www.coe.int/TCY

Strasbourg, 15 novembre 2016 T-CY (2016)32

Comité de la Convention cybercriminalité (T-CY)

16e réunion plénière

Strasbourg, 14 – 15 novembre 2016

Rapport de réunion

1 Introduction

La 16e réunion plénière du Comité T-CY, qui s'est tenue à Strasbourg les 14 et 15 novembre 2016, a été présidée par Erick PLANKEN (Pays-Bas) et ouverte par Jan KLEIJSSEN (Directeur de la société de l'information et de la lutte contre la criminalité, DG 1, Conseil de l'Europe). Quelque 170 représentants des États parties et des Observateurs y ont participé.

2 Décisions

Le T-CY a décidé :

Point 2 de l'ordre du jour : état d'avancement des signatures, des ratifications et des adhésions à la Convention de Budapest et à son Protocole

- de prendre acte des mesures en cours sur la voie de la ratification ou de l'adhésion à la Convention ou à son Protocole en Argentine, en Autriche, au Chili, en Colombie, au Costa Rica, au Ghana, au Mexique, à Monaco, au Maroc, aux Philippines, au Sénégal, en Afrique du Sud et aux Tonga ;

- de se féliciter de l'intérêt témoigné pour la Convention de Budapest par les observateurs ad hoc du Bélarus, du Cap Vert, de la Corée, de Singapour et de la Tunisie ;

- d'encourager les Etats ayant signé ou ayant été invités à adhérer à devenir Parties dans les plus brefs délais ;

- de demander au Bureau et au Secrétariat du T-CY que le T-CY effectue des visites dans les États qui ont signé la Convention ou qui ont été invités à y adhérer pour faciliter l'achèvement du processus ;

- d'inviter les membres du T-CY à encourager le processus d'adhésion, y compris en consultation avec leur Représentation respective à Strasbourg, conformément au plan d'activité du T-CY ;

- de rappeler aux États que les instruments d'adhésion ou de ratification doivent inclure les déclarations relatives à la désignation des autorités compétentes en matière d'extradition (article 24 de la Convention de Budapest), aux demandes d'entraide judiciaire (article 27), ainsi qu'aux points de contact joignables vingt-quatre heures sur vingt-quatre, sept jours sur sept (article 35) ;

- d'encourager l'ensemble des États parties à la Convention de Budapest à signer et ratifier le Protocole additionnel (STE 189) relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, ou à y adhérer ;

- d'insister sur l'intérêt et l'utilité de la Convention de Budapest à l'échelle internationale dont ont témoigné les participants au T-CY originaires de tous les continents ;

Point 3 de l'ordre du jour : Informations fournies par les Parties et les Observateurs – tour de table

- de noter avec intérêt les informations fournies sur les politiques en matière de cybercriminalité, les évolutions législatives, la formation ou les grandes affaires par l'Albanie, l'Argentine, l'Arménie, l'Australie, l'Autriche, l'Azerbaïdjan, le Bélarus, la

Belgique, la Bosnie-Herzégovine, la Bulgarie, le Canada, le Cap-Vert, le Chili, la Colombie, le Costa Rica, la Croatie, la République tchèque, le Danemark, la République dominicaine, l'Estonie, la Finlande, la France, la Géorgie, l'Allemagne, le Ghana, la Hongrie, l'Islande, Israël, l'Italie, le Japon, la Corée, la Lettonie, la Lutuanie, le Liechtenstein, la République de Maurice, le Mexique, la Moldova, le Monténégro, Monaco, le Maroc, les Pays-Bas, la Norvège, les Philippines, la Pologne, le Portugal, la Roumanie, la Fédération de Russie, le Sénégal, la Serbie, Singapour, la Slovaquie, la Slovénie, l'Espagne, le Sri Lanka, l'Afrique du Sud, la Suisse, « l'ex-République yougoslave de Macédoine », les Tonga, la Tunisie, la Turquie, l'Ukraine et les États-Unis.

Point 4 de l'ordre du jour : Dialogue avec les organisations internationales (observateurs du T-CY)

- d'accueillir favorablement les informations fournies par l'Union européenne (Commission européenne, EUROJUST et ENISA), le Secrétariat du Commonwealth, INTERPOL, l'Organisation des États américains et l'Organisation pour la sécurité et la coopération en Europe ;

Point 5 de l'ordre du jour : Groupe sur les preuves dans le cloud – examen des résultats préliminaires

- d'accueillir avec satisfaction le rapport du Groupe sur les preuves dans le cloud et, pour ce qui concerne :

  - la recommandation 1, le T-CY décide que les Parties devraient donner suite aux recommandations du T-CY sur l'entraide judiciaire adoptées en décembre 2014 et relevant, pour l'essentiel, de la responsabilité des autorités nationales (recommandations 1 à 15)[1]. Le T-CY doit examiner les progrès réalisés et les programmes de renforcement des capacités, si nécessaire, pour soutenir la mise en œuvre ;

  - la recommandation 2, le T-CY prend note du large soutien apporté au projet de Note d'orientation sur les injonctions de produire des données relatives aux abonnés, telle que révisée lors de la 16e réunion plénière, mais observe que certaines Parties doivent mener des consultations approfondies au sein de leurs capitales. Le T-CY invite les Parties à soumettre des observations écrites, le cas échéant, sur le projet de Note d'orientation (version du 15 novembre 2016) avant le 10 décembre 2016 en vue de son adoption ou de nouvelles consultations. Si de nouvelles consultations s'avèrent nécessaires, les Parties intéressées sont conviées à la réunion du Groupe sur les preuves dans le cloud des 30 et 31 janvier 2017. Les commentaires et observations d'organisations et d'États observateurs sont les bienvenus à tout moment ;

  - la recommandation 3, le T-CY décide d'inviter les Parties et les Observateurs à examiner les procédures nationales concernant l'accès aux informations relatives aux abonnés afin de garantir la mise en œuvre pleine et entière de l'article 18 de la Convention de Budapest ;

  - la recommandation 4, le T-CY décide de prendre des mesures concrètes – dans l'attente de solutions à plus long terme – pour faciliter une coopération plus cohérente entre les fournisseurs de services et les autorités judiciaires pénales, notamment :

[1] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

- que le T-CY organise des réunions annuelles avec les fournisseurs de services ;
- que le Secrétariat du T-CY et le C-PROC tiennent à jour des ressources en ligne sur les politiques et règles de procédure relatives aux fournisseurs dans les Parties ;
- que le C-PROC associe les fournisseurs aux projets de renforcement des capacités ;
- que le T-CY assure la liaison avec l'Union européenne ;

- la recommandation 5, le T-CY convient, sur le principe, de la nécessité d'un protocole additionnel. Pour faciliter une prise de décision formelle du T-CY d'ici juin 2017 dans le but de lancer la rédaction d'un Protocole, le T-CY prolonge le mandat du Groupe sur les preuves dans le cloud et demande que ledit groupe présente au T-CY, au printemps 2017, un projet de mandat pour le processus de rédaction et des informations complémentaires sur des éléments envisageables.

