cours de négociation devrait fournir des outils supplémentaires, notamment pour la coopération en situation d'urgence;

- le réseau étendu de praticiens participant au Comité de la Convention sur la cybercriminalité (T-CY) et aux activités de consolidation des capacités - les membres peuvent faire appel aux autres membres et s'appuyer les uns les autres en tant que de besoin dans l'enquête et les poursuites liées à des affaires de cybercriminalité que le plus souvent sont de nature transnationale. Cet avantage n'a pas de prix;

- la promotion des réformes et le renforcement des lois, procédures et mécanismes pour la coopération internationale par le T-CY et ses activités de consolidation des capacités. Par exemple, en 2014, il a été procédé à une évaluation du fonctionnement des dispositions relatives à l'entraide judiciaire contenues dans la Convention de Budapest, et un ensemble de recommandations a été adopté. En 2017, le Comité a alors passé en revue les suites données par les Parties à ces recommandations et analysé les bonnes pratiques, mais a aussi encouragé à poursuivre les efforts.

On trouvera ci-après des exemples communiqués par les Parties qui illustrent comment la Convention de Budapest apporte une aide concrète.

3.1 Exemples d'entraide dans la pratique

Tous les Etats reconnaissent l'efficacité limitée de l'entraide judiciaire et la nécessité d'améliorer le processus lorsqu'il s'agit d'enquêter sur des cyberdélits transnationaux et de sécuriser des preuves électroniques volatiles. Même si la Convention n'a pas résolu tous les problèmes, elle a contribué à améliorer la situation et à mettre en place une coopération efficace. L'une des Parties a relevé que, en tant que petit pays pauvre, elle ne pouvait tout simplement pas trouver les ressources pour négocier tous les accords bilatéraux dont elle aurait besoin pour obtenir rapidement des données électroniques auprès de tous les pays à qui elle pourrait demander de l'assistance. Cependant, une fois qu'elle a adhéré à la Convention, des douzaines de pays partenaires étaient immédiatement tenues de lui apporter assistance. Cette perspective de relations immédiates permettant d'obtenir une assistance nécessaire a été un facteur crucial dans la décision de ce pays d'adhérer à la Convention. Une autre partie, Malte, a ajouté qu'étant donné que la majorité des attaques liées à la cybercriminalité sont par nature transnationales, la Convention de Budapest est indispensable pour enquêter efficacement sur les auteurs de ces attaques, en particulier pour des pays comme Malte, qui n'ont pas de fournisseurs de services internationaux dans leur propre juridiction.

Dans la même veine, de nombreuses Parties ont décrit les améliorations apportées à leur capacité à obtenir une entraide formelle et informelle après l'adhésion à la Convention, et ont fourni des statistiques[1] et des exemples dans ce sens.

- La **Bosnie-Herzégovine** a déclaré que le meilleur exemple de coopération internationale se trouve dans les plates-formes des fournisseurs de services créées spécifiquement pour cela – par exemple, celle de Facebook. Ces plates-formes, qui servent aux représentants des services répressifs, permettent d'échanger extrêmement rapidement des informations opérationnelles. Ainsi, dans des enquêtes sur l'utilisation illégale de droits de propriété intellectuelle et la mise en danger d'un fonctionnaire impliqué dans des affaires de sécurité, le Bureau du Procureur de la Bosnie-Herzégovine s'est servi des dispositions de la Convention lorsqu'il a demandé à des fournisseurs de services étrangers la conservation des données et la divulgation de données liées aux abonnés.
  La plupart des Bureaux des Procureurs de la Bosnie-Herzégovine ont signalé qu'ils avaient enquêté ou étaient en train d'enquêter sur des affaires qui impliquaient des crimes visés par la Convention. En tout, en 2019, environ 110 enquêtes de cette nature ont été entamées, dont bon nombre ont abouti à des poursuites. De plus, en 2019, le ministère de l'intérieur de la Republika Srpska a signalé 115 crimes liés à la high-tech, dont 12 impliquant des crimes contre la sécurité des données informatiques et 103 d'autres crimes liés à la high-tech.

[1] Il convient de noter que les statistiques concernant l'utilisation des incriminations et outils prévus par la Convention de Budapest ne sont pas complètes ou entièrement fiables – en fait, on peut penser qu'elles sous-estiment de manière chronique l'utilisation réelle. Certains pays ne tiennent pas de statistiques; des pays à structure fédérale peuvent tenir des statistiques distinctes, qu'il n'est pas possible d'extraire; de nombreux pays ne tiennent pas des statistiques d'une manière qui suit les infractions matérielles prévues par la Convention (ils utiliseront par exemple un terme générique tel que « fraude » plutôt qu'une référence légale faisant le lien avec la Convention de Budapest; enfin, les pays tiennent normalement des statistiques par catégorie infractionnelle, et non par l'utilisation ou non de certains outils procéduraux dans une enquête. En partie pour les mêmes raisons, les statistiques concernant le système 24/7 (analysé plus bas), sous-estiment également le recours à ce mécanisme. A contrario, lorsqu'il existe des statistiques, elles mélangent parfois des demandes qui recourent à des mécanismes ou réseaux différents (par exemple le réseau G7) et pas uniquement au réseau 24/7 prévu par la Convention de Budapest.

La coopération policière internationale via INTERPOL à Sarajevo est très intense pour ce qui est de l'échange de données concernant la pornographie enfantine (en vertu de l'article 9 de la Convention) et la disruption de ses chaînes de distribution. En 2019, INTERPOL à Sarajevo a ouvert 30 nouvelles affaires liées à la pornographie enfantine. Cinq venaient des services répressifs nationaux, et 25 autres ont été ouvertes à la demande des bureaux des contacts nationaux dans d'autres pays.
Le ministère de l'Intérieur de la Republika Srpska a collaboré à plusieurs opérations internationales en 2015 et 2016, notamment Darkode (avec les États-Unis: production et utilisation d'un virus informatique et fraude informatique); Odisej (avec l'Allemagne: fraude informatique, accès non autorisé à un ordinateur, réseau informatique, réseau de télécommunications et traitement de données électroniques etc.); et PLEJADE avec le Royaume-Uni, les États-Unis, la Suisse, l'Autriche, l'Allemagne, le Japon, le Canada, l'Irlande et Monaco: extorsion et blocage ou limitation de l'accès à un réseau informatique public.

► La **France** envoie ou reçoit de nombreuses demandes d'assistance pour obtenir des données électroniques. Ces demandes reposent soit sur des instruments bilatéraux, en particulier l'accord avec les États-Unis, soit sur des instruments multilatéraux, y compris l'accord entre l'Union européenne et les États-Unis et la Convention de Budapest. La France relève que les dispositions de la Convention de Budapest (en particulier les articles 29 et 35) et sa communauté de personnes de confiance sont particulièrement importantes pour la conservation de données avant des demandes formelles.
Dans un exemple de 2018 impliquant l'enlèvement et le meurtre d'un mineur ainsi que des infractions associées, la France avait fait une demande pour récupérer des données électroniques. L'État requis a répondu que sa norme en matière de preuve n'avait pas été respectée et a refusé de donner suite à la demande. Toutefois, une demande d'entraide judiciaire formelle été transmise à l'État requis, et a été exécutée en 2018
Dans une demande entrante de 2018 concernant une enquête sur une personne morale pour un ensemble de cyber-infractions, notamment pour les chefs de conspiration et de fraude électronique (vente d'outils et de programmes pour désactiver des programmes antivirus), la France s'est vue demander de conserver les données sur un compte ainsi que des données liées à une adresse IP. Cette demande a été exécuté en juin 2019.
En 2019, la France a envoyé 55 demandes d'entraide judiciaire émanant de services français pour des données électroniques, toutes ces demandes se fondant sur la Convention, et a traité 20 demandes entrantes de cette nature.

► La **Géorgie** n'a qu'un tout petit nombre d'accords d'entraide avec des pays en-dehors de l'Europe. En l'absence d'accord, la Convention de Budapest s'est révélée un outil important pour la Géorgie s'agissant de traiter avec des partenaires européens dans des enquêtes multinationales graves. Dans plusieurs affaires, du fait des informations spontanées partagées sur la base de l'article 26 de la Convention, le nombre d'enquêtes géorgiennes ayant abouti a atteint un niveau sans précédent. Elle cite deux exemples:

- Affaire du maliciel GozNym.en 2019, la Géorgie a participé à une opération multinationale à grande échelle de services répressifs qui a permis de démanteler un réseau organisé de cybercriminalité complexe et opérant au niveau mondial. Le réseau criminel avait utilisé le maliciel GozNym pour voler à 41 1000 victimes - essentiellement des entreprises et leurs institutions financières - quelque 100 000 000 de dollars. Le réseau criminel dirigé par un ressortissant géorgien était composé de membres venant pour l'essentiel d'Europe de l'Est.
- L'opération a culminé par le déclenchement de poursuites pénales à l'encontre des membres du réseau dans quatre pays différents, à la suite de la coopération entre la

Géorgie, les Etats-Unis, l'Ukraine, la République de Moldova, l'Allemagne, la Bulgarie, Europol et Eurojust. La Géorgie a poursuivi avec succès le dirigeant du syndicat criminel et son associé qui ont été condamné à sept ans et cinq ans de prison respectivement. Le ministère public géorgien s'est appuyé fortement sur les preuves partagées par les partenaires internationaux de l'opération. Pour plus d'informations, vous pouvez suivre les liens ici, ici, ici et ici.

- Affaire de pornographie enfantine internationale. En 2019, la police géorgienne a arrêté des ressortissants australiens, géorgiens et américains sur des accusations d'exploitation sexuelle des enfants et de pornographie enfantine. Dans l'opération de police multinationale, les services répressifs sont démantelé un réseau de trafic d'enfants qui exploitait des fillettes parfois d'à peine huit ans pour produire du matériel pornographique ensuite commercialisé à la fois localement et au niveau international, essentiellement via le Dark Web. L'opération de police a été précédée d'une coopération intensive entre les autorités géorgiennes, australiennes et américaines, ainsi qu'avec Europol. Trois des personnes arrêtées ont été condamnées par un tribunal géorgien à 19 ans de prison chacune, le procès est en cours pour 21 autres.

► La **Hongrie** a fourni plusieurs exemples d'améliorations de l'assistance mutuelle et a indiqué que le fait d'utiliser la Convention pour ce faire aboutit à une procédure rapide, plus professionnelle et plus directe que l'entraide judiciaire entre autorités judiciaires. Les suivants exemples ont été cités:

- Dans une affaire liée au terrorisme, la Hongrie a appris que la personne objet de l'enquête avait des serveurs fonctionnant aussi dans une autre Partie à la Convention. Elle a donc demandé à celle-ci une assistance via le réseau 24/7. La Hongrie a également utilisé l'accès transfrontière à des données stockées sur informatique en vertu de l'article 32 de la Convention, étant donné que le suspect utilisait un serveur privé virtuel physiquement situé dans la Partie requise.
  Dans la deuxième affaire, le sujet non identifié changeait régulièrement et illégalement le blocage d'identité de l'abonné sur des iPhone 6 commercialisés par la société X à prix soldé si un acheteur achetait un nouveau contrat de téléphone. À la demande d'acheteurs de téléphones, le sujet débloquait les téléphones, ce qui permettait aux acheteurs de les utiliser avec n'importe quel fournisseur de réseau ou de les revendre à un prix plus élevé que le prix d'achat d'origine. Le changement légal du blocage de la carte SIM peut être initié par la société X d'Apple Inc. via un programme installé sur les ordinateurs de la société X. Le sujet de l'enquête avait infecté les ordinateurs de la société X avec un cheval de Troie qui lui permettait d'utiliser le programme au moyen d'un serveur à distance. Ainsi, le sujet avait un accès illégal aux programmes qui seraient ensuite utilisés légalement par la compagnie X pour débloquer les téléphones. L'auteur de l'infraction a débloqué 707 téléphones mobiles et a été poursuivi pour intrusion dans un système d'information et dans un grand volume de données. Conformément à l'article 29 de la Convention, l'autorité hongroise d'enquête a demandé au département de la justice américain de conserver les données informatiques stockées concernant les demandes de déblocage de cartes SIM envoyées par la société X à Apple. Une demande d'entraide judiciaire, basée en partie sur les articles 4, 23, 25, 29 et 31 de la Convention et en partie sur un traité bilatéral d'entraide judiciaire, a ensuite été envoyée aux autorités américaines pour obtenir la divulgation des données conservées par Apple. Ces données étaient nécessaires pour établir les faits d'espèce et identifier les utilisateurs finaux des téléphones débloqués, et donc aider à identifier le ou les suspects.
- Dans son dernier exemple, la Hongrie a demandé aux autorités ukrainiennes la divulgation de données dans une affaire concernant l'atteinte à l'intégrité de données et de systèmes

d'information. Le dirigeant d'une société avait signalé à la police qu'un inconnu avait accédé illégalement au serveur téléphonique de la société et passé un très grand nombre d'appels aux Seychelles et en Guinée-Bissau, entre autres, ce qui avait occasionné une perte de 7 500 000 HUF. L'inconnu utilisait un numéro de téléphone de la société après l'avoir appelé à partir d'un numéro ukrainien. Les autorités Ukrainiennes ont répondu à la demande.