Point 6 de l'ordre du jour : État d'avancement du troisième cycle d'évaluation du T-CY sur l'article 13 relatif aux sanctions et mesures

- de prendre note de l'état d'avancement du rapport d'évaluation du T-CY sur l'article 13 et de l'approche proposée par le Bureau du T-CY ;

- d'inviter le Bureau à préparer un projet de rapport d'évaluation et à le diffuser en mai 2017 pour examen à la 17e réunion plénière du T-CY, qui aura lieu en juin 2017 ;

Point 7 de l'ordre du jour : Suivi du rapport d'évaluation en matière d'entraide judiciaire

- de souligner l'importance d'accroître l'efficience de l'entraide judiciaire en matière de lutte contre la cybercriminalité et de preuves électroniques, et ainsi de donner suite aux recommandations du T-CY adoptées en décembre 2014 ;

- de saluer l'appui fourni pour donner suite aux recommandations du T-CY en matière d'entraide judiciaire dans les pays du Partenariat oriental par le biais du projet conjoint Cybercrime@EAP II de l'Union européenne et du Conseil de l'Europe ;

- d'accueillir favorablement les réponses au questionnaire sur les suites données par les 18 Parties et d'inviter les Parties et les Observateurs qui ne l'ont pas encore fait à adresser leurs réponses au plus tard le 15 décembre 2016 ;

- d'inviter le Bureau du T-CY à présenter un rapport sur les suites données pour examen à la 17e réunion plénière du T-CY en juin 2017 ;

- d'accueillir favorablement l'outil en ligne sur l'entraide judiciaire élaboré par le Conseil de l'Europe au titre de la communauté Octopus et d'inviter les Parties à compléter cet outil par des informations pertinentes ;

- de prendre note des résultats des tests « ping » effectués par le Secrétariat du T-CY pour vérifier le fonctionnement des points de contact joignables vingt-quatre heures sur vingt-quatre, sept jours sur sept, et d'inviter les représentants du T-CY à donner suite au niveau national pour clarifier, si nécessaire, les responsabilités, les coordonnées des points de contact et les procédures ;

Point 8 de l'ordre du jour : Notes d'orientation

- d'adopter la Note d'orientation du T-CY sur les aspects du terrorisme couverts par la Convention de Budapest (T-CY (2016)11) ;

- de prendre note des informations fournies par l'Ukraine sur des cyberattaques visant des infrastructures essentielles ;

Point 9 de l'ordre du jour : Dotation financière du T-CY pour 2016-2017

- de se féliciter des contributions volontaires de l'Estonie, du Japon, de Monaco et des États-Unis concernant le projet Cybercrime@Octopus pour 2016-2017, y compris en vue de soutenir les travaux du TCY ;

- d'appeler les Parties et les Observateurs à fournir des contributions supplémentaires, de préférence non affectées, pour le projet Cybercrime@Octopus, y compris en vue de soutenir les travaux du T-CY ;

Point 10 de l'ordre du jour : Activités des projets de renforcement des capacités et du Bureau du Conseil de l'Europe pour le Programme sur la cybercriminalité (C-PROC)

- de se féliciter de l'envergure croissante des activités de renforcement des capacités mises en œuvre grâce au Bureau du Conseil de l'Europe pour le Programme sur la cybercriminalité (C-PROC) en Roumanie ;

- de remercier les donateurs (Estonie, Japon, Monaco, Roumanie, Royaume-Uni et États-Unis) de leurs contributions volontaires pour le renforcement des capacités ainsi que l'Union européenne pour le financement accordé au titre de programmes conjoints du Conseil de l'Europe et de l'Union européenne ;

- d'appeler le Conseil de l'Europe
  - à présenter à certains Etats parties, Etats signataires et Etats invités à adhérer à la Convention de Budapest l'éventail complet des activités de renforcement des capacités, y compris concernant la formation sur le terrain ;
  - à aider tout État intéressé par la Convention de Budapest à consolider sa législation interne en matière de cybercriminalité et de preuves électroniques ;
  - à contribuer aux activités connexes des organisations partenaires ;

Point 11 de l'ordre du jour : Questions diverses

- de prendre note du soutien vigoureux à la création d'un groupe de travail du T-CY sur le cyberharcèlement et d'autres formes de violence en ligne, en particulier à l'encontre de femmes et d'enfants, sur la base de l'article 1.1.j du Règlement du T-CY, et

  - de charger le Groupe d'étudier le sujet sous forme d'exercice de cartographie, notamment d'approches comparatives de la législation et de documentation sur les bonnes pratiques, en vue de présenter les résultats intermédiaires à la 17e réunion plénière et un rapport final à la 18e réunion plénière du T-CY ;
  - de nommer Markko KUNNAPU (Estonie), Erik PLANKEN (Pays-Bas), Gareth SANSOM (Canada), Betty SHAVE (consultante), Cristina SCHULMAN (Roumanie), Eirik Tronnes HANSEN (Norvège), Lilija OMELJANCUK (Lituanie) et Branislav KADLECIK (Slovaquie) ;
  - de saluer le fait que d'autres parties soient disposées à fournir des contributions écrites ;

- d'organiser des réunions en conjonction avec les réunions du Bureau du T-CY, sans remboursement des dépenses autres que celles prévues pour le Bureau, excepté si des contributions volontaires viennent à être disponibles ;

Point 12 de l'ordre du jour : Prochaine réunion du T-CY

- d'organiser la 17e réunion plénière du T-CY à Strasbourg au cours de la période du 19 au 21 juin 2017[2], sous réserve de financement.