► L'**Italie** a communiqué un exemple concret de coopération internationale:

Le 14 juin 2013, le bureau de contact italien a reçu une demande urgente de coopération de son homologue norvégien. L'Italie a été informée qu'un ressortissant afghan résidant en Norvège avait poignardé à mort sa femme deux jours avant. L'homme avait ensuite pris la fuite avec sa fille de deux ans et était arrivé en Italie, selon les informations entrées dans le Système d'Information Schengen SIRENE par les autorités norvégiennes. Ces dernières avaient donné des signes physiques distinctifs et une description du suspect.
L'analyse des connections Skype et du numéro de téléphone mobile fournis par la police norvégienne a révélé deux adresses IP italiennes. Dans l'intervalle, le Bureau du Procureur avait obtenu une injonction pour un traçage en temps réel et un positionnement en vue de géolocaliser l'appareil.
En conséquence, entre la nuit du 15 juin et le lendemain matin, le téléphone mobile a été géolocalisé dans un secteur précis de Rome. Dans ce secteur, le 16 juin, des officiers de police italien ont repéré un jeune homme en compagnie d'une petite fille dont l'âge correspondait à celui de la fillette tel qu'il avait été signalé par la police norvégienne.
Les officiers de police italien ont examiné des effets personnels saisis du suspect, procédé à des contrôles et été en mesure de s'assurer de l'identité de l'homme qui a ensuite été arrêté. Des photos de la personne arrêtée et de l'enfant ont été envoyées aux autorités norvégiennes, qui ont confirmé les identités.
Le sujet a été extradé et l'enfant ramenée en Norvège, où un programme pour sa protection avait été mis en place et des parents étaient venus l'accueillir et l'héberger.

► Le **Panama** a signalé qu'il a été en mesure d'obtenir le soutien en janvier 2020 de services d'autres pays tels que la NCA britannique, pour l'investigation dans une affaire de DDoS.

► En **Roumanie**, le service roumain le plus pertinent pour la coopération internationale en matière de cybercriminalité – le Service de lutte contre la cybercriminalité, relevant de la Direction d'enquête sur la criminalité organisée et le terrorisme (DIICOT) – qui est également le Point de contact 24/7 pour le réseau instauré par l'article 35 de la Convention, a signalé pour 2019 144 demandes entrantes de conservation de données stockées sur informatique et 39 demandes sortantes, ainsi que 407 demandes d'entraide juridique dans des affaires de cybercriminalité (321 demandes actives et 86 passives). Outre ces demandes d'assistance et d'entraide, les procureurs du Service de lutte contre la cybercriminalité ont démarré 3 équipes communes d'enquête auxquelles ils ont participé.

► En **Serbie,**

- le Bureau du Procureur spécial serbe pour la criminalité high-tech et le service correspondant du ministère de l'Intérieur mènent depuis 2011 une opération, encore en cours aujourd'hui, baptisée « Armageddon », concernant les abus sexuels d'enfants sur Internet. Conformément à la Convention de Lanzarote, ces affaires sont considérées comme urgentes. Dans la plupart d'entre elles, la coopération internationale est utilisée pour recueillir des preuves.

La Serbie a souligné que, dans l'affaire suivante, elle a reçu une entraide efficace et efficiente : non seulement toutes les preuves demandées ont été réunies rapidement, mais l'officier de liaison hongrois en Serbie a personnellement apporté les preuves au procureur serbe.

Dans cette affaire, des procédures préliminaires avaient été entamées sur la base d'informations provenant de l'autorité hongroise et reçues via Interpol. Les autorités hongroises avaient reçu une plainte pénale de la part d'une victime mineure qui avait été en communication avec une personne inconnue sur un réseau social enregistré en Hongrie. Après avoir gagné la confiance de la victime, le suspect visé par l'enquête l'avait menacée et forcée à lui envoyer des photos d'elle nue et se livrant à des activités sexuelles devant la caméra.

Les autorités hongroises ont envoyé à la Serbie les registres de connexion de l'IP pour les comptes que l'accusé avait utilisés sur le réseau social, qui appartenaient à un fournisseur serbe de services sur Internet. Le Bureau spécial du Procureur a obtenu une injonction du tribunal et localisé la communication. Il a ensuite obtenu un mandat de perquisition, et l'intervention d'un expert a permis de mettre à jour des preuves du crime sur des dispositifs électroniques appartenant à l'accusé, qui avaient été saisis par la police.

Simultanément, le Bureau spécial du Procureur a soumis une demande d'entraide et a reçu du bureau du procureur compétent en Hongrie des déclarations de la victime et d'autres autres témoins ainsi que des copies des communications électroniques de la victime.

La mise en accusation a fait valoir que l'accusé, à de nombreuses reprises sur une période de deux ans, avait utilisé la victime mineure pour produire des photographies pornographiques et du contenu audiovisuel. Il avait menacé de poster sur l'Internet des photos de la victime en maillot de bain, sans vêtements ainsi que les matériels vidéo susmentionnés. Ces menaces et ordres étaient envoyés via un réseau social et Skype. L'accusé conservait toutes les photos et le matériel vidéo sur son ordinateur.

L'accusé a été condamné au chef des délits d'affichage, obtention et possession de matériel pornographique et de pornographie enfantine, ainsi que de coercition, et condamné à une peine de prison.

- Dans une autre affaire, au printemps 2020, la Serbie – avec l'Autriche, la Bulgarie, l'Allemagne et avec le soutien d'Eurojust – a participé à des opérations qui ont donné de bons résultats contre deux groupes criminels organisés suspectés de fraude aux investissements à grande échelle dans des opérations boursières sur Internet. Au cours d'une journée d'action, menée le 2 avril 2020, quatre suspects ont été arrêtés en Bulgarie. En Allemagne, 2,5 millions d'euros ont été gelés sur le compte bancaire de sociétés impliquées dans le montage frauduleux. Les autorités serbes ont arrêté cinq suspects et perquisitionné neuf endroits, ce qui a permis de saisir cinq appartements, trois voitures, un montant d'espèces considérable et de l'équipement informatique. En outre, plus d'une trentaine de comptes bancaires ont été mis sous surveillance. Sur la base des informations rassemblées durant cette journée d'action, les autorités ont engagé une autre opération contre une société à Belgrade le 4 avril, au cours de laquelle elles ont arrêté un suspect et saisi des serveurs, d'autres matériels informatiques et des documents. Dans cette affaire, les autorités serbes, entre autres, ont recouru à l'article 26 de la Convention de Budapest (information spontanée) pour partager des informations avec d'autres partenaires.

► La **Slovaquie** demande souvent une entraide sur la base juridique de la Convention. Les articles 23, 25 et 31 de la Convention sont ceux qui sont le plus souvent invoqués (en plus de l'article 29 pour la conservation). Les demandes sortantes portent sur diverses formes de preuves, concernant notamment des données sur l'abonné, le trafic et le contenu. La majorité des

demandes slovaques sont envoyées aux grands fournisseurs américains (tels que Microsoft, Google, Facebook et Instagram) ainsi qu'à d'autres prestataires de services majeurs voire plus petits.

► La majorité des demandes adressées à l'**Espagne** concernent des données de transactions et, dans une moindre mesure, les données de contenu. La très grande majorité des demandes proviennent des États-Unis. La demande la plus récente provenant de ce pays décrivait un montage de botnet dans lequel différents pays et entreprises étaient concernés. La demande visait, entre autres mesures, les données de transaction liées à une adresse IP associée à la société responsable du botnet.

► Le **Sri Lanka** a signalé auparavant qu'il avait déjà envoyé 37 demandes internationales et reçu des réponses à 30 d'entre elles. Il a été en mesure d'identifier plusieurs numéros de téléphone utilisés pour créer de faux comptes Facebook, qui ont fait aboutir des enquêtes pénales.
En avril 2019, le Sri Lanka a été confronté à de graves attaques terroristes (les « attentats à la bombe de Pâques au Sri Lanka ») durant lesquels plus de 250 personnes ont été tuées et des centaines blessées. Face à cette urgence nationale, des preuves électroniques ont été demandées immédiatement à toute une série de fournisseurs de services. Un certain nombre de pays ont fourni immédiatement une assistance internationale, dont des Etats Parties à la Convention, et le Sri Lanka été en mesure de réunir des preuves électroniques, notamment des détails de comptes, de correspondances et des contenus dans certains cas. Des preuves électroniques ont été en outre obtenues au moyen d'enquêtes communes, basées sur les amendements législatifs introduits depuis que le pays est devenu Partie à la Convention de Budapest. Dans de nombreux cas, des informations spontanées ont été partagées entre services répressifs localement en vertu de l'article 26 de la Convention.

► La plupart des demandes **suisses** sortantes concernant la cybercriminalité sont adressées aux États-Unis pour obtenir des informations de Facebook, Google et d'autres services fournisseurs américains de services sur Internet. Ces deux dernières années, le nombre de demandes adressées à la Turquie, au Ghana et à des pays non-Parties – Hong Kong et le Nigéria – a augmenté. De manière générale, les demandes suisses concernent l'identification de suspects par la divulgation de données de trafic. L'interception de données de contenu n'est pas souvent demandée – elle est demandée uniquement dans des enquêtes complexes qui s'accompagnent d'autres mesures de surveillance technique en Suisse et/ou dans des pays tiers. Les fraudes informatiques, tels que les fraudes à la romance, l'extorsion par demande de rançon, la pornographie enfantine et d'autres actes criminels de ce type concernent essentiellement les enquêtes suisses. La Suisse déclare qu'elle utilise fréquemment l'accès transfrontière en vertu de l'article 32.
La Suisse a indiqué que la disposition de la Convention de Budapest la plus utilisée est son article 29, qui concerne les demandes de conservation de données, et indiqué qu'elle ne reçoit quasiment pas de demandes d'entraide judiciaire sans une demande préalable de conservation article 29. La Suisse constate actuellement une augmentation des demandes entrantes d'entraide mutuelle portant en général sur des données liées au trafic. Étant donné que plusieurs fournisseurs en Suisse offrent des services de communication cryptée et que ceux-ci peuvent être utilisés de manière abusive par des criminels, le nombre de demandes entrantes liées à ce domaine ne cesse d'augmenter. Le négoce de cryptoactifs proposés par des fournisseurs de Suisse est également un des principaux facteurs dans les demandes d'entraide judiciaire.

► La **Turquie** a fourni plusieurs exemples:

- Dans la première affaire citée par ce pays, le Système de notification en ligne de la police nationale turque a reçu un avertissement prévenant qu'il allait y avoir un attentat à la bombe dans une ville du sud du pays. Le système capture automatiquement l'IP source, qui menait à une société de communication américaine. Après que la Turquie eut téléphoné et envoyé un courriel à la société, celle-ci a indiqué que l'IP était attribué à une société de croisière américaine. Celle-ci a déterminé que l'IP concernait un de ses navires, qui se trouvait à ce moment-là dans un autre pays. L'équipage à bord du bateau a vérifié la caméra de sécurité et les enregistrements et repéré le suspect, un Turc. Après avoir commencé par refuser de parler, celui-ci a admis qu'il avait envoyé l'avertissement alors qu'il était pris de boisson. Il a été licencié, son visa a été annulé et il a été arrêté à l'aéroport à son retour en Turquie.
- Dans une autre affaire, la Turquie a reçu des informations sur un possible attentat de l'E.I. en Turquie et a obtenu des informations sur l'abonné pour empêcher l'attentat.
- Dans son dernier exemple, la Turquie a reçu d'une source une capture d'écran avec une conversation entre deux terroristes du PKK disant qu'ils étaient à Paris et qu'ils envisageaient de faire exploser une bombe à l'aéroport de Schiphol le lendemain. La Turquie a fait passer cet avertissement aux autorités des Pays-Bas afin qu'ils puissent prendre leurs précautions.

3.2 Utilisation des points de contact 24/7

Les Parties utilisent largement le réseau 24/7 et ont donné à l'appui des statistiques et des exemples.

► La **Belgique** a reçu en 2019 10 demandes émanant des Pays-Bas, des États-Unis, de la Lettonie, de la France et de la Suisse et en a envoyé 27 à 12 parties différentes, à savoir le Canada, la France, l'Allemagne, la Hongrie, la Lettonie, les Pays-Bas, la Pologne, la Suisse, la Turquie, l'Ukraine, le Royaume-Uni et les Etats-Unis.

► Le point de contact 24/7 en **Bosnie-Herzégovine** a envoyé essentiellement des demandes de conservation de données de comptes de messagerie à des prestataires de services sur Internet dans d'autres pays; il a parfois obtenu des données sur l'abonné. La plupart des demandes ont été adressée au point de contact 24/7 des États-Unis et cela peut être caractérisé comme étant une coopération exemplaire. La coopération a également été établie avec les points de contact en Allemagne, France, Pays-Bas, Lettonie etc. et dans des pays non-Parties. Le Bureau du Procureur de Bosnie-Herzégovine a envoyé au moins trois demandes de conservation de données en vertu de l'article 29 de la Convention dans le cadre d'enquêtes sur des faits de chantage, atteinte ou accès non autorisé à des données et programmes informatisés, fraude informatique, exploitation des enfants, usage non autorisée de droits de propriété intellectuelle et autres types d'affaires.

Dans une des affaires citées en exemple, le Bureau du Procureur du District de Brčko a fait une demande de conservation pour des données liées à une certaine adresse IP via le point de contact 24/7. Le destinataire de la demande a répondu que cela concernait un réseau privé virtuel (VPN) et a fourni des informations sur le service et le fournisseur de services. Il n'a pas été possible de geler les données, mais l'identité de la cible a été déterminée sur la base des informations qui avaient été divulguées.

En 2019, 21 demandes ont été introduites par des institutions nationales et 3 par d'autres points de contact sur la cybercriminalité. 86 affaires de cybercriminalité ont été ouvertes par le biais des canaux d'Interpol demande d'institutions nationales et 21 sur demande de bureaux de contact nationaux étrangers.

► Le **Chili** a signalé qu'il a fait appel au réseau 24/9 19 fois dans les trois mois entre mi-octobre 2019 et fin janvier 2020 pour des demandes concernant trois pays.

► La **République tchèque** a résolu une affaire avec l'assistance du réseau 24 /7. Un psychologue tchèque a reçu plusieurs mails contenant des pensées suicidaires de la part d'une personne utilisant le portail seznam.cz. Les connexions de l'IP à la boîte de messagerie ont été obtenues. Dès que le fournisseur du service de messagerie (Deutsche Telekom) a été identifié, une coopération immédiate a été demandée via le point de contact allemand, qui a établi le point d'arrivée de l'utilisateur de l'adresse IP. L'utilisateur qui avait envoyé les messages électroniques était un ressortissant tchèque vivant en Allemagne.

► Entre 2016 et 2019, la **République dominicaine** a envoyé 34 demandes de conservation et 3 demandes au titre des réseaux 24/7 (Convention de Budapest, G7 et INTERPOL).

► La **France** utilise énormément le réseau 24/7 de la Convention de Budapest, non seulement pour des infractions liées à l'informatique mais pour toutes questions qui nécessitent des preuves électroniques. Elle a eu recours au réseau au moment des attentats contre Charlie Hebdo pour obtenir des informations sur des forums étrangers concernant la possibilité qu'il y ait de nouveaux attentats terroristes.
En pratique, les demandes visent une conservation en attendant une demande formelle d'entraide judiciaire. Au-delà de ce rôle essentiel pour la conservation des données, le point de contact peut donner les premiers conseils techniques ou juridiques au service d'où émane la demande. Il peut aussi transmettre des demandes d'assistance immédiate lorsque la sécurité physique d'une personne est en cause (enlèvement, menaces etc.).
En 2019, le point de contact français a traité 268 demandes liées à la Convention de Budapest, toutes pour la conservation de données, dont 130 demandes entrantes (provenant de 24 pays) et 138 demandes sortantes. Dans plusieurs affaires de terrorisme, cela a permis la conservation urgente de données essentielles.

► **Israël** a signalé quatre affaires significatives dans lesquelles il a été fait appel au réseau 24/7.

- Durant avril et mai 2019, trois demandes de gel de données et d'obtention d'informations à réaliser en temps réel concernant une fraude par compromission de la messagerie d'une société ont été reçues de la part de trois Parties européennes. Les adresses IP ont abouti à un suspect israélien. Durant l'enquête en temps réel, plusieurs téléphones cellulaires prépayés israéliens qui étaient utilisés pour commettre le crime ont été localisés. Plusieurs des personnes liées à ces affaires sont déjà connues pour fraude et compromission de messagerie commerciale. Après la localisation de cette base d'opération, les Parties européennes devraient envoyer les demandes d'entraide judiciaire concernant l'affaire afin d'ouvrir une enquête israélienne. Tout au long de la gestion en temps réel de ces événements, une connexion directe été ouverte entre le centre 24/7 d'Israël et les autres points de contact pour obtenir les informations supplémentaires nécessaires à la progression de l'enquête.
- Une demande de conservation a été reçue d'une Partie européenne concernant une adresse IP suspecte impliquée dans une tentative de pénétrer illégalement dans des systèmes gouvernementaux locaux de cette Partie. L'IP a abouti à un fournisseur de stockage israélien. Les activités d'enquête liées à ce fournisseur ont découvert un suspect, ressortissant d'un pays latino-américain. Une copie complète du serveur été faite, les informations ont été transmises au CERT national et en tant qu'informations contextuelles/pistes à des contreparties.

- Le service de la police nationale israélienne chargé de la criminalité économique et financière a reçu une communication concernant un suspect qui se serait livré à des menaces de mort et à des intimidations de témoins, via Telegram. Le service a apporté son aide dans cette situation d'urgence pour explorer toutes les pistes menant vers le suspect. Après avoir détecté des adresses suspectes d'IP aboutissant à des sociétés de communication dans cinq pays non-Parties en Asie du Sud, ainsi qu'à deux Parties dans les Etats d'Amérique et en Europe, des demandes d'urgence ont été faites à ces pays. Compte tenu de toutes les preuves, il apparaît que le suspect est sophistiqué et utilise des mesures de cryptage multiples (télégramme et VPN). En plus, des informations ont été reçus du pays d'Asie du Sud concernant le suspect, qui possède un compte lié au compte Telegram à partir duquel les messages menaçants avaient été envoyés.
- En septembre 2019, des commentaires menaçants visant le premier ministre et le Président d'Israël ont été postés sur le site Web d'information israélien à partir de différents profils. Les informations obtenues sur le site web d'actualité ont indiqué que deux des profils menaçants étaient liés à une seule adresse IP, qui aboutissait à une société de communication américaine. Une demande d'urgence a été adressée au point de contact 24/7 américain pour localiser immédiatement le suspect. Des enquêtes menées par des homologues, il est apparu que le suspect est un citoyen israélien résidant illégalement aux États-Unis. En conséquence, les États-Unis ont lancé la procédure d'extradition et le suspect sera arrêté à son arrivée à Israël.

► L'**Italie** a indiqué que le réseau 24/7 est essentiellement utilisé pour envoyer et recevoir des demandes de conservation de preuve électronique (journaux de connexion, enregistrement etc.). Dans de nombreuses affaires, le contact italien a également envoyé et reçu des demandes pour des informations de base concernant l'abonné qui peuvent être divulguées immédiatement entre polices, quand cela est possible.
En outre, l'Italie a constaté que le réseau s'est révélé utile pour transférer des informations et des alertes concernant des cyberattaques et des cybermenaces à l'encontre d'infrastructures critiques dans d'autres pays et pour fournir des indicateurs de compromission, s'ils sont disponibles.
En 2018, l'Italie a reçu 39 demandes entrantes et en a envoyé 69. 28 autres pays étaient concernés.

► Le **Luxembourg** est devenu Partie à la Convention en juillet 2014 et a instauré un point de contact 24/7. Celui-ci a traité 75 demandes depuis lors, dont 25 en 2019. Le Luxembourg signale que l'utilisation du réseau augmente très rapidement.

► Le **Panama** a signalé que, couvert par les articles 16 et 17 de la Convention de Budapest, il a réussi à aider des pays tels qu'Israël, la Suisse et l'Australie, par le biais de leurs points de contact.

► En 2019, la **Slovaquie** a envoyé 321 demandes de point de contact 24/7 à 13 parties, pour la plupart d'entre elles concernant les États-Unis (193), suivis de l'Allemagne (34), de la République tchèque (29) et du Royaume-Uni (14). Elle a reçu 380 demandes dont la majeure partie émanaient des États-Unis (164), suivies de la République tchèque (39), de l'Allemagne (22) et du Royaume-Uni (15).

► En février 2019, l'**Espagne** a reçu une demande du point de contact britannique pour la conservation du trafic NetFlow d'une adresse IP (ce protocole stocke des informations sur l'IP et le port source/destination à des fins statistiques et de gestion du réseau). Ces informations émanant d'un prestataire espagnol de services sur Internet étaient nécessaires pour une enquête

en cours. Elles n'ont jamais été utilisées en Espagne ; les opérateurs les stockent pour deux jours au maximum. Le point de contact espagnol a demandé les conservations tous les deux jours et est parvenu à obtenir que les données soient disponibles à la réception d'une demande d'entraide judiciaire.
En mai 2019, dans une enquête sur une intrusion dans un réseau privé en Espagne, le contact espagnol a envoyé une demande de conservation de contenu à un fournisseur de services situé en Israël. Le service s'est avéré être un serveur privé virtuel, et le point de contact non seulement a préservé les données mais a fourni les informations de base sur l'abonné, ce qui s'est révélé très utile pour poursuivre l'enquête.

- Ces quatre dernières années, la **Turquie** a reçu 43 demandes de conservation, dont 21 conservations ont été exécutées, cinq autres demandes étant encore en cours de traitement. Le reste a été refusé car les données n'étaient plus disponibles ou du fait de difficultés techniques – par exemple, du fait de l'utilisation de NAT (Network Address Translation).

- Entre janvier et septembre 2019, le **Royaume-Uni** a signalé 77 demandes entrantes de conservation émanant de 18 Parties et 169 demandes de conservation sortantes destinées à 27 Parties[2].

3.3 Améliorations à la coopération du secteur privé du fait de l'adhésion à la Convention

La plupart des Parties insistent sur le fait que deux pouvoirs leur procurent un avantage significatif : la capacité de demander directement la conservation à des fournisseurs américains (ou de faire en sorte que des fonctionnaires du gouvernement américain envoient rapidement les demandes de conservation en leur nom) et la capacité de demander directement des informations sur l'abonné à des fournisseurs américains. Ces deux pouvoirs ne sont pas liés uniquement à la Convention de Budapest. Toutefois, certains pays se sont montrés plus désireux d'y recourir, ou ont eu plus de succès avec les fournisseurs, depuis qu'ils sont devenus Parties à la Convention.

De plus, en mars 2017, le T-CY a adopté une Note d'orientation sur les injonctions de produire concernant des informations liées à l'abonné (article 18 Convention de Budapest) qui illustre comment l'article 18.1.b de la Convention peut servir de fondement juridique pour demander des informations sur l'abonné à un prestataire de services qui propose ses services sur le territoire d'une Partie.

La coopération avec des fournisseurs basés aux États-Unis est particulièrement importante pour les enquêtes menées par des pays autres que les Etats-Unis, étant donné que les données désirées sont souvent détenues aux Etats-Unis ou sous le contrôle de fournisseurs basés aux États-Unis. De nombreux pays sont conscients que, si les données demandées sont couvertes par le droit américain, le fournisseur peut librement divulguer certains types de ces données à des agences américaines sans qu'il soit nécessaire de demander une entraide judiciaire formelle. Les pays sont également conscients que, lorsque les plus gros fournisseurs américains décident de répondre ou non à ces demandes discrétionnaires, ils tiennent compte explicitement du fait que le pays demandeur est Partie ou non à la Convention.

C'est pourquoi la coopération transnationale – et pas uniquement nationale – avec le secteur privé est importante.

[2] Ces statistiques couvrent également les demandes via le réseau du G7.

- La **Bosnie-Herzégovine** a signalé qu'en général, ses services répressifs ont signé des accords de coopération avec les fournisseurs locaux de télécommunications, ce qui permet aux services répressifs d'accéder à certaines bases de données. Ces derniers organisent également et participent à des tables rondes, des ateliers des conférences où ils échangent des informations et des expériences avec des fournisseurs de télécommunications, des institutions financières et des sociétés de technologies de l'information.
  Le ministère de l'Intérieur de la Republika Srpska a signalé que la coopération avec le secteur privé national et international a grandement progressé grâce à la Convention. La plupart des sociétés ont établi des lignes de contact pour des représentants des services répressifs qui peuvent ainsi obtenir les informations nécessaires pour suite à donner.
  Dans une affaire impliquant l'utilisation non autorisée de droits de propriété intellectuelle, le Bureau du Procureur de la Bosnie-Herzégovine a autorisé un service de police à envoyer une demande de divulgation volontaire de données, sur la base de l'article 18.1.b. de la Convention de Budapest, directement à un fournisseur de services américain.

- Le **Chili** a expliqué que sa coopération avec le secteur privé, en particulier avec des fournisseurs de services sur Internet non-chiliens, s'est améliorée après son adhésion à la Convention. Sur la base de l'article 18 de la Convention, le Chili reçu des informations liées à l'abonné, y compris des informations sur l'IP, une coopération directe s'est mise en place avec des entreprises privées, notamment Facebook, Instagram, Uber, Google, Microsoft et d'autres. Avant son adhésion, le Chili obtenait une coopération moins bonne ; les fournisseurs de services sur Internet ne répondaient pas à ses demandes.

- La **France** soutient le Comité de la Convention sur la cybercriminalité (T-CY) dans son interprétation large de l'article 18 de la Convention (production rapide de données liées à l'abonné par les fournisseurs de service). Pour la France, l'article 18.1.b tel qu'il est compris par le T-CY offre une base juridique pour obtenir – directement de la part des fournisseurs de services - des données qui sont indispensables aux enquêtes criminelles. L'obtention d'une divulgation rapide de données détenues par des fournisseurs de services étrangers demeure difficile.

Les données disponibles montrent que la plupart des Parties utilisent la possibilité des fournisseurs de services américains de discuter volontairement d'informations sur l'abonné et que le niveau de coopération s'est considérablement amélioré dans les cinq années entre 2014 et 2019, même si que toutes les Parties ne participent au même niveau à cette coopération.

Une des caractéristiques envisagées pour le futur Deuxième protocole additionnel à la Convention de Budapest est de donner une base juridique plus claire à la coopération directe avec les fournisseurs de services dans d'autres Parties pour la divulgation d'informations liées à l'abonné. La coopération directe serait alors possible avec d'autres fournisseurs de service, pas seulement les Américains.