[2] Les dates de la réunion de la 17e plénière ont été changes du 7 au 9 juin 2017.

3 Annexes

3.1 Ordre du jour annoté

(Veuillez noter que les points de l'ordre du jour marqués d'un * relèvent de la décision des membres représentant les Parties contractantes à la Convention de Budapest)

1. Ouverture de la 16e réunion plénière et adoption de l'ordre du jour
2. Etat des signatures et des ratifications de la Convention de Budapest et de son Protocole et état des adhésions à ces deux instruments Les participants sont invités à examiner l'état des signatures, des ratifications ou des adhésions par divers pays.
3. Informations communiquées par les Parties et les observateurs – Tour de table - Les participants sont invités à donner des informations sur les évolutions législatives, les principaux cas, les événements importants, la formation dispensée à d'autres pays, y compris par des organisations internationales, etc. Les signataires et les Etats invités à adhérer sont priés de rendre compte des progrès réalisés en vue de la ratification de la Convention de Budapest sur la cybercriminalité et de son Protocole sur la xénophobie et le racisme et de l'adhésion à ces instruments. Brèves interventions (deux minutes par intervention).
4. Dialogue avec des organisations internationales (observateurs du T-CY) Les représentants des organisations internationales ayant le statut d'observateur auprès du T-CY sont invités à présenter les activités pertinentes et à engager un dialogue avec les membres du T-CY. Sont observateurs la Commission de l'Union africaine, le Secrétariat du Commonwealth, l'Union européenne (Commission, ENISA, EUROJUST, EUROPOL), INTERPOL, l'UIT, l'OEA, l'OCDE, l'OSCE, l'ONUDC et le G7.
5. Groupe sur les preuves dans le nuage : Examen des résultats Le T-CY est invité à examiner: - Le rapport final du Cloud Evidence Group; - La note d'orientation provisoire sur les injonctions de produire des données relatives aux abonnés (Article 18 Convention de Budapest) en vue d'adoption; - Recommandations proposées par le Cloud Evidence Group dans son rapport final en vue de son adoption; - Suivi par le T-CY.
6. Statut du 3e cycle d'évaluation du T-CY consacré à l'article 13 (sanctions et mesures) La 11ème réunion plénière du a décidé de consacrer le 3ème cycle d'évaluation à l'article 13 (sanctions et mesures) et a adopté le questionnaire. Le Bureau du T-CY informera sur le statut en cours du rapport d'évaluation.
7. Suivi du rapport d'évaluation sur l'entraide judiciaire

Le rapport d'évaluation sur l'entraide judiciaire invite les Parties à suivre les recommandations relevant de la responsabilité des autorités nationales et faire un rapport au T-CY au plus tard 18 mois après l'adoption du présent rapport sur les mesures prises pour permettre la T-CY, conformément aux règles de procédure (article 2.1.g), afin d'examiner les progrès accomplis.

Le Secrétariat fera un compte rendu sur les réponses reçues de la part des Parties au questionnaire concernant le suivi des recommandations sur l'entraide judiciaire.

Le Secrétariat présentera l'outil sur la coopération internationale.

8. Notes d'orientation du T-CY

Le T-CY est invité à examiner :

- La Note d'orientation sur le terrorisme en vue de son adoption;
- Etude de cas sur les attaques contre les centrales électriques.

9. Dotations financières du TCY pour 2016-2017

Le Secrétariat informera les participants de l'état des ressources financières dont disposera le T-CY en 2016 et 2017.

A la suite de la décision sur le financement du T-CY prise à la 9e réunion plénière, les Parties sont invitées à envisager d'apporter une aide financière au T-CY par des contributions volontaires au projet CyberCrime@Octopus.

10. Activités des projets de renforcement des capacités et le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC)

Le Secrétariat donnera des renseignements à jour sur les projets de renforcement des capacités et sur le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) de Bucarest.

11. Divers

- T-CY working group on cyber bullying and other forms of online violence against women and children

Le Bureau propose de créer un groupe de travail – fondé sur l'Article 1.1.j du Règlement – afin d'étudier le sujet sous la forme d'un inventaire comprenant des approches comparatives de législations ainsi que la documentation de bonnes pratiques. Une étude plus ciblée pourrait suivre par la suite. Le groupe de travail se réunirait en conjonction avec la prochaine réunion du Bureau. Les résultats provisoires de cet inventaire pourraient être présentés à la prochaine réunion du T-CY en juin 2017. Markko KUNNAPU (Estonie), Eirik PLANKEN (Pays-Bas), Gareth SANSOM (Canada), Betty SHAVE (Consultant), Cristina SCHULMAN (Roumanie) et Eirik Tronnes HANSEN (Norvège) se sont portés volontaires pour ce groupe.

12. La prochaine réunion du T-CY*

Les membres du T-CY sont invités à se prononcer concernant la proposition de tenir la 17e réunion plénière du 19 au 21 juin 2017.

Cette proposition est soumise à la disponibilité de fonds.

3.2 Note d'Orientation sur les Injonctions de production concernant les abonnés (tel que révisé lors de la 16ème réunion plénière)

www.coe.int/TCY

Strasbourg, version 15 novembre 2016 T-CY(2015)16

Comité de la Convention de la Cybercriminalité (T-CY)

Note d'orientation T-CY #10 (PROJET)

Injonctions de production concernant des informations sur les abonnés

(Article 18 Budapest Convention)

Proposition révisée telle que discutée pat le T-CY lors de sa 16ème réunion plénière (14-15 novembre 2016)

Contact

Alexander Seger
Secrétaire du Comité de la Convention Cybercriminalité (T-CY)
Direction Générale des Droits de l'Homme et de l'État de droit
Conseil de l'Europe, Strasbourg, France

Tél +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

A sa 8e Plénière (décembre 2012), le Comité de la Convention sur la Cybercriminalité (T-CY) a décidé de publier des Notes d'orientation visant à faciliter l'usage et la mise en œuvre effectives de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des développements du droit, des politiques et des techniques[3].

Les Notes d'orientation reflètent une analyse de l'application de la Convention partagée par toutes ses Parties.