	Demandes d'informations sur des comptes reçues/divulguées par Facebook, Google/YouTube et Microsoft/Skype					
	En 2014			En 2019		
Des Parties	**Reçues**	**Divulguées**	**%**	**Reçues**	**Divulguées**	**%**
Albanie	19	4	21%	30	20	67%
Andorre	pas Partie			3	2	67%
Argentine	pas Partie			6648	5292	80%
Arménie	10	2	20%	27	15	56%
Australie	5482	3796	69%	8046	6494	81%
Autriche	231	64	28%	843	449	53%
Azerbaïdjan	0	0	0%	0	0	0%
Belgique	1789	1313	73%	2836	2379	84%
Bosnie-Herzégovine	13	8	62%	111	83	75%
Bulgarie	4	3	75%	73	41	56%
Cabo-Verde	pas Partie			0	0	0%
Canada	742	436	59%	4266	3407	80%
Chili	pas Partie			1253	798	64%
Colombie	pas Partie			836	465	56%
Costa Rica	pas Partie			101	60	59%
Croatie	45	34	76%	114	90	79%
Chypre	38	21	55%	40	23	58%
République tchèque	332	204	61%	737	573	78%
Danemark	343	221	64%	306	163	53%
République dominicaine	54	30	56%	326	161	49%
Estonie	35	19	54%	327	241	74%
Finlande	143	102	71%	417	346	83%
France	19184	12098	63%	33020	24121	73%
Géorgie	1	0	0%	20	13	65%
Allemagne	20696	12348	60%	43372	28094	65%
Ghana	pas Partie			3	0	0%
Grèce	pas Partie			1614	1023	63%
Hongrie	338	159	47%	810	347	43%
Islande	3	2	67%	5	2	40%
Israël	pas Partie			1755	1354	77%
Italie	7434	3913	53%	8917	4907	55%
Japon	1000	786	79%	883	634	72%
Lettonie	2	2	100%	91	45	49%
Liechtenstein	pas Partie			0	0	0%
Lituanie	35	22	63%	377	307	81%
Luxembourg	143	112	78%	248	76	31%
Malte	367	196	53%	495	237	48%
Monaco	pas Partie			14	8	57%
Maroc	pas Partie			262	182	69%

	Demandes d'informations sur des comptes reçues/divulguées par Facebook, Google/YouTube et Microsoft/Skype					
	En 2014			En 2019		
Ile Maurice	0	0	0%	0	0	0%
Moldova	13	7	54%	35	9	26%
Monténégro	7	1	14%	41	32	78%
Pays-Bas	1063	851	80%	2664	2083	78%
Macédoine du Nord	0	0	0%	147	69	47%
Norvège	342	235	69%	525	332	63%
Panama	88	68	77%	38	11	29%
Paraguay	pas Partie			43	15	35%
Pérou	pas Partie			152	100	66%
Philippines	pas Partie			58	23	40%
Pologne	1742	548	31%	11399	6659	58%
Portugal	2203	1355	62%	4023	2102	52%
Roumanie	79	40	51%	515	297	58%
Saint-Marin	pas Partie			1	0	0%
Sénégal	pas Partie			7	0	0%
Serbie	16	9	56%	396	286	72%
Slovaquie	104	36	35%	48	17	36%
Slovénie	10	6	60%	98	63	64%
Espagne	3892	2255	58%	7442	4198	56%
Sri Lanka	0	0	0%	99	42	42%
Suisse	396	270	68%	1917	1290	67%
Tonga	pas Partie		%	1	1	100%
Turquie	8016	5621	70%	9740	6071	62%
Ukraine	5	2	40%	91	60	66%
Royaume-Uni	16599	12557	75%	31644	26424	84%
Etats-Unis	64591	50026	77%	136101	114127	84%
Total hors Etats-Unis	**93158**	**59756**	**64%**	**190350**	**132633**	**70%**
Total Etats-Unis compris	**157749**	**109782**	**70%**	**326451**	**246760**	**76%**

4 Renforcement des capacités

4.1 Logique sous-jacente

Renforcer les capacités des praticiens pour enquêter, poursuivre et juger la cybercriminalité et d'autres infractions impliquant des preuves électroniques est probablement la meilleure façon d'apporter une réponse efficace en justice pénale à ces défis.

Alors que la communauté internationale se divise depuis des décennies sur la meilleure manière de traiter les questions de cybercriminalité au niveau international, il y a toujours eu cependant un large consensus autour de la consolidation des capacités, qui était également un résultat intermédiaire des travaux du groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité en février 2013.

Le Conseil de l'Europe a donc décidé en octobre 2013 de renforcer ses propres capacités pour une consolidation plus efficace des capacités des Etats membres en établissant le Bureau des programmes pour la cybercriminalité «Cybercrime Programme Office (C-PROC)» à Bucarest, Roumanie. Le C-PROC a soutenu près d'un millier d'activités depuis son entrée en fonction en avril 2014. Il gère actuellement des projets pour un volume de près de 40 millions d'euros, que ce soient des programmes conjoints avec l'Union européenne ou des projets financés par des contributions volontaires.

Intitulé du projet	Durée	Budget	Financement
Cybercrime@Octopus	janv. 2014 – déc. 2020	4 millions EUR	Contributions volontaires (Estonie, Hongrie, Japon, Monaco, Pays-Bas, Roumanie, Slovaquie, Royaume-Uni, Etats-Unis et Microsoft)
Projet étendu GLACY+ sur une action globale contre la cybercriminalité	mars 2016 – fév2024	19millions EUR	PC UE/CdE
Projet iPROCEEDS-2 ciblant les produits du crime sur Internet en Europe du Sud-Est et en Turquie	janv. 2020 – juin 2023	5millions EUR	PC UE/CdE
Projet EndOCSEA@Europe contre l'exploitation et l'abus sexuel des enfants en ligne	juil. 2018 – juin 2021	1 million EUR	Fonds "End Violence against Children"
CyberSouth sur la consolidation des capacités dans le Voisinage Sud	juil. 2017 – déc. 2021	5 millions EUR	PC UE/CdE
Projet CyberEast sur la lutte contre la cybercriminalité pour la cyber-résilience dans la Région du partenariat oriental	juin 2019 – juin 2022	4,2 millions EUR	PC UE/CdE

Ces projets peuvent aider tout pays ou territoire qui en fait la demande à développer son droit interne sur la cybercriminalité de manière pratique, au moyen d'études documentaires, de conseils, d'ateliers dans le pays ou en ligne et d'autres activités de ce même type. Parmi ces exemples récents, on citera le Burkina Faso, les Fidji, la Gambie, le Guatemala, la Namibie ou le Niger.

Des experts de nombreux pays participent également à des événements régionaux sur différents thèmes liés à la cybercriminalité, organises par le C-PROC ou en collaboration avec des organisations nationales, régionales ou internationales.

Toutefois, pour l'accès à la totalité des activités – notamment des programmes de formation durable pour la police, les procureurs et les juges; des unités spécialisées sur la cybercriminalité; des systèmes de signalement de la cybercriminalité; des mesures pour renforcer la coopération public/privé, interservices et internationale; la protection des enfants contre la violence sexuelle en ligne – la priorité est donnée aux Etats qui ont demandé l'adhésion à la Convention de Budapest

L'idée est que si un Etat demande à adhérer à la Convention de Budapest, cela témoigne de l'engagement politique nécessaire qui justifie le soutien au développement de son droit interne dans le droit fil de ce traité et le renforcement des capacités des autorités de justice pénale pour appliquer cette législation dans l'enquête, la poursuite et la sanction de cyber-infractions et d'autres infractions impliquant des preuves électroniques.

La participation n'est pas limitée à l'Europe seulement, tous les pays ou autres régions sont potentiellement concernés. Les Philippines et le Sri Lanka en Asie, ou encore le Ghana, l'Ile Maurice, le Maroc ou le Sénégal en Afrique, mais aussi la République dominicaine en Amérique latine ou le Tonga au Pacifique, et d'autres pays, ont décidé de fonder leur droit interne sur la Convention de Budapest et de demander l'adhésion à ce traité. En conséquence, ils ont pu être retenus pour participer à une large gamme d'activités.

4.2 Exemples d'activités de consolidation de capacités qui ont été menées

Il faudrait plus d'une centaine de pages pour dresser une liste exhaustive des activités soutenues ces dernières années dans plus d'une centaine de pays dans le monde, et il n'est pas possible de se livrer ici à une évaluation complète de l'impact de toutes ses activités.[3] Nous présentons donc toute une série d'exemples ci-après montrant que les Etats qui se sont engagés à adhérer à la Convention de Budapest peuvent bénéficier d'un soutien cohérent et pluriannuel pour leur permettre d'appliquer ce traité concrètement et de s'engager dans une coopération internationale efficace.
Il convient également de souligner que le Conseil de l'Europe, mais aussi d'autres organisations et gouvernements ont lancé toute une gamme d'initiatives de renforcement des capacités à partir de 2013[4].

[3] La liste complète des activités sera fournie sur demande. Pour plus de détails sur les projets et leur impact veuillez consulter le site www.coe.int/cybercrime.

[4] On citera à titre d'exemple l'ONUDC et son Programme mondial sur la Cybercriminalité; l'Union européenne a adopté en 2013 une stratégie de la cybersécurité prônant la consolidation des capacités et cet engagement reste d'actualité comme le montrent les Conclusions du Conseil sur les lignes directrices de l'UE en matière de consolidation des cyber-capacités externes (EU External Cyber Capacity Building Guidelines) de juin 2018; le Gouvernement des Etats-Unis - via le Département d'Etat et le Département de la Justice notamment – aide d'autres pays par des formations et par d'autres moyens; Le Foreign and Commonwealth Office du Royaume-Uni finance le GCSCC (Global Cyber Security Capacity Centre) et a monté un programme de consolidation des capacités en cybersécurité (Cyber Security Capacity Building Programme); le Gouvernement des Pays-Bas a créé en 2015 et finance le GFCE (Global Forum on Cyber Expertise (GFCE); la Banque mondiale a développé en 2016 une boîte à outils - "Combatting cybercrime – Tools et Capacity Building for Emerging Economies"; l'OEA (Organisation of American States) soutient ses Etats membres en matière de consolidation de leurs capacités concernant la cybercriminalité et la cybersécurité; INTERPOL a établi un Groupe d'experts mondiaux sur la cybercriminalité et assure des formations ciblées dans différentes régions du monde, souvent en coopération avec d'autres organisations telles que le Conseil de l'Europe; la CNUCED (UNCTAD) continue de soutenir les pays pour le développement de leur cadre réglementaire en matière de TIC, y compris contre la cybercriminalité.

4.2.1 Afrique: Sénégal

Après plusieurs réformes législatives, le gouvernement sénégalais a adopté la Loi 2008-11 du 25 janvier 2008 sur la cybercriminalité qui s'inspire directement de nombreuses dispositions de la Convention de Budapest. En novembre 2016, de nouveaux amendements ont été introduits au Code pénal et au Code de procédure pénale pour créer et continuer d'améliorer le cadre juridique concernant la cybercriminalité et pour faciliter le recueil de preuves électroniques.

En 2011, le Sénégal a demandé l'adhésion à la Convention de Budapest et y a été invité, devenant Partie à ce traité en 2017.

Depuis 2013, le Sénégal est un pays prioritaire pour le projet GLACY sur l'action mondiale contre la cybercriminalité, et en 2016, il est également devenu un point nodal régional au titre du projet étendu GLACY + sur l'action mondiale contre la cybercriminalité. Le Sénégal a bénéficié des activités suivantes:

Date	Lieu	Titre
Multiple	Strasbourg, France	Conférences Octopus 2009, 2013, 2015, 2016, 2018, 2019
10-14 fév2014	Dakar, Sénégal	Rapport de situation nationale et évaluation du pays au Sénégal
24-27 mars 2014	Dakar, Sénégal	Conférence de lancement du projet GLACY combinée avec des ateliers sur la coopération internationale et les systèmes de statistique/compte-rendu
12-16 mai 2014	La Haye, Pays-Bas	Atelier international sur les stratégies de formation des services répressifs
2-3 juin 2014	Bucarest, Roumanie	Atelier international pour dégager un consensus sur le concept pour la formation judiciaire, organisé à l'Institut national roumain de la Magistrature
17-18 juin 2014	Strasbourg, France	11e Plénière T-CY
7-18 sept 2014	Bruxelles, Belgique	Formation des services répressifs pour des participants du Sénégal et du Maroc (Partie 1)
1-3 oct 2014	Singapour	Participation à la Conférence INTERPOL-Europol sur la cybercriminalité
13-17 oct 2014	Bruxelles, Belgique	Formation des services répressifs pour des participants du Sénégal et du Maroc (Partie 2)
nov 2014	-	Contribution d'un expert sénégalais au Rapport d'analyse sur le projet d'amendement de la législation du Royaume marocain par rapport aux exigences de la Convention du Conseil de l'Europe sur la cybercriminalité
2-3 déc 2014	Strasbourg, France	12e Plénière T-CY
8-12 déc 2014	Dakar, Sénégal	Session d'introduction – formation du personnel judiciaire
26-27 mars 2015	Colombo, Sri Lanka	Atelier international sur les stratégies en matière de cybercriminalité, pour tous les pays participant à GLACY
15-19 juin 2015	Strasbourg, France	13e Plénière T-CY et Conférence Octopus
7-11 sept 2015	Dakar, Sénégal	Session d'introduction à la cybercriminalité pour les services répressifs – Police
14-18 sept 2015	Dakar, Sénégal	Session d'introduction à la cybercriminalité pour les services répressifs –Gendarmerie

23-24 nov 2015	Dakar, Sénégal	Réunion des Gendarmeries africaines
30 nov – 2 déc 2015	Strasbourg, France	14e Plénière T-CY
8-11 fév2016	Dakar, Sénégal	Soutien à la tenue de la Session de formation introductive pour la Justice
21-23 mars 2016	Port Louis, Ile Maurice	Deuxième Atelier international sur l'adaptation et l'actualisation du Manuel de la preuve électronique par l'élaboration des Procédures opérationnelles standard pour l'informatique forensique, pour tous les pays participant à GLACY
30 mars – 1 avril 2016	Dakar, Sénégal	Mission consultative sur les systèmes de signalement de cyber-délits, combinée avec atelier sur les systèmes de signalement et la coopération interservices
11-13 avril 2016	Afrique du Sud	Atelier international sur l'intégration des programmes de formation judiciaire (avec la participation de tous les pays participant à GLACY)
25-27 avril 2016	Colombo, Sri Lanka	Atelier international et formation pour les points de contact 24/7 des pays du GLACY (avec la participation de tous les pays participant à GLACY)
2-4 mai 2016	Dakar, Sénégal	Session de formation judiciaire avancée
9-11 mai 2016	Dakar, Sénégal	Améliorer la coopération internationale sur la cybercriminalité et la preuve électronique en Afrique de l'Ouest (projet GLACY)
23-26 mai 2016	Strasbourg, France	15e Plénière T-CY
1-3 juin 2016	Dakar, Sénégal	Atelier dans le pays sur les stratégies de formation pour les services répressifs et la sensibilisation aux questions de CY pour la police nationale
27-28 juillet 2016	Rabat, Maroc	Atelier international sur l'efficacité de la législation en matière de cybercriminalité et la preuve électronique telle que mesurée par des statistiques
15-18 août 2016	Dakar, Sénégal	Réunions de bilan des progrès et rapports de situation actualisés pour la participation du pays aux projets GLACY/GLACY+
28-30 sept 2016	Singapour	4e Conférence INTERPOL-Europol cybercriminalité
26-28 oct 2016	Bucarest, Roumanie	Conférence de clôture GLACY pour faire le point sur les résultats du projet et adopter la déclaration sur les priorités stratégiques et l'évènement de lancement du projet GLACY+
14-18 nov 2016	Strasbourg, France	16e Plénière T-CY et Conférence Octopus
16-17 janv2017	Dakar, Sénégal	Mission consultative et atelier sur les politiques en matière de cybercriminalité
25-26 janv2017	Nairobi, Kenya	Participation à l'atelier ICANN sur la consolidation des capacités pour les services répressifs africains
27 fév– 1 mars 2017	Singapour	INTERPOL ateliers de formation communs pour les services répressifs, de poursuite, les autorités centrales pour l'entraide judiciaire et le renforcement des PC24/7, et Atelier international sur la coopération avec les fournisseurs de services sur Internet
14-17 mars 2017	Dakar, Sénégal	Formation régionale CdE-ECOWAS Introduction pour les services judiciaires à la cybercriminalité et à la preuve électronique, pays d'Afrique de l'Ouest et Mauritanie (projet GLACY+)
29-31 mars 2017	Accra, Ghana	Atelier international sur les statistiques de la justice pénale concernant la cybercriminalité et la preuve électronique, avec tous les pays participant à GLACY+

10-13 avril 2017	Vienne, Autriche	Participation à la 3eRéuniondu Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité (UNIEG)
7-9 juin 2017	Strasbourg, France	17e Plénière T-CY
19-23 juin 2017	Dakar, Sénégal	Session de formation des formateurs pour premiers intervenants, Gendarmerie
21-23 août 2017	Dakar, Sénégal	Ateliers sur la protection des données et les outils et services d'INTERPOL combines avec un soutien – comment créer et renforcer les points de contact 24/7 pour la cybercriminalité et la preuve électronique
11-13 sept 2017	Abuja, Nigéria	Conférence régionale conjointe CdE-ECOWAS sur l'harmonisation de la législation sur la cybercriminalité et la preuve électronique avec l'Etat de droit et les protections des droits de l'homme (projet GLACY+)
11-13 oct 2017	Port Louis, Ile Maurice	4e Réunion du Groupe de travail africain sur la cybercriminalité pour les chefs de services de lutte contre la cybercriminalité
20-24 nov 2017	Singapour	INTERPOL, Session de développement pour les instructeurs
27-29 nov 2017	Strasbourg, France	18e Plénière T-CY
11-13 déc 2017	Cebu, Philippines	Atelier international sur les stratégies de formation judiciaires sur la cybercriminalité et la preuve électronique
7-8 mars 2018	La Haye, Pays-Bas	Conférence internationale conjointe CdE/Eurojust sur la coopération judiciaire en matière de cybercriminalité
26-27 mars 2018	Dakar, Sénégal	Conseil sur la rationalisation des procédures pour l'entraide judiciaire concernant la cybercriminalité et la preuve électronique
5-7 mai 2018	Dakar, Sénégal	Atelier AfGWG (AfriNIC Government Working Group) et ICANNs Capacity Development Workshop pour les services répressifs et services de protection des consommateurs des membres du GAC africain
7-11 mai 2018	Dakar, Sénégal	Formation de base régionale des formateurs des services répressifs sur la cybercriminalité et la preuve électronique pour des officiers de gendarmerie africains
14-18 mai 2018	Vienne, Autriche	Commission des Nations unies pour la prévention du crime et la justice pénale
18-22 juin 2018	Singapour	INTERPOL, Session de développement pour les instructeurs
9-13 juillet 2018	Strasbourg, France	19e Plénière T-CY et Conférence Octopus
4-7 sept 2018	Strasbourg, France	Conférence sur l'économie souterraine
18-20 sept 2018	Singapour	6e Conférence INTERPOL-Europol sur la cybercriminalité
16-18 oct 2018	Addis Abeba, Ethiopie	Forum africain sur les politiques de consolidation des capacités contre la cybercriminalité par des organisations internationales/régionales, organisé en collaboration avec la Commission de l'Union africaine
12-15 nov 2018	Dakar, Sénégal	Formation judiciaire avancée sur la cybercriminalité et la preuve électronique pour les juges, les procureurs et les avocats avec la

		participation de pays francophones et lusophones de la Région ECOWAS
27-30 nov 2018	Strasbourg, France	20e Plénière T-CY et Plénière Rédaction du Protocole
4-6 déc 2018	Accra, Ghana	5e Réunion du Groupe de travail africain d'INTERPOL sur la cybercriminalité pour les chefs de services de lutte contre la cybercriminalité
17-21 déc 2018	Dakar, Sénégal	Session de formation ECTEG: cybercriminalité et formation à l'informatique forensique spécialisée pour des membres des services répressifs
24-30 mars 2019	Vienne, Autriche	Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
4-5 avril 2019	Cotonou, Bénin	Contribution d'un expert du Sénégal à l'atelier de sensibilisation à la Convention de Budapest
15-16 avril 2019	Bruxelles, Belgique	Cyber Forum de l'UE
15-17 mai 2019	Bucarest, Roumanie	Atelier de présentation FREETOOL en coopération avec University College Dublin
3-7 juin 2019	Dakar, Sénégal	Formation régionale de formateurs pour les premiers intervenants sur la cybercriminalité et la preuve électronique pour les gendarmeries africaines
24-27 juin 2019	Accra, Ghana	Conférence sur la protection des données et de la vie privée, Région africaine
25-27 juin 2019	Singapour	Atelier sur les canaux et voies de coopération internationale en matière de cybercriminalité
8-11juillet 2019	Strasbourg, France	21e Plénière T-CY et 4ePlénière Rédaction du Protocole
10-12 juillet 2019	Strasbourg, France	Conférence internationale des formateurs judiciaires sur la cybercriminalité et la preuve électronique
3-6 sept 2019	Strasbourg, France	Conférence sur l'économie souterraine
23-26 sept 2019	Lagos, Nigéria	Atelier régional africain sur la cybercriminalité, la cybersécurité nationale et la politique de l'internet
21-23 oct 2019	Dakar, Sénégal	Mission consultative sur les capacités des CERT, lab d'informatique forensique et la coopération public-privé
24-25 oct 2019	Dakar, Sénégal	Mission consultative sur le signalement et le suivi de la cybercriminalité et atelier sur la collecte et le contrôle des statistiques de justice pénale sur la cybercriminalité et la preuve électronique
30 sept - 1 oct 2019	La Haye, Pays-Bas	Conférence internationale Eurojust-CdEsur les enquêtes en ligne: Darknet et violence sexuelle en ligne contre les enfants
9-11 oct 2019	La Haye, Pays-Bas	Conférence Europol-INTERPOL sur la cybercriminalité
18-20 nov 2019	Strasbourg, France	22e Plénière T-CY et 5ePlénière Rédaction du Protocole
2-4 déc 2019	Nairobi, Kenya	6e Réunion du Groupe de travail africain d'INTERPOL sur la cybercriminalité pour les chefs de services de lutte contre la cybercriminalité

4.2.2 Asie: Sri Lanka

Le Sri Lanka a adopté sa Loi sur la criminalité informatique en 2007. Cette loi a été largement inspirée de la Convention de Budapest. En 2008, un premier atelier à Colombo a bénéficié d'un soutien et, dans les années qui ont suivi, des experts du Sri Lanka ont participé à plusieurs autres activités.

En 2015, toutefois, le Sri Lanka été invité à adhérer à la Convention de Budapest et est devenu Partie à ce traité. Cela a permis la mise en œuvre d'un très grand nombre d'activités concentrées tout particulièrement sur la formation des services répressifs, des procureurs et des juges de ce pays.

En 2020, non seulement le Sri Lanka est devenu un pays prioritaire pour le soutien, mais il sert de point nodal pour partager son expérience et des experts du Sri Lanka sont maintenant devenus des praticiens formateurs dans d'autres pays de la région Asie-Pacifique.

Date	Lieu	Titre
27-28 oct 2008	Colombo, Sri Lanka	Atelier sur la cybercriminalité pour les juges, les procureurs et les enquêteurs au Sri Lanka
5-6 avril 2011	Colombo, Sri Lanka	Atelier régional sur la coopération contre la cybercriminalité en Asie du sud
4-5 oct 2013	Colombo, Sri Lanka	Atelier sur la consolidation des capacités en matière de lutte contre la cybercriminalité: formation judiciaire et des services répressifs
Multiple	Strasbourg, France	Conférences Octopus 2008, 2009, 2010, 2011, 2013, 2015, 2016, 2018, 2019
26-27 mars 2015	Colombo, Sri Lanka	Conférence pour les décideurs: Evaluer la menace de la cybercriminalité
26-27 mars 2015	Colombo, Sri Lanka	Atelier international sur les stratégies en matière de lutte contre la cybercriminalité (durant la Conférence de Colombo)
26-27 mars 2015	Colombo, Sri Lanka	Atelier international sur les statistiques de la justice pénale et les systèmes de suivi (durant la Conférence de Colombo)
30 sept – 2 oct 2015	La Haye, Pays-Bas	Participation à la Conférence INTERPOL-Europol sur la cybercriminalité
4-8 nov 2015	Colombo, Sri Lanka	Formation pour les premiers intervenants: formation de formateurs
30 nov – 2 déc 2015	Strasbourg, France	14 e Plénière T-CY
12-14 janv2016	Colombo, Sri Lanka	Mission d'exploration sur les systèmes de suivi de la cybercriminalité, combinée avec un atelier sur les systèmes de suivi et la base juridique pour la coopération interservices
8-10 fév2016	Colombo, Sri Lanka	Formation à l'informatique forensique: recueil de données à chaud, pour les services répressifs & CERT
11-12 fév2016	Colombo, Sri Lanka	Visite d'étude du Tonga au SL-CERT
21-23 mars 2016	Port Louis, Ile Maurice	Deuxième Atelier international sur l'adaptation et l'actualisation du Manuel de la preuve électronique par l'élaboration des Procédures opérationnelles standard pour l'informatique forensique, pour tous les pays participant à GLACY
31 mars-3 avril 2016	Colombo, Sri Lanka	Cours de formation judiciaire introductif pour les juges
5-6 avril 2016	Colombo, Sri Lanka	Cours de formation judiciaire introductif pour les procureurs

11-13 avril 2016	Afrique du Sud	Atelier international sur l'intégration des programmes de formation judiciaire (avec la participation de tous les pays participant à GLACY)
25-27 avril 2016	Colombo, Sri Lanka	Atelier international et formation pour les points de contact 24/7 des pays du GLACY (avec la participation de tous les pays participant à GLACY)
23-26 mai 2016	Strasbourg, France	15e Plénière T-CY
27-28 juil 2016	Rabat, Maroc	Atelier international sur l'efficacité de législation sur la cybercriminalité et la preuve électronique mesurée par les statistiques
8-11 août 2016	Colombo, Sri Lanka	Réunion de bilan des progrès et rapports de situation actualisés pour la participation du pays aux projets GLACY/ GLACY+
31 août – 2 sept 2016	Colombo, Sri Lanka	Formation judiciaire avancée avec la participation de juges du Tonga et adaptation des supports révisés de la formation judiciaire avancée
24-25 sept 2016	Colombo, Sri Lanka	Soutien à la tenue au niveau national de la formation judiciaire introductive
28-30 sept 2016	Singapour	4eConférence INTERPOL-Europol sur la cybercriminalité
26-28 oct 2016	Bucarest, Roumanie	Conférence de clôture de GLACY pour discuter des résultats du projet et adopter la déclaration sur les priorités stratégiques et l'évènement de lancement du projet GLACY+
14-18 nov 2016	Strasbourg, France	16e Plénière T-CY et Conférence Octopus
27 fév– 1 mars 2017	Singapour	Ateliers de formation conjoints avec INTERPOL pour les services de lutte contre la cybercriminalité, services de poursuite, autorités centrales chargées de l'entraide judiciaire et renforcement des PC 24/7 et Atelier international sur la coopération avec les fournisseurs de services sur Internet
29-31 mars 2017	Accra, Ghana	Atelier international sur les statistiques de justice pénale sur la cybercriminalité et la preuve électronique, avec tous les pays participant à GLACY+
10-13 avril 2017	Vienne, Autriche	Participation à la 3e réunion du Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
5-8 juin 2017	Madrid, Espagne	Participation au Groupe de travail eurasien d'INTERPOL sur la cybercriminalité pour les chefs de services et à la réunion opérationnelle en marge sur la compromission de messageries commerciales
7-9 juin 2017	Strasbourg, France	17e Plénière T-CY
14-16 juin 2017	Bruxelles, Belgique	Atelier international pour les services de lutte contre la cybercriminalité et établissements de formation des services répressifs sur les stratégies de formation (niveau technique) et l'accès aux supports de formation de l'ECTEG
28-30 juil 2017	Colombo, Sri Lanka	Atelier résidentiel pour les Juges de la Cour suprême sur la cybercriminalité et la preuve électronique
9-13 août 2017	Colombo, Sri Lanka	Soutien à l'atelier sur la cybercriminalité pour l'entrée en fonction des nouveaux juges
16-20 août 2017	Katmandou, Népal	Formation spéciale sur la cybercriminalité pour les personnels de justice népalais avec des formateurs de l'institut de la