La présente Note[4] traite la question des injonctions de produire relatives à des informations sur les abonnés visées à l'article 18, à savoir dans des situations où :

- une personne à qui il est fait injonction de produire des données informatiques spécifiées est présente sur le territoire d'un État Partie (Article 18.1.a) ;[5]
- un fournisseur de services à qui il est fait injonction de produire des informations sur un abonné propose un service sur le territoire de l'État Partie sans forcément être situé sur le territoire en question (Article 18.1.b).

Il est pertinent de publier une Note d'orientation sur ces aspects de l'Article 18, étant donné :

- que des informations sur des abonnés sont le plus souvent recherchées dans des enquêtes pénales ;
- que l'article 18 a une compétence nationale ;
- que, du fait de l'essor du « cloud computing » et du stockage de données à distance, les autorités compétentes cherchant à accéder à des données informatiques spécifiées - en particulier à des informations relatives à l'abonné – pour mener des enquêtes pénales et des poursuites se sont heurtées à un certain nombre de difficultés ;
- qu'actuellement, les pratiques et les procédures, ainsi que les conditions et les sauvegardes en matière d'accès à des informations concernant les abonnés varient considérablement d'un État Partie de la Convention à l'autre ;
- qu'il est nécessaire de traiter les problèmes qui se posent en matière de vie privée et de protection des données à caractère personnel, pour ce qui est du fondement juridique de la juridiction relative aux services offerts sur le territoire d'un État partie sans que le fournisseur de services soit établi sur ce territoire, ainsi qu'en ce qui concerne l'accès à des données stockées dans des juridictions étrangères ou en des lieux inconnus ou multiples « dans le cloud » ;
- que la possibilité de faire exécuter des injonctions de produire nationales à l'encontre de fournisseurs établis hors du territoire d'un État Partie pose d'autres problèmes qui ne peuvent être traités dans le cadre d'une note d'orientation et que les Etats Parties peuvent demander les informations relatives aux abonnés par le biais de l'entraide judiciaire.

[3] Voir le mandat du T-CY (article 46 de la Convention de Budapest).
[4] Cette Note d'orientation s'appuie sur les travaux du Groupe sur les Preuves dans le Cloud.
[5] Il est important de rappeler que l'article 18.1.a de la Convention de Budapest n'est pas limité aux seules informations relatives aux abonnés, mais qu'il concerne tout type de données informatiques spécifiées. En revanche, la présente Note d'orientation ne traite que la seule production d'informations concernant les abonnés.

La mesure visée à l'article 18 doit s'appliquer dans des enquêtes et procédures pénales spécifiques relevant du champ d'application de l'article 14 de la Convention de Budapest. Les injonctions doivent donc être délivrées dans des cas spécifiques en ce qui concerne des abonnés spécifiés.

2 Article 18 de la Convention de Budapest[6]

2.1 Texte de la disposition

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sons son contrôle relatives aux abonnés et concernant de tels services.

Extrait du Rapport explicatif :

173. En vertu du paragraphe 1(a), toute Partie doit veiller à ce que ses autorités répressives compétentes aient le pouvoir d'ordonner à une personne présente sur son territoire de communiquer des données électroniques spécifiées, stockées dans un système informatique ou un support de stockage, qui sont en possession ou sous le contrôle de cette personne. L'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé en possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la partie ayant ordonné leur communication (par exemple, sous réserve des privilèges applicables, toute personne qui reçoit l'injonction de produire des informations stockées sur son compte au moyen d'un service de stockage en ligne à distance, droit produire ces informations). Par ailleurs, la simple possibilité technique d'accéder à des données stockées à distance (par exemple, la possibilité, pour un utilisateur, d'accéder, par une liaison du réseau, à des données stockées à distance qui ne sont pas sous son contrôle légitime) ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Dans certains États, la notion juridique de « possession » recouvre la possession matérielle et de droit de manière assez large pour satisfaire à cette exigence de « possession ou de contrôle ».

En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire, de « communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services ». De même qu'au paragraphe 1(a), l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement ou à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression « qui se rapportent à ces services » signifie que le pouvoir en

[6] Voir l'annexe pour l'article 18 et les extraits *in extenso* du Rapport explicatif.

question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction[7].

L'exigence selon laquelle les données relatives aux abonnés doivent être produites concerne les services d'un fournisseur offerts sur le territoire de l'Etat Partie, même si ces services sont fournis via un domaine géographique technique faisant référence à une autre juridiction.

- les données relatives aux abonnés devant être produites concernent les services d'un fournisseur offerts sur le territoire de la Partie, même si ces services sont fournis

2.2 Que recouvre l'expression « données relatives aux abonnés » ?

L'expression « données relatives aux abonnés » est définie à l'article 18.3 de la Convention de Budapest :

> 3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
>
> a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
>
> b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
>
> c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

L'obtention de données relatives aux abonnés constitue une ingérence moins contraignante à l'égard des droits individuels que l'obtention de données relatives au trafic ou au contenu.

2.3 Qu'est-ce qu'un « fournisseur de services » ?

La Convention de Budapest sur la cybercriminalité prévoit une notion large du « fournisseur de services », qui est défini à l'article 1.c de la Convention de Budapest :

Aux fins de la présente Convention, l'expression :

> c. « fournisseur de services » désigne :
>
> i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;
>
> ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

L'article 18.1.b s'applique pour tout fournisseur de services présent sur le territoire de la partie ou offrant des services sur ce dernier[8].

[7] Paragraphe 173 du Rapport explicatif.

[8] Les instruments de l'Union européenne font la distinction entre fournisseurs de services de communication électroniques et fournisseurs de services dans la société de l'Internet. La notion de « fournisseur de services » visée à l'article 1.c de la Convention de Budapest recouvre ces deux aspects.

3. Interprétation par le T-CY de l'article 18 de la Convention de Budapest en ce qui concerne les données relatives aux abonnés

3.1 Portée de l'article 18.1.a

- La portée est large : une « personne » (notion qui peut englober celle de « fournisseur de services) physiquement ou légalement présente sur le territoire de la Partie.
- Pour ce qui est des données informatiques, la portée est large mais n'est pas indéfinie : toutes données informatiques « spécifiées » (ce qui entraîne que l'article 18.1.a n'est pas limité aux « données relatives aux abonnés » et couvre tout type de données informatiques).
- Les données informatiques spécifiées sont en possession ou sous le contrôle de cette personne.
- Les données informatiques spécifiées sont stockées dans un système informatique ou un moyen de stockage informatique.
- L'injonction de produire est émise et exécutable par les autorités compétentes dans la Partie dans la juridiction de laquelle l'injonction est demandée/accordée.

3.2 Portée de l'article 18.1.b

La portée de l'article 18.1.b est plus étroite que celle de l'article 18.1.a. L'alinéa b :

- est limité au « fournisseur de services »[9] ;
- est limité aux « données relatives aux abonnés » ;
- le fournisseur de services destinataire de l'injonction n'est pas nécessairement présent physiquement sur le territoire, mais les services sont prêtés sur le territoire et le fournisseur de services peut donc être considéré comme établi sur le territoire.

3.3 Compétence

L'article 18.1.b est limité aux circonstances où l'autorité de justice pénale délivrant l'injonction de produire est compétente pour l'infraction en vertu de l'article 22 de la Convention de Budapest[10].

---

[9] Le concept de « personne » est plus large que celui de « fournisseur de services », même si un « fournisseur de services » peut être une « personne ».

[10] Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 – 11 de la présente Convention, lorsque l'infraction est commise :
   a sur son territoire ; ou
   b à bord d'un navire battant pavillon de cette Partie ; ou
   c à bord d'un aéronef immatriculé dans cette Partie ; ou
   d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies aux paragraphes 1b – 1d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnées à l'article 24, paragraphe 1 de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de décider quelle est celle qui est le mieux à même d'exercer les poursuites.

Seront en général concernées les situations où l'abonné est ou était résident ou présent sur le territoire lors de la commission de l'infraction.

La présente interprétation de l'article 18 ne préjuge pas de compétences plus larges ou supplémentaires en vertu du droit interne des Parties.

L'accord à la présente Note d'orientation n'implique ni le consentement à l'application extraterritoriale d'une ordonnance de production nationale délivrée par un autre État ni ne créer de nouvelles obligations ou relations entre les Etats Parties.

3.4 Quelles sont les caractéristiques d'une « injonction de produire » ?

Une « injonction de produire » au sens de l'article 18 est une mesure nationale qui doit être prise selon le droit pénal interne. Elle est limitée par la compétence d'adjudication et d'exécution de la Partie dans laquelle l'injonction est délivrée.

Les injections de produire relevant de l'article 18 portent « sur des données informatiques ou des informations relatives à l'abonné qui sont en la possession ou sous le contrôle d'une personne ou d'un fournisseur de services. La mesure n'est applicable que pour autant que la personne ou le fournisseur de services conserve ces données ou ces informations. Certains fournisseurs de services, par exemple, ne gardent pas trace des usagers de leurs services. »[11]

Selon le paragraphe 171 du rapport explicatif de la Convention de Budapest, les injonctions de produire constituent une mesure souple qui est moins contraignante que la perquisition ou la saisie ou encre d'autres pouvoirs coercitifs et qui peuvent servir de base juridique appropriée pour la coopération avec les fournisseurs de services.

3.4 Quel effet produit la localisation des données ?

Le fait que les informations relatives aux abonnés soient stockées dans une autre juridiction ne fait pas obstacle à l'application de l'article 18 de la Convention de Budapest. Le Rapport explicatif précise :

- concernant l'article 18.1.a, que « l'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la Partie ayant ordonné leur communication. »[12] ;

- concernant l'article 18.1.b, que « l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement et à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société) »[13].

Ceci couvre les situations dans lesquelles la facilité de stockage est située hors du territoire de l'Etat Partie.

---

[11] Paragraphe 172 du Rapport explicatif.
[12] Paragraphe 173 du Rapport explicatif. Une « personne » au sens de l'article 18.1.a de la Convention de Budapest peut être une personne physique ou une personne morale, notamment un fournisseur de services.
[13] Paragraphe 173 du Rapport explicatif.

En ce qui concerne l'article 18.1.b, une des situations courantes est celle où un fournisseur de services a son siège dans une juridiction, applique le régime juridique d'une deuxième juridiction et stocke les données dans une troisième. Des données peuvent être répliquées dans plusieurs juridictions ou se déplacer entre plusieurs juridictions à la discrétion du fournisseur de services sans information ni contrôle de l'abonné. Les régimes juridiques admettent de plus en plus, tant dans la sphère du droit pénal qu'en matière de protection de la vie privée et des données, que la localisation des données n'est pas le facteur déterminant pour établir la compétence juridictionnelle.

3.6 Que recouvre la notion de « offrant des prestations sur le territoire d'une Partie » ?

L'essor du « Cloud computing » a amené à s'interroger sur le point de savoir quand un fournisseur de services est considéré comme offrant ses prestations sur le territoire de la Partie et étant par là-même tenu d'obéir à une injonction nationale de produire des données relatives à un abonné. Cette question a fait l'objet d'une série d'interprétation par les tribunaux dans diverses juridictions, dans des affaires civiles comme pénales.

Le T-CY est parvenu à la conclusion qu'en ce qui concerne l'article 18.1.b, un fournisseur de services « offre un service sur le territoire de la partie » lorsque :

- le fournisseur de services permet à des personnes sur le territoire de la Partie de s'abonner à ses services (et ne bloque pas, par exemple, l'accès à ces services) ;

et

- oriente ses activités vers ces abonnés (par exemple, en faisant localement de la publicité ou en faisant de la publicité dans la langue du territoire de la Partie), ou utilise les informations relatives aux abonnés (ou les données de trafic associées) dans le cours de ses activités, ou interagit avec des abonnés dans l'Etat Partie.

Un Etat Partie peut exiger que pour l'application d'une ordonnance de production nationale, le service soit offert de manière telle que le fournisseur puisse être considéré comme étant établi dans le territoire, ou qu'il ait dans le cas contraire un lien réel et substantiel pour le territoire de l'Etat Partie.

3.7 Considérations générales et sauvegardes

L'on part du principe que les Parties à la Convention forment une communauté de confiance et que les principes de l'état de droit et droits de l'homme sont respectés conformément aux dispositions de l'article 15 de la Convention de Budapest.

> Article 15.3 - Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.