		magistrature du Sri Lanka, en partenariat avec l'Académie judiciaire du Népal
22-24 sept 2017	Colombo, Sri Lanka	Atelier en résidence pour les juges de district et magistrats sur la cybercriminalité et la preuve électronique (Lot 1/4)
13-15 oct 2017	Colombo, Sri Lanka	Atelier en résidence pour les juges de district et magistrats sur la cybercriminalité et la preuve électronique (lot 2/4)
20-24 nov 2017	Singapour	INTERPOL, Session de développement pour les instructeurs
27-29 nov 2017	Strasbourg, France	18e Plénière T-CY
11-13 déc 2017	Cebu, Philippines	Atelier international sur les stratégies de formation judiciaires sur la cybercriminalité et la preuve électronique
18-19 déc 2017	Colombo, Sri Lanka	Conférence annuelle pour les juges organisée par l'Institut des juges du Sri Lanka
19-21 fév2018	Colombo, Sri Lanka	Mission consultative sur l'établissement de la Division cybercriminalité au sein du CID
7-8 mars 2018	La Haye, Pays-Bas	Conférence internationale conjointe CdE/Eurojust sur la coopération judiciaire en matière de cybercriminalité
12-16 mars 2018	Hong Kong	Participation au Cours Cyber Command Course organisé par la Police de Hong Kong
13-15 mars 2018	Dhaka, Bangladesh	Participation à l'Atelier sur la cybercriminalité et la cybersécurité pour les pays membres du BIMSTEC
16-18 mars 2018	Colombo, Sri Lanka	Atelier en résidence pour les juges de district et magistrats sur la cybercriminalité et la preuve électronique (Lot 3/3)
27-30 mars 2018	Chisinau, Moldova	Participation à la Réunion régionale: exercice de coopération en matière de cybercriminalité organisé dans le cadre du projet Cybercrime@EAP 2018
4-6 avril 2018	Colombo, Sri Lanka	Intégration de supports ECTEG dans la stratégie de formation pour les personnels des services répressifs
8-10 mai 2018	Téhéran, Iran	Participation au Groupe de travail eurasien d'INTERPOL sur la cybercriminalité pour les Chefs de services
14-18 mai 2018	Vienne, Autriche	Commission des Nations unies pour la prévention du crime et la justice pénale
18-22 juin 2018	Singapour	INTERPOL, Session de développement pour les instructeurs
27-29 juin 2018	Londres, Royaume-Uni	Participation au 3e Groupe d'experts en informatique forensique d'INTERPOL
9-13 juil 2018	Strasbourg, France	19e Plénière T-CY et Conférence Octopus
4-7 sept 2018	Strasbourg, France	Conférence sur l'économie souterraine
29 oct – 2 nov 2018	Colombo, Sri Lanka	Formation ECTEG: cybercriminalité et formation spécialisée en informatique forensique pour les personnels des services répressifs
14-16 nov 2018	Colombo, Sri Lanka	Ateliers sur la protection des données et les Outils et Services d'INTERPOL combinés avec un soutien sur comment créer et renforcer les points de contact 24/7 pour la cybercriminalité et la preuve électronique
27-30 nov 2018	Strasbourg, France	20ePlénière T-CY et Plénière Rédaction du Protocole
2-3 mars 2019	Colombo, Sri Lanka	Soutien à l'atelier sur la cybercriminalité pour l'entrée en fonction de nouveaux juges

18-22 mars 2019	Hong Kong	Participation à la formation Cyber Command Course organisée par la Police de Hong Kong
24-30 mars 2019	Vienne, Autriche	Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
15-16 avril 2019	Bruxelles, Belgique	Cyber Forum UE
15-17 mai 2019	Bucarest, Roumanie	Atelier de présentation de FREETOOL en coopération avec University College Dublin
22-24 mai 2019	Seoul, Korea	Participation au 20eSymposium International sur la réponse à la cybercriminalité (ISCR 2019)
25-27 juin 2019	Singapour	Atelier sur les canaux et voies de coopération internationale en matière de cybercriminalité
8 juil 2019	Bruxelles, Belgique	Visite d'étude de juges du Sri Lanka en Belgique et atelier sur la cybercriminalité et la preuve électronique
16-27 juil 2019	Leon, Espagne	Participation au Camp d'été Cybersécurité 2019
8-11 juil 2019	Strasbourg, France	21e Plénière T-CY et 4e Plénière Rédaction du Protocole
10-12 juil 2019	Strasbourg, France	Conférence internationale des formateurs judiciaires sur la cybercriminalité et la preuve électronique
28 juil 2019	Bucarest, Roumanie	Revue du cadre pour une proposition de loi sri-lankaise sur la protection des données personnelles
2-6 sept 2019	Manille, Philippines	Participation à la formation à l'analyse des maliciel, organisée par INTERPOL
3-6 sept 2019	Strasbourg, France	Conférence sur l'économie souterraine
30 sept - 1 oct 2019	La Haye, Pays-Bas	Eurojust-CdE,Conférence internationale sur les enquêtes en ligne: Darknet et violence sexuelle en ligne contre les enfants
8 oct 2019	La Haye, Pays-Bas	Réunion des PC 24/7 des Parties à la Convention de Budapest
9-11 oct 2019	La Haye, Pays-Bas	Conférence Europol-INTERPOL sur la cybercriminalité
30 oct - 1 nov	Suva, Fidji	Participation d'un expert du Sri Lanka à la Mission consultative sur la législation concernant la cybercriminalité à Fidji
18-20 nov 2019	Strasbourg, France	22e Plénière T-CY et 5e Plénière Rédaction du Protocole
26-28 fév2020	Tbilissi, Géorgie	Réunion internationale sur la coopération avec des fournisseurs de services étrangers

4.2.3 Europe: Serbie

En 2005, le Conseil de l'Europe a lancé le projet Paco Serbie sur la criminalité économique dont un volet portait sur la cybercriminalité. C'était là le premier projet du Conseil de l'Europe portant spécifiquement sur ce thème, en dehors d'une Conférence Octopus sur la cybercriminalité qui avait été organisée en 2004. La Serbie a signé la Convention de Budapest la même année, et est devenue Partie à ce traité en 2009.

Entre 2009 et 2013, la Serbie a été un pays prioritaire dans le cadre du projet Cybercrime@IPA sur la coopération régionale sur la cybercriminalité en Europe du sud-est.

En 2016, un nouveau projet régional été lancé dans cette région: iPROCEEDS, couvrant la période 2016 à 2019, se concentrait sur les produits du crime en ligne. La Serbie a été là-encore un pays prioritaire, et cela vaut aussi pour le projet de suivi iPROCEEDS-2 qui a commencé en janvier 2020.

Le tableau ci-après ne recense que les activités au titre du projet iPROCEEDS auxquelles ont participé des experts de la Serbie:

Date	Lieu	Titre
14-15 avril 2016	Belgrade, Serbie	Visite d'évaluation du pays pour faire l'état des lieux initial
24–25 mai 2016	Strasbourg, France	15e Plénière du Comité de la Convention sur la cybercriminalité (T-CY)
13-14 juin 2016	Ohrid, Macédoine du Nord	Atelier régional sur le partage d'information privé/public et les mécanismes d'échange d'information entre les institutions du secteur financier, les services de lutte contre la cybercriminalité et d'autres parties prenantes (combiné avec la Conférence d'ouverture du projet iPROCEEDS)
7-8 sept 2016	Belgrade, Serbie	Mission consultative et atelier sur les mécanismes de signalement
13-15 sept 2016	Helsinki, Finlande	Participation de services de lutte contre la cybercriminalité à RISE (Régional Internet Security Event) - Finlande 2016 (Team Cymru)
28-30 sept 2016	Singapour	Conférence annuelle INTERPOL-Europol cybercriminalité
11-12 oct 2016	Zagreb, Croatie	Atelier régional pour faire l'état des lieux des programmes de formation judiciaire sur la cybercriminalité, la preuve électronique et les produits du crime en ligne
24-25 oct 2016	Dublin, Irlande	Réunion internationale sur la coopération privé/public
25 nov 2016	Tirana, Albanie	Atelier régional sur les mécanismes de signalement: Bonnes pratiques internationales
14-15 nov 2016	Strasbourg, France	16e Plénière du Comité de la Convention sur la cybercriminalité (T-CY)
16-18 nov 2016	Strasbourg, France	Participation à la Conférence Octopus 2016
12-13 déc 2016	Bucarest, Roumanie	Atelier régional sur les risques de blanchiment de capitaux liés aux nouvelles technologies
16-17 janv2017	Belgrade, Serbie	Atelier sur la fraude financière et à la carte de crédit en ligne
28 Feb-3 mars 2017	Bucarest, Roumanie	Formation régionale pour les services de lutte contre la cybercriminalité, contre le crime économique et financier, les enquêteurs financiers et les procureurs spécialisés sur les monnaies virtuelles et le dark web (EMPACT)
19-20 avril 2017	Belgrade, Bucarest	Atelier sur la coopération interservices et internationale pour le dépistage, la saisie et la confiscation des produits du crime en ligne
24-28 avril 2017	Tbilissi, Géorgie	Exercice de simulation d'une affaire régionale sur la cybercriminalité et les investigations financières

10 avril 2017	Belgrade, Serbie	Réunion sur la Coopération public-privé
10-13 avril 2017	Vienne, Autriche	Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
12-13 juin 2017	Luxembourg	Atelier international pour les services de lutte contre la cybercriminalité, contre la criminalité économique, les enquêteurs financiers, les CRF et les procureurs spécialités, sur les techniques de recherche, de saisie et de confiscation des produits du crime en ligne en coopération avec la CRF du Luxembourg (combiné avec la 3e Réunion du Comité directeur du projet)
15-16 juin 2017	Bruxelles, Belgique	Atelier international sur les stratégies de formation à la cybercriminalité pour les services répressifs et l'accès à des supports de l'ECTEG en coopération avec INTERPOL et ECTEG
20-24 juin 2017	Budva, Monténégro	Formation régionale de formateurs pour dispenser le module de formation de base pour les juges et les procureurs sur la cybercriminalité, la preuve électronique et les produits du crime en ligne
22-23 juin 2017	Belgrade, Serbie	Mission d'évaluation des lignes directrices pour prévenir et détecter/identifier les produits du crime en ligne
5-8 sept 2017	Barcelone, Espagne	Conférence sur l'économie souterraine 2017 (organisée par Team Cymru)
27-29 sept 2017	La Haye, Pays-Bas	5e Conférence INTERPOL/Europol cybercriminalité
4-5 oct 2017	Ljubljana, Slovénie	Atelier régional pour partager des expériences concernant des indicateurs et lignes directrices pour les entités du secteur financier en vue de prévenir le blanchiment d'argent en ligne, en coopération avec la CRF de la Slovénie
9-11 oct 2017	Bakou, Azerbaïdjan	Conférence régionale sur la cybercriminalité et le blanchiment d'argent en coopération avec le réseau Global Prosecutor's E-Crime Network (GPEN) et le Gouvernement de l'Azerbaïdjan
12-13 oct 2017	Bucarest, Roumanie	Visite d'étude de représentants de CERT à la CERT-RO
30-31 oct 2017	Sofia, Bulgarie	Forum régional Europe du Sud-Est sur Cybersécurité et cybercriminalité en coopération avec le ministère de l'Intérieur de la Bulgarie
2-3 nov 2017	Bucarest, Roumanie	Atelier régional pour évaluer le cadre réglementaire national pour l'obtention et l'utilisation de la preuve électronique dans les procedures pénales
27-29 nov 2017	Strasbourg, France	8e Plénière de T-CY et 1ePlénière Rédaction du Protocole
4-7 déc 2017	Belgrade, Serbie	Session nationale du module de formation introductive sur la cybercriminalité, la preuve électronique et les produits du crime en ligne
11-15 déc 2017	Dublin, Irlande	Programme de master à distance
20-21 déc 2017	Skopje, Macédoine du Nord	Atelier régional pour le partage de bonnes pratiques concernant les mécanismes de signalement en place dans la région IPA (combiné avec la4eRéuniondu Comité directeur du projet)
7-8 mars 2018	La Haye, Pays-Bas	Conférence internationale conjointe sur la coopération judiciaire en matière de cybercriminalité en coopération avec EUROJUST
3-5 avril 2018	Vienne, Autriche	Réunion du Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité

3-4 mai 2018	Kyiv, Ukraine	Réunion régionale sur la coopération internationale sur la cybercriminalité et la preuve électronique
8-12 mai 2018	Dublin, Irlande	Programme de master à distance à l'UCD
14-18 mai 2018	Vienne, Autriche	27e session de la Commission des Nations unies pour la prévention du crime et la justice pénale "Réponses de la justice pénale pour prévenir et contrer la cybercriminalité sous toutes ses formes, par le renforcement de la coopération au niveau national et international"
14-15 mai 2018	Bucarest, Roumanie	Atelier régional sur les statistiques de la justice pénale sur la cybercriminalité et la preuve électronique
5-6 juin 2018	Tbilissi, Géorgie	EuroDIG 2018 – focus sur l'action de la justice pénale dans le cyberespace
12–15 juin	Belgrade, Serbie	Deuxième session nationale du module de formation introductive sur la cybercriminalité, la preuve électronique et les produits du crime en ligne
9-10 juil 2018	Strasbourg, France	19e Plénière T-CY
11-13 juil 2018	Strasbourg, France	Conférence Octopus cybercriminalité
4-7 sept 2018	Strasbourg, France	Conférence sur l'économie souterraine 2018 (co-organisée avec Team Cymru) (combinée avec la 5e Réunion du Comité directeur du projet)
4-5 oct 2018	Zagreb, Croatie	Forum régional sur la fraude en ligne en Europe du Sud-Est en coopération avec l'Académie judiciaire de la Croatie
5-7 nov 2018	Budapest, Hongrie	Formation sur les monnaies virtuelles en coopération avec le Centre de Formation internationale, International College of Financial Investigations
12-15 nov 2018	Bucarest, Roumanie	Exercice régional de simulation de cas sur la cybercriminalité et les investigations financières
27-29 nov 2018	Strasbourg, France	20e Plénière de T-CY et Plénière Rédaction du Protocole
10-14 déc 2018	Dublin, Irlande	Programme de master à distance
11–12 mars 2019	Belgrade, Serbie	Conseil aux autorités publiques et au groupe de travail sur la réforme du droit pour mettre le cadre juridique en conformité avec les normes de l'UE et du Conseil de l'Europe
25–26 mars 2019	Vienne, Autriche	6e Réunion du Groupe de rédaction du protocole, T-CY
27 – 29 mars 2019	Vienne, Autriche	Réunion du Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
29 mars 2019	Bucarest, Roumanie	6e Réunion du Comité directeur du projet
8-11 avril 2019	Belgrade, Serbie	Exercice régional de simulation de cas sur la cybercriminalité et les investigations financières (pour la Bosnie-Herzégovine, le Monténégro et la Serbie)
22 avril 2019	Belgrade, Serbie	Conseils sur les enseignements tirés des exercices de simulation
30 avril 2019	Zagreb, Croatie	Conférence internationale sur l'informatique forensique et la preuve informatique: DataFocus 2019
8-9 mai 2019	Bucarest, Roumanie	Exercise en salle sur la coopération internationale sur la cybercriminalité
15-17 mai 2019	Bucarest, Roumanie	Réunion sur "Free Forensic Tools for the Law Enforcement Community" (FREETOOL) en coopération avec l'UCD