3.8 Application de l'article 18 en ce qui concerne les données relatives aux abonnés

La production de données relatives aux abonnés en vertu de l'article 18 de la Convention de Budapest peut donc être ordonnée si les critères suivants sont remplis dans une enquête pénale spécifique et pour des abonnés spécifiés :

SI
l'autorité de justice pénale est compétente pour l'infraction conformément à l'article 22 de la

<table>
<tr><td colspan="3">Convention de Budapest ;</td></tr>
<tr><td colspan="3">ET SI
le fournisseur de services possède ou contrôle les données relatives à l’abonné ;</td></tr>
<tr><td colspan="3">ET SI</td></tr>
<tr><td>Article 18.1.a
Le fournisseur de services est physiquement ou légalement présent ou représenté sur le territoire de la Partie. Par exemple, le fournisseur de services est enregistré en tant que fournisseur de services de communication électroniques, ou des serveurs ou parties de son infrastructures sont situés sur le territoire de la Partie.</td><td>OU</td><td>Article 18.1.b
Le fournisseur de services « offre un service sur le territoire de la Partie », autrement dit :
- le fournisseur de services permet à des personnes sur le territoire de la Partie de s’abonner à ses services,[14] ET
- oriente ses activités vers les abonnés, ou utilise les informations relatives aux abonnés dans le cours de ses activités, ou interagit avec des abonnés sur le territoire de la Partie ;</td></tr>
<tr><td colspan="3">ET SI</td></tr>
<tr><td></td><td></td><td>- les données relatives aux abonnés devant être produites concernent les services d’un fournisseur offerts sur le territoire de l’Etat Partie, même si ces services sont fournis via un domaine géographique technique faisant référence à une autre juridiction.</td></tr>
</table>

4. Déclaration du T-CY

Le T-CY s’accorde à dire que les positions présentées ci-dessus constituent le socle commun sur lequel s’entendent les Parties en ce qui concerne la portée et les éléments de l’article 18 de la Convention de Budapest concernant la production de données relatives aux abonnés.

5 Annexes : Extraits de la Convention de Budapest

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

[14] Veuillez noter le Paragraphe 183 Rapport explicatif : « La mention d’un « contrat ou arrangement de service » s’entend au sens très large de toute type de relation sur la base duquel un abonné utilise les services d’un fournisseur ».

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Rapport explicatif

170. Au paragraphe 1 de cet article, les Parties sont invitées à habiliter leurs autorités compétentes à contraindre une personne présente sur leur territoire à fournir des données informatiques stockées spécifiées ou un fournisseur de services offrant ceux-ci sur le territoire d'une Partie à communiquer les données relatives à l'abonné. Les données en question sont des données stockées ou existantes et n'englobent pas les données qui n'existent pas encore, comme les données relatives au trafic ou au contenu se rapportant aux communications futures. Au lieu de requérir des États qu'ils appliquent systématiquement des mesures contraignantes à l'égard de tiers, telles que la perquisition et la saisie de données, il est essentiel que les États disposent dans leur droit interne d'autres pouvoirs d'enquête qui leur donnent un moyen moins intrusif d'obtenir des informations utiles pour les enquêtes pénales.

171. Une « injonction de produire » constitue une mesure souple que les services répressifs peuvent mettre en oeuvre dans bien des situations, en particulier dans les cas où il n'est pas nécessaire de recourir à une mesure plus contraignante ou plus onéreuse. L'instauration d'un tel mécanisme procédural sera aussi utile pour les tiers gardiens des données qui, tels les fournisseurs d'accès Internet, sont souvent disposés à collaborer avec les services de lutte contre la criminalité sur une base volontaire en leur fournissant les données sous leur contrôle, mais préfèrent disposer d'une base juridique appropriée pour apporter cette aide, les déchargeant de toute responsabilité contractuelle ou autre.
172. L'injonction de produire porte sur des données informatiques ou des informations relatives à l'abonné qui sont en la possession ou sous le contrôle d'une personne ou d'un fournisseur de services. La mesure n'est applicable que pour autant que la personne ou le fournisseur de services conserve ces données ou ces informations. Certains fournisseurs de services, par exemple, ne gardent pas trace des usagers de leurs services.

173. En vertu du paragraphe 1(a), toute Partie doit veiller à ce que ses autorités répressives compétentes aient le pouvoir d'ordonner à une personne présente sur son territoire de communiquer des données électroniques spécifiées, stockées dans un système informatique ou un support de stockage, qui sont en possession ou sous le contrôle de cette personne. L'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la Partie ayant ordonné leur communication (par exemple, sous réserve des privilèges applicables, toute personne qui reçoit l'injonction de produire des informations stockées sur son compte au moyen d'un service de stockage en ligne à distance, doit produire ces informations). Par ailleurs, la simple possibilité technique d'accéder à des données stockées à distance (par exemple, la possibilité, pour un utilisateur, d'accéder, par une liaison du réseau, à des données stockées à distance qui ne sont pas sous son contrôle légitime) ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Dans certains Etats, la notion juridique de « possession » recouvre la possession

matérielle et de droit de manière assez large pour satisfaire à cette exigence de « possession ou de contrôle ».

En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire, de « communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services ». De même qu'au paragraphe 1(a), l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement et à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression « qui se rapportent à ces services » signifie que le pouvoir en question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction.

174. Les conditions et sauvegardes visées au paragraphe 2 de l'article peuvent, en fonction du droit interne de chaque Partie, exclure des données ou informations confidentielles. Une Partie pourra prescrire des choix différents concernant les conditions, les autorités compétentes et les sauvegardes à propos de la communication de tel ou tel type de données informatiques ou de données relatives à l'abonné détenues par telle ou telle catégorie de personnes ou de fournisseurs de services. Ainsi, par exemple, en ce qui concerne certains types de données telles que les données relatives à l'abonné connues de tous, une Partie pourra habiliter les agents de la force publique à émettre une injonction de ce genre tandis qu'une ordonnance d'un tribunal pourrait être requise dans d'autres situations. En revanche, dans certaines situations, une Partie pourrait exiger ou se voir imposer par des sauvegardes relevant des droits de l'homme d'exiger qu'une injonction de produire soit émise uniquement par une autorité judiciaire afin de pouvoir obtenir certains types de données. Les Parties pourraient souhaiter limiter la divulgation de ces données aux fins de lutte contre la criminalité aux situations dans lesquelles une injonction de produire en vue de la divulgation de ces données a été rendue par une autorité judiciaire. Par ailleurs, le principe de proportionnalité introduit une certaine souplesse dans l'application de la mesure, par exemple en l'excluant dans les affaires sans gravité.

175. Les Parties peuvent également envisager d'instaurer des mesures relatives à la confidentialité. L'article ne mentionne pas spécifiquement la confidentialité, ceci afin de préserver le parallélisme avec le monde non électronique, où la confidentialité n'est en général pas imposée en ce qui concerne les injonctions de produire. Toutefois, dans le monde électronique, et en particulier le monde en ligne, une injonction de produire peut parfois servir de mesure préliminaire dans le cadre d'une enquête, précédant d'autres mesures telles que la perquisition et la saisie ou l'interception en temps réel d'autres données. Le succès de l'enquête pourrait dépendre de la confidentialité.

176. S'agissant des modalités de production, les Parties peuvent instaurer l'obligation de produire des données informatiques ou des informations relatives à l'abonné de la manière spécifiée dans l'injonction. Elles pourraient ainsi mentionner le délai dans lequel la divulgation doit intervenir ou la forme sous laquelle les données doivent être divulguées (« texte en clair », en ligne, sortie imprimée ou disquette).

177. L'expression « informations relatives aux abonnés » est définie au paragraphe 3. En principe, elle désigne toute information détenue par l'administration d'un fournisseur de services et qui se rapporte à un abonné à ses services. Les données relatives aux abonnés peuvent être contenues sous forme de données informatiques ou sous toute autre forme, telle que des documents-papier. Comme les informations relatives aux abonnés ne se présentent pas toutes sous la forme de données informatiques, une disposition spéciale a été insérée dans l'article pour tenir compte de ce type d'informations. Le terme d'« abonné » vise à englober de nombreuses catégories de clients des fournisseurs de services : personne ayant payé un abonnement, client qui paie au fur et à mesure les services qu'il utilise, personne bénéficiant de services gratuits. Sont aussi incluses les informations concernant les personnes habilitées à utiliser le compte de l'abonné.

178. Dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires dans deux situations spécifiques. Premièrement, elles sont nécessaires pour déterminer les services et mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, tels que le type de service téléphonique utilisé (par exemple téléphonie mobile), le type de services connexes utilisé (renvoi automatique d'appel, messagerie téléphonique, etc.), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. D'autres informations relatives aux abonnés, telles que les informations commerciales figurant dans les dossiers de facturation et de paiement de l'abonné, peuvent également être utiles aux enquêtes pénales surtout lorsque l'infraction faisant l'objet de l'enquête concerne un cas de fraude informatique ou un autre délit économique.

179. En conséquence, les informations relatives aux abonnés recouvrent différents types d'informations sur l'utilisation d'un service et l'usager de ce service. S'agissant de l'utilisation du service, l'expression désigne toute information, autre que des données relatives au trafic ou au contenu, permettant d'établir le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période pendant laquelle l'intéressé a été abonné au service en question. L'expression « dispositions techniques » désigne l'ensemble des mesures prises pour permettre à l'abonné de profiter du service de communication offert.
Ces dispositions incluent notamment la réservation d'un numéro ou adresse technique (numéro de téléphone, adresse de site Web ou nom de domaine, adresse électronique, etc.) ainsi que la fourniture et l'enregistrement du matériel de communication utilisé par l'abonné (appareils de téléphonie, centres d'appel ou réseaux locaux).

180. Les informations relatives aux abonnés ne sont pas limitées aux informations se rapportant directement à l'utilisation du service de communication. Elles désignent également toutes les informations, autres que des données relatives au trafic ou au contenu, qui permettent d'établir l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'utilisateur, et tout autre numéro d'accès et les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou arrangement de service entre l'abonné et le fournisseur de services. Elles désignent en outre toute autre information, autre que des données relatives au trafic ou au contenu, relative à l'endroit où se trouvent les équipements de communication, information disponible sur la base d'un contrat ou arrangement de service. Cette dernière information peut n'avoir d'intérêt pratique que dans le cas d'équipements non portatifs, mais le fait de savoir si les équipements en question sont portatifs ou de connaître l'endroit où ils se trouveraient (sur la base de l'information fournie en vertu du contrat ou de l'arrangement de service) peut être utile à l'enquête.

181. Cet article ne fait toutefois pas obligation aux fournisseurs de services de conserver des données sur leurs abonnés. Et les fournisseurs ne seront pas non plus tenus, en vertu de la Convention, de s'assurer de l'exactitude desdites données. En d'autres termes, les fournisseurs de services ne sont pas astreints à enregistrer les données relatives à l'identité des utilisateurs des télécartes donnant accès aux services radiotéléphoniques mobiles. Ils ne sont pas non plus obligés de vérifier l'identité des abonnés ou de s'opposer à l'emploi de pseudonymes par les utilisateurs de leurs services.

182. Les pouvoirs et procédures faisant l'objet de la présente section étant instaurés aux fins d'enquêtes ou de procédures pénales spécifiques (article 14), les injonctions de produire sont appelées à être utilisées dans des affaires individuelles concernant le plus souvent un abonné. Ainsi, par exemple, sur la base de la mention du nom de telle ou telle personne dans l'injonction de produire, un numéro de téléphone ou une adresse électronique peuvent être demandés. Sur la base d'un certain numéro de téléphone ou d'une certaine adresse électronique, le nom et l'adresse de l'abonné peuvent être demandés. La mention susvisée n'autorise pas les Parties à rendre une ordonnance aux fins de divulgation de quantités non sélectives d'informations relatives aux abonnés par un fournisseur de services relatives à des groupes d'abonnés, par exemple aux fins d'extraction de données.

183. La mention d'un « contrat ou arrangement de service » s'entend au sens très large de tout type de relation sur la base duquel un abonné utilise les services d'un fournisseur.