25-27 juin 2019	Singapour	Atelier sur les canaux et voies de coopération internationale sur la cybercriminalité en coopération avec INTERPOL
26-27 juin 2019	Bucarest, Roumanie	4e Symposium annuel sensibilisation à la cybersécurité, organisé par l'Anti-Phishing Working Group
8-11 juil 2019	Strasbourg, France	21e Plénière T-CY et 4e Plénière PDP
10-12 juil 2019	Strasbourg, France	Première Réunion internationale des formateurs nationaux sur la cybercriminalité et la preuve électronique
3-6 sept 2019	Strasbourg, France	Conférence sur l'économie souterraine 2019
17-20 sept 2019	Bucarest, Roumanie	Formation régionale sur les enquêtes en ligne sous pseudonyme
30 sept-1 oct 2019	La Haye, Pays-Bas	Conférence internationale commune sur les enquêtes sur Internet en coopération avec EUROJUST
8 oct 2019	La Haye, Pays-Bas	Réunion des PC 24/7 créés par la Convention de Budapest
9-11 oct 2019	La Haye, Pays-Bas	Conférence annuelle INTERPOL-Europol cybercriminalité
14 oct 2019	Belgrade, Serbie	Atelier de bilan des progrès dans tous les secteurs des projets
21-25 oct 2019	Bucarest, Roumanie	Formation régionale sur le renseignement en source ouverte
18-22 nov 2019	Strasbourg, France	22e Plénière de T-CY et Conférence Octopus
25–28 nov 2019	Belgrade, Serbie	Session de formation introductive sur la cybercriminalité, la preuve électronique et les produits du crime en ligne pour les juges et les procureurs
2-6 déc 2019	Bucarest, Roumanie	Formation pilote ECTEG sur les cryptomonnaies et les enquêtes sur le Dark Web en coopération avec SELEC
3 déc 2019	Dublin, Irlande	Cérémonie de remise des diplômes pour les étudiants de l'UCD ayant obtenu leur master en investigations contre la cybercriminalité et informatique forensique, venus des aires concernées par le projet et soutenus par iPROCEEDS
9-10 déc 2019	Strasbourg, France	Conférence de clôture: évaluation des progrès marqués et définition de la marche à suivre

4.2.4 Amérique latine: République dominicaine

La République dominicaine a adopté sa loi 53-07 sur les crimes et délits liés à la haute technologie, publiée le 23 avril 2007, qui repose sur la Convention de Budapest. En 2013, elle est devenue le premier pays d'Amérique latine à devenir Partie à ce traité. En 2016, la République dominicaine non seulement est devenue pays prioritaire du projet GLACY+, mais également un point nodal pour l'Amérique latine et la région des Caraïbes. Les activités menées jusqu'ici concernaient:

Date	Lieu	Titre
13-15 mai 2008	Port of Espagne, Trinidad et Tobago	Atelier sur la législation en matière de cybercriminalité dans les Caraïbes
Multiple	Strasbourg, France	Conférences Octopus 2008, 2009, 2010, 2011, 2013, 2015, 2016, 2018, 2019
19-23 sept 2016	Saint-Domingue, République dominicaine	Visite d'évaluation initiale du pays en vue de le faire participer au projet GLACY+

28-30 sept 2016	Singapour	4e Conférence INTERPOL-Europol cybercriminalité
26-28 oct 2016	Bucarest, Roumanie	Conférence de clôture de GLACY pour discuter des résultats du projet et adopter la déclaration sur les priorités stratégiques et l'évènement de lancement du projet GLACY+
14-18 nov 2016	Strasbourg, France	16e Plénière T-CY et Conférence Octopus
27 fév– 1 mars 2017	Singapour	Ateliers de formation conjoints INTERPOL pour les services de lutte contre la cybercriminalité, services de poursuite, autorités centrale chargées de l'entraide judiciaire et renforcement des PC 24/7 et Atelier international sur la coopération avec les fournisseurs de services sur Internet
29-31 mars 2017	Accra, Ghana	Atelier international sur les statistiques de la justice pénale sur la cybercriminalité et la preuve électronique, avec tous les pays participant à GLACY+
24-28 avril 2017	Saint-Domingue, République dominicaine	Cours d'introduction de FdF sur la cybercriminalité et la preuve électronique pour les juges, les procureurs et les avocats et adaptation de supports au contexte local
10-13 avril 2017	Vienne, Autriche	Participation à la 3e réunion du Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité (UNIEG)
24-28 avril 2017	Manille, Philippines	Participation d'un délégué du Ghana à la formation INTERPOL sur l'analyse des maliciels
7-9 juin 2017	Strasbourg, France	17e Plénière T-CY
14-16 juin 2017	Bruxelles, Belgique	Atelier international pour les services de lutte contre la cybercriminalité et établissements de formation des services répressifs sur les stratégies de formation (niveau technique) et l'accès à des supports de formation de l'ECTEG
10-13 oct 2017	Saint-Domingue, République dominicaine	Soutien à la tenue du cours d'intro sur la cybercriminalité et la preuve électronique pour des juges et procureurs
16-17 oct 2017	Saint-Domingue, République dominicaine	Mission consultative sur le signalement de la cybercriminalité et atelier sur la collecte et le suivi des statistiques de la justice pénale sur la cybercriminalité et la preuve électronique
4-7 déc 2017	Saint-Domingue, République dominicaine	Forum sur les politiques concernant le renforcement des capacités de lutte contre la cybercriminalité, par des organisations internationales/régionales en AL et dans les Caraïbes
20-24 nov 2017	Singapour	INTERPOL, Session de développement pour les instructeurs
27-29 nov 2017	Strasbourg, France	18e Plénière T-CY
11-13 déc 2017	Cebu, Philippines	Atelier international sur les stratégies de formation judiciaires sur la cybercriminalité et la preuve électronique
7-8 mars 2018	La Haye, Pays-Bas	Conférence internationale conjointe CdE/Eurojust sur la coopération judiciaire en matière de cybercriminalité
3-5 avril 2018	Vienne, Autriche	Réunion du Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité (UNIEG)
14-18 mai 2018	Vienne, Autriche	Commission des Nations unies pour la prévention du crime et la justice pénale
11-15 juin	Saint-Domingue, République dominicaine	Cours ECTEG: informatique forensique, recueil de données à chaud, pour les personnels des services répressifs
18-22 juin 2018	Singapour	INTERPOL, Session de développement pour les instructeurs

26-28 juin 2018	Saint-Domingue, République dominicaine	Ateliers sur la protection des données et les outils et services d'INTERPOL combinés avec un soutien pour créer et renforcer les points de contact 24/7 pour la cybercriminalité et la preuve électronique
27-29 juin 2018	Londres, Royaume-Uni	Participation au 3eGroupe d'experts d'INTERPOL sur l'informatique forensique
9-13 juil 2018	Strasbourg, France	19e Plénière T-CY et Conférence Octopus
27-31 août 2018	Singapour	Atelier international conjoint pour les Services d'enquête en matière de cybercriminalité et les autorités centrales chargées des entraides judiciaires
4-7 sept 2018	Strasbourg, France	Conférence sur l'économie souterraine
18-20 sept 2018	Singapour	6eConférenceINTERPOL-Europol cybercriminalité
25-26 oct 2018	Saint-Domingue, République dominicaine	Congrès international sur la cybercriminalité organisé par l'Institut judiciaire de la République dominicaine
27-30 nov 2018	Strasbourg, France	20e Plénière T-CY et Plénière Rédaction du Protocole
11-15 mars 2019	Saint-Domingue, République dominicaine	Formation judiciaire avancée sur la cybercriminalité et la preuve électronique pour les juges, magistrats et procureurs
24-30 mars 2019	Vienne, Autriche	Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
2-3 avril 2019	Saint-Domingue, République dominicaine	Conseils pour la rationalisation des procédures d'entraide judiciaire en ce qui concerne la cybercriminalité et la preuve électronique
4-5 avril 2019	Saint-Domingue, République dominicaine	Mission consultative sur l'intégration/ prise en compte transversale de modules de formation dans les programmes des établissements de formation
15-16 avril 2019	Bruxelles, Belgique	Cyber Forum UE
15-17 mai 2019	Bucarest, Roumanie	Atelier de présentation de FREETOOL en coopération avec University College Dublin
28-30 mai 2019	Saint-Domingue, République dominicaine	Développement d'investigations liées à la cybercriminalité, de capacités en informatique forensique et de procédures opérationnelles sur la preuve numérique pour les services répressifs, combine avec des ateliers et conseils sur la coopération interservices et les partenariats privé public pour lutter contre la cybercriminalité
3-7 juin 2019	Saint-Domingue, République dominicaine	Formation aux enquêtes sur les cryptomonnaies dispensée à des services de cyber-police
12-14 juin 2019	Saint-Domingue, République dominicaine	Conférence régionale sur la cybercriminalité et politiques et stratégies en matière de cybersécurité
25-27 juin 2019	Singapour	Atelier sur les canaux et voies de coopération internationale en matière de cybercriminalité
1-3 juil 2019	Salvador	Mission consultative et atelier sur législation pour FOPREL
8-11 juil 2019	Strasbourg, France	21e Plénière T-CY et 4e Plénière Rédaction du Protocole
10-12 juil 2019	Strasbourg, France	Conférence internationale des formateurs judiciaires sur la cybercriminalité et la preuve électronique
3-6 sept 2019	Strasbourg, France	Conférence sur l'économie souterraine

30 sept - 1 oct 2019	La Haye, Pays-Bas	Conférence internationale Eurojust-CdE sur les enquêtes en ligne: Darknet et violence sexuelle en ligne contre les enfants
8 oct 2019	La Haye, Pays-Bas	Réunion des PC 24/7 des Parties à la Convention de Budapest
9-11 oct 2019	La Haye, Pays-Bas	Conférence Europol-INTERPOL cybercriminalité
11-14 nov 2019	Punta Cana, République dominicaine	Réunion avec les chefs des services de lutte contre la cybercriminalité de la région pour discuter d'activités opérationnelles et organiser une opération conjointe
18-20 nov 2019	Strasbourg, France	22e Plénière T-CY et 5e Plénière Rédaction du Protocole
16-18 déc 2019	Saint-Domingue, République dominicaine	Mission consultative sur la législation relative à la protection des données

4.2.5 Pacifique: Tonga

En 2003, le Tonga a adopté sa loi sur les infractions informatiques qui couvre largement les dispositions de la Convention de Budapest. Une réforme majeure pour un cadre légal plus complet est en cours. En décembre 2013, le Tonga a demandé à adhérer à la Convention de Budapest et est devenu Partie à ce traité en 2017.

Après sa demande d'adhésion en décembre 2013, le Tonga est devenu immédiatement un pays prioritaire du projet GLACY. En 2016, est ensuite devenu un point nodal régional pour la région du Pacifique sud dans le cadre du projet GLACY+.

Le Royaume du Tonga a participé aux activités suivantes:

Date	Lieu	Titre
16-17 juin 2010	Nu'alofa, Tonga	Réunion des ministres des TIC de la région Pacifique
27-29 avril 2011	Nu'alofa, Tonga	Atelier régional Pacifique sur la cybercriminalité
Multiple	Strasbourg, France	Conférences Octopus 2011, 2015, 2016, 2018, 2019
24-27 mars 2014	Dakar, Sénégal	Conférence de lancement du projet GLACY combinée avec ateliers sur la coopération internationale et systèmes de signalement/statistiques
28 avril – 2 mai 2014	Nu'alofa, Tonga	Rapport de situation nationale et évaluation du pays
12-16 mai 2014	La Haye, Pays-Bas	Atelier international sur les stratégies de formation des services répressifs
2-3 juin 2014	Bucarest, Roumanie	Atelier international pour dégager un consensus sur le concept pour la formation judiciaire, organisé à l'Ecole nationale de la Magistrature de la Roumanie
17-18 juin 2014	Strasbourg, France	11e Plénière T-CY
1-3 oct 2014	Singapour	Participation à la Conférence INTERPOL-Europol cybercriminalité
2-3 déc 2014	Strasbourg, France	12e Plénière T-CY
Jan-mai 2015	Nu'alofa, Tonga	Analyse du projet de législation du Tonga
26-27 mars 2015	Colombo, Sri Lanka	Atelier international sur les stratégies de lutte contre la cybercriminalité pour tous les pays de GLACY
24 avril& 1 mai 2015	Nu'alofa, Tonga	Formation introductive judiciaire FdF pour des juges et procureurs