3.5 Note d'orientation sur les aspects du terrorisme couverts par la Convention de Budapest

www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, version 15 novembre 2016 T-CY(2016)11

Comité de la Convention Cybercrime (T-CY)

Note d'orientation #11 du T-CY
Aspects du terrorisme
couverts par la Convention de Budapest

Adoptée par la 16e Plénière du T-CY (14-15 novembre 2016)

Contact :

Alexander Seger
Secrétaire exécutif du Comité de la Convention sur la cybercriminalité
Direction Générale des droits de l'homme et de l'Etat de droit
Conseil de l'Europe, Strasbourg, France

Tél +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1. Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies.[15]

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente Note traite de la manière dont différents articles de la Convention s'appliquent au terrorisme.

Bon nombre de pays sont parties à de nombreux traités, et soumis aux Résolutions du Conseil de Sécurité des Nations Unies, qui exigent l'incrimination de différentes formes de terrorisme, de la facilitation du terrorisme, du soutien au terrorisme et des actes préparatoires au terrorisme.
Dans des affaires de terrorisme, les pays s'appuient souvent sur des infractions qui dérivent de ces traités visant des thèmes spécifiques, ainsi que sur des infractions supplémentaires incriminées en droit interne.

La Convention de Budapest n'est pas un traité s'appliquant spécifiquement au terrorisme. Toutefois, les infractions matérielles visées par la Convention peuvent être transposées aux actes de terrorisme, pour faciliter le terrorisme, pour soutenir le terrorisme – y compris financièrement - ou aux actes préparatoires au terrorisme.

En outre, les outils procéduraux et d'entraide judiciaire internationales prévus dans la Convention sont applicables aux enquêtes et poursuites pour faits de terrorisme et connexes à ces infractions.

La portée et les limites sont définies par les articles par les articles 14.2 et 25.1 de la Convention de Budapest :

> Article 14 2
>
> 2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:
> a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;
> b à toutes les autres infractions pénales commises au moyen d'un système informatique; et
> c à la collecte des preuves électroniques de toute infraction pénale.
>
> Article 25.1
>
> « Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. »

Le lecteur peut également se référer aux articles 23 et 27.1 de la Convention de Budapest ainsi que les Notes d'orientation, telles que celles sur les attaques visant des infrastructures

[15] Voir le mandate du T-CY (Article 46 Convention de Budapest).

d'information critiques ou celle sur les attaques par déni de service et déni de service distribué.

2. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (ETS 185)

2.1 Dispositions procédurales

Les pouvoirs procéduraux visés par la Convention à ses articles 14 à 21 peuvent être utilisés dans une enquête ou procédure pénale spécifique relevant de tout type d'affaire, comme le prévoit l'article 14.

De fait, les mesures procédurales spécifiques peuvent être très utiles, pour exemple dans une affaire de terrorisme, si un système informatique a été utilisé pour commettre ou faciliter une infraction ou si les preuves de l'infraction sont stockées sous forme électronique, ou encore si un suspect peut être identifié grâce aux informations relatives à l'abonné, y compris pour ce qui est d'une adresse IP (Internet Protocol). Ainsi, dans des affaires de terrorisme, les parties peuvent recourir à la conservation accélérée, aux injonctions de produire, aux ordonnances de perquisition et de saisie ainsi qu'à d'autres outils pour recueillir les preuves dans des enquêtes et poursuites en matière de terrorisme ou d'affaires connexes dans le cadre du champs exposé ci au-dessus.

2.2 Dispositions relatives à l'entraide judiciaire internationale

Les pouvoirs en matière de coopération internationale (articles 23 à 35) sont d'une portée similaire.

Ainsi, les Parties doivent assurer la conservation accélérée, délivrer des injonctions de produire, des ordonnances de perquisition et de saisie ainsi qu'utiliser d'autres outils ainsi que d'autres dispositions de coopération internationale disponibles pour coopérer avec d'autres Parties dans des enquêtes et poursuites en matière de terrorisme ou d'affaires connexes dans le cadre du champs exposé ci au-dessus.

2.3 Dispositions de droit pénal matériel

Enfin, comme indiqué plus haut, les terroristes et groupes terroristes peuvent perpétrer des actes incriminés par la Convention pour parvenir à leurs fins.

Articles pertinents	Exemples
Article 2 – Accès illégal	Il peut y avoir accès illégal à un système informatique pour obtenir des informations permettant l'identification personnelle (par exemple, informations concernant des employés publics qui permettront d'en faire la cible d'une attaque).
Article 3 – Interception illégale	Des transmissions non-publiques de données informatiques vers, depuis ou dans un système informatique peuvent être interceptées illégalement pour obtenir des informations concernant le lieu où se trouve une personne (afin de la cibler).
Article 4 – Atteinte à l'intégrité des données	Des données informatiques peuvent être endommagées, effacées, détériorées, altérées ou supprimées (ainsi, les enregistrements médicaux d'un hôpital peuvent être altérés et devenir dangereux du fait qu'ils sont incorrects, ou encore l'interférence avec un système de contrôle de trafic aérien peut avoir des conséquences pour la sûreté des vols).
Article 5 – Atteinte à l'intégrité du système	Le fonctionnement d'un système informatique peut être entravé à des fins terroristes (par exemple, entrave au bon fonctionnement du système qui

	stocke les enregistrements des opérations boursières, ce qui peut rendre ces dernières non fiables, ou encore entrave au fonctionnement d'infrastructures critiques).
Article 6 – Abus de dispositifs	La vente, l'achat en vue de l'utilisation, l'importation, la distribution ou autre forme de mise à disposition de mots de passes, codes d'accès informatiques ou données similaires permettant l'accès de systèmes informatiques peuvent faciliter une attaque terroriste (par exemple, permettre d'endommager le réseau de distribution d'électricité d'un pays).
Article 7 – Falsification informatique	Des données informatiques (par exemple celles utilisées dans les passeports électroniques) peuvent être ajoutées, altérées, effacées ou supprimées, avec pour conséquence que des données non authentiques sont prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.
Article 8 – Fraude informatique	Des données informatiques peuvent être ajoutées, altérées, effacées ou supprimées, et/ou le fonctionnement d'un système informatique altéré, avec pour résultat que des victimes perdent des biens ou avoirs (par exemple, une attaque contre le système bancaire d'un pays peut entraîner la perte d'avoirs pour un certain nombre de victimes).
Article 11 – Tentative et complicité	Les infractions spécifiées dans le traité peuvent donner lieu à tentative ou complicité à des fins terroristes.
Article 12 – Responsabilité des personnes morales	Les infractions