27-29 avril 2015	Nu'alofa, Tonga	Session de formation pour les premiers intervenants, services répressifs
30 avril 2015	Nu'alofa, Tonga	Atelier sur l'établissement de CERT au niveau national
30 avril 2015	Nu'alofa, Tonga	Atelier sur la coopération interservices
15-19 juin 2015	Strasbourg, France	13e Plénière T-CY et Conférence Octopus
août-sept 2015	Nu'alofa, Tonga	Soutien à la rédaction de textes législatifs pour le Tonga
30 sept – 2 oct 2015	La Haye, Pays-Bas	Participation à la Conférence INTERPOL-Europol cybercriminalité
30 nov – 2 déc 2015	Strasbourg, France	14e Plénière T-CY
24-26 fév2016	Nu'alofa, Tonga	Soutien Atelier régional GPEN pour les procureurs/avocats du Pacifique
21-23 mars 2016	Port Louis, Ile Maurice	Deuxième Atelier international sur l'adaptation et l'actualisation du Manuel de la preuve électronique par le développement des Procédures opérationnelles standard pour l'informatique forensique (avec la participation de tous les pays de GLACY)
24-25 mars 2016	Port Louis, Ile Maurice	Visite d'étude du Tonga au CERT-MU
11-13 avril 2016	Afrique du Sud	Atelier international l'intégration des programmes de formation judiciaire (avec la participation de tous les pays de GLACY)
25-27 avril 2016	Colombo, Sri Lanka	Atelier international et formation pour les points de contact 24/7 des pays du GLACY (avec la participation de tous les pays de GLACY)
23-26 mai 2016	Strasbourg, France	15e Plénière T-CY
30-31 mai 2016	Nu'alofa, Tonga	Mission consultative au Tonga sur les systèmes de signalement de la cybercriminalité et atelier sur les systèmes de signalement, la coopération interservices et la coopération public-privé
1-3 juin 2016	Nu'alofa, Tonga	Réunions de bilan des progrès et rapports de situation actualisés pour la participation du pays aux projets GLACY/GLACY+
27-28 juil 2016	Rabat, Maroc	Atelier international sur l'efficacité de la législation sur la cybercriminalité et la preuve électronique mesurée par les statistiques
28-30 sept 2016	Singapour	4e Conférence INTERPOL-Europol cybercriminalité
26-28 oct 2016	Bucarest, Roumanie	Conférence de clôture de GLACY pour discuter des résultats du projet et adopter la déclaration sur les priorités stratégiques et l'évènement de lancement du projet GLACY+
14-18 nov 2016	Strasbourg, France	16e Plénière T-CY et Conférence Octopus
27 fév– 1 mars 2017	Singapour	Ateliers de formation conjoints INTERPOL pour les services de lutte contre la cybercriminalité, services de poursuite, autorités centrales chargées de l'entraide judiciaire et renforcement des PC 24/7 et Atelier international sur la coopération avec les fournisseurs de services sur Internet
29-31 mars 2017	Accra, Ghana	Atelier international sur les statistiques de la justice pénale sur la cybercriminalité et la preuve électronique, avec tous les pays participant à GLACY+
23-25 mai 2017	Nu'alofa, Tonga	Atelier régional sur la cybercriminalité et la preuve électronique pour les procureurs du réseau PILON

26-mai 2017	Nu'alofa, Tonga	Conseils sur la rationalisation des procédures d'entraide judiciaire liées à la cybercriminalité et la preuve électronique
5-8 juin 2017	Madrid, Espagne	Participation au Groupe de travail eurasien d'INTERPOL sur la cybercriminalité pour des chefs de service et participation à la réunion opérationnelle en marge concernant la compromission des messageries commerciales
7-9 juin 2017	Strasbourg, France	17e Plénière T-CY
3-5 juil 2017	Nu'alofa, Tonga	Mission consultative sur les capacités des CERT, les lab. d'informatique forensique et la coopération public-privé
6 juil 2017	Nu'alofa, Tonga	Atelier sur les systèmes de signalement de cybercriminalité et la collecte et le suivi des statistiques de justice pénale sur la cybercriminalité et la preuve électronique.
10-13 juil 2017	Nu'alofa, Tonga	Développement des enquêtes en matière de cybercriminalité, capacités en informatique forensique combiné avec des ateliers dans le pays et des conseils sur la coopération interservices et les partenariats privé public pour lutter contre la cybercriminalité
25-29 sept 2017	Nu'alofa, Tonga	Cours introductif de formation judiciaire FdF sur la cybercriminalité et la preuve électronique pour les juges, les procureurs et les avocats et adaptation de supports pédagogiques au contexte local, avec la participation de pays sélectionnés de la Région Pacifique
6-10 nov 2017	Suva, Fidji	Participation à la Formation INTERPOL cybercriminalité pour la Région Pacifique
20-24 nov 2017	Singapour	INTERPOL, Session de développement pour les instructeurs
27-29 nov 2017	Strasbourg, France	18e Plénière T-CY
11-13 déc 2017	Cebu, Philippines	Atelier international sur les stratégies de formation judiciaires sur la cybercriminalité et la preuve électronique
7-8 mars 2018	La Haye, Pays-Bas	Conférence internationale conjointe CdE/Eurojust sur la coopération judiciaire en matière de cybercriminalité
12-16 mars 2018	Hong Kong	Participation au the Cyber Command Course organisée par la Police de Hong Kong
27-30 mars 2018	Chisinau, Moldova	Participation à la Réunion régionale: exercice de coopération cybercriminalité organisé dans le cadre du projet Cybercrime@EAP 2018
8-10 mai 2018	Téhéran, Iran	Participation au Groupe de travail eurasien d'INTERPOL sur la cybercriminalité pour des Chefs de Services
14-18 mai 2018	Vienne, Autriche	Commission des Nations unies pour la prévention du crime et la justice pénale
12-15 juin 2018	Nu'alofa, Tonga	Atelier régional cybercriminalité (PILON)
18-22 juin 2018	Singapour	INTERPOL, Session de développement pour les instructeurs
9-13 juil 2018	Strasbourg, France	19ePlénière T-CY et Conférence Octopus
20-24 août 2018	Nu'alofa, Tonga	Cours ECTEG, en parallèle: 1. Forensique en source ouverte et 2. Forensique mobile
27-30 août 2018	Nu'alofa, Tonga	Formation judiciaire avancée sur la cybercriminalité et la preuve électronique pour les juges, les procureurs et les avocats avec la participation de pays de la Région Pacifique

30 août	Nu'alofa, Tonga	Mission consultative dans le pays sur l'intégration/prise en compte transversal de modules de formation dans les programmes des établissements de formation
4-7 sept 2018	Strasbourg, France	Conférence sur l'économie souterraine
27-30 nov 2018	Strasbourg, France	20e Plénière T-CY et Plénière Rédaction du Protocole
18-22 mars 2019	Hong Kong	Participation à la formation Cyber Command Course organisée par la Police de Hong Kong
24-30 mars 2019	Vienne, Autriche	Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité
15-16 avril 2019	Bruxelles, Belgique	Cyber Forum UE
15-17 mai 2019	Nu'alofa, Tonga	Ateliers dans le pays sur la protection des données et les Outils et Services d'INTERPOL combines avec un soutien à la création et au renforcement des points de contact 24/7 pour la cybercriminalité et la preuve électronique
15-17 mai 2019	Bucarest, Roumanie	Atelier de présentation de FREETOOL en coopération avec University College Dublin
27-31 mai 2019	Vanuatu	PILON Atelier régional sur la cybercriminalité et la preuve électronique dans le Pacifique. Coopération internationale
25-27 juin 2019	Singapour	Atelier sur les canaux et voies de coopération internationale en matière de cybercriminalité
8-11 juil 2019	Strasbourg, France	21e Plénière T-CY et 4e Plénière Rédaction du Protocole
10-12 juil 2019	Strasbourg, France	Conférence internationale des formateurs judiciaires sur la cybercriminalité et la preuve électronique
2-6 sept 2019	Manille, Philippines	Formation INTERPOL sur l'analyse des maliciels
3-6 sept 2019	Strasbourg, France	Conférence sur l'économie souterraine
25-27 sept 2019	Nu'alofa, Tonga	Intégration de supports pédagogiques ECTEG dans les instituts de formation des services répressifs et autres organismes de formation pour d'autres professionnels de l'application de la loi
30 sept - 1 oct 2019	La Haye, Pays-Bas	Conférence internationale Eurojust-CdE sur les enquêtes en ligne: Darknet et violence sexuelle en ligne contre les enfants
8 oct 2019	La Haye, Pays-Bas	Réuniondes PC 24/7 des Parties à la Convention de Budapest
9-11 oct 2019	La Haye, Pays-Bas	Conférence Europol-INTERPOL cybercriminalité
18-20 nov 2019	Strasbourg, France	22e Plénière T-CY et 5e Plénière Rédaction du Protocole
26-28 fév2020	Tbilissi, Géorgie	Réunion internationale sur la coopération avec des fournisseurs de services étrangers

4.3 Renforcement des capacités: les enseignements tirés

Des programmes pour renforcer les capacités de la justice pénale concernant la cybercriminalité et la preuve électronique sont mis en œuvre depuis une quinzaine d'années, mais se sont significativement accrus ces sept dernières années. Le résultat de la réunion de 2013 du Groupe d'experts intergouvernementaux des Nations unies sur la cybercriminalité semble avoir contribué à cette expansion.

L'expérience montre que la consolidation des capacités:

- fonctionne, répond aux besoins et a un impact en termes
  - de législation assortie de protections,
  - d'enquêtes et procédures pénales,
  - de coopération public/privé, interservices et internationale,
  - de formation durable;
- facilite la coopération et les synergies pluri-acteurs;
- procure des avantages en matière de développement humain et concourt aux Objectifs de développement durable;
- contribue à combler la fracture numérique;
- s'appuie sur un large soutien international et peut contribuer à surmonter les clivages politiques.

5 Conclusion

N'importe quel pays peut utiliser la Convention de Budapest comme ligne directrice, liste de contrôle ou modèle pour ses lois et un grand nombre le font déjà. Cependant, devenir Partie à ce traité procure des avantages supplémentaires pour ce qui est de la coopération formelle et informelle ainsi que de la consolidation des capacités:

- La convention fournit une **base juridique pour la coopération internationale** en matière de cybercriminalité et de preuve électronique. La section III du traité prévoit des dispositions générales et spécifiques de coopération entre les Parties « dans la plus grande mesure possible » non seulement pour ce qui est de la cybercriminalité (infractions à l'encontre et au moyen d'ordinateurs) mais aussi pour ce qui concerne tout crime impliquant des preuves électroniques. Les Parties font amplement usage de ce cadre dans la pratique.
- Les Parties sont **membres du Comité de la Convention sur la cybercriminalité (T-CY)** et partagent des informations et des expériences, évaluent la mise en œuvre de la Convention, interprètent la Convention au moyen des notes d'orientation, ou préparent des formulaires-types pour des demandes d'entraides et autres outils pour faciliter l'application du traité afin de combattre plus efficacement la cybercriminalité. Par expérience, il semble que les nouvelles Parties sont en mesure de partager de nouvelles connaissances avec d'autres membres et rapidement de participer activement aux réunions et d'occuper des positions de premier plan au sein du T-CY.
- Grâce au T-CY, les Parties contribuent à faire évoluer la Convention de Budapest, par exemple, sous la forme de Notes d'orientation ou de Protocoles additionnels. Ainsi, même si un État n'a pas participé à la négociation du traité d'origine, une nouvelle Partie peut participer aux **négociations des futurs instruments**. Le Deuxième protocole additionnel à venir sur une

coopération internationale renforcée et l'accès aux preuves dans le Cloud donnera aux praticiens des outils supplémentaires et leur permettra de gagner en d'efficacité dans leur coopération avec d'autres Parties ainsi qu'avec des fournisseurs de services.

- L'adhésion à la Convention de Budapest signifie l'adhésion à des **réseaux de praticiens** –au nombre desquels le réseau de points de contact 24/7 - et donc la capacité à fonctionner dans un environnement de coopération caractérisé par la confiance.

- Les Parties à la Convention sont en mesure d'améliorer **leur coopération avec secteur privé**. Il semble que les entités du secteur privé soient plus promptes à coopérer avec les autorités de justice pénale des Parties à la Convention, étant donné que les Parties doivent avoir un cadre juridique national sur la cybercriminalité et la preuve électronique qui respecte les protections de l'article 15.

- Les Etats demandant l'adhésion à la Convention ou qui y ont adhéré peuvent devenir **des pays prioritaires ou des points nodaux pour les programmes de consolidation des capacités (capacity building).** Une telle assistance technique a pour but de faciliter la pleine mise en œuvre de la Convention et de renforcer la capacité à coopérer au niveau international. Les donateurs fournissent régulièrement des ressources pour soutenir les pays dans cette entreprise, en particulier par le Bureau du programme sur la cybercriminalité du Conseil de l'Europe (C-PROC).

Près de vingt ans se sont écoulés depuis l'ouverture de la Convention à la signature, et l'expérience montre qu'il n'y a que des avantages à y adhérer.

Etant donné les bénéfices que procure la Convention de Budapest dans la pratique, et son évolution future grâce au 2e protocole additionnel, ce traité demeurera particulièrement pertinent et étoffera le nombre de ses Etats Parties dans les années à venir.

6 Annexe: Etats Parties, Signataires et Etats invités à adhérer à la Convention de Budapest (situation au 30 juin 2020)

Parties		**Etats signataires ou invités à adhérer**
Andorre	Maroc	Bénin
Argentine	Pays-Bas	Brésil
Arménie	Macédoine du Nord	Burkina Faso
Australie	Norvège	Guatemala
Autriche	Panama	Irlande
Azerbaïdjan	Paraguay	Mexique
Belgique	Pérou	Niger
Bosnie-Herzégovine	Philippines	Nigéria
Bulgarie	Pologne	Afrique du Sud
Cabo-Verde	Portugal	Suède
Canada	Roumanie	Tunisie
Chili	Saint-Marin	
Colombie	Sénégal	
Costa Rica	Serbie	
Croatie	Slovaquie	
Chypre	Slovénie	
République tchèque	Espagne	
Danemark	Sri Lanka	
République dominicaine	Suisse	
Estonie	Tonga	
Finlande	Turquie	
France	Ukraine	
Géorgie	Royaume-Uni	
Allemagne	Etats-Unis d'Amérique	
Ghana		
Grèce		
Hongrie		
Islande		
Irlande		
Israël		
Italie		
Japon		
Lettonie		
Liechtenstein		
Lituanie		
Luxembourg		
Malte		
Ile Maurice		
République de Moldova		
Monaco		
Monténégro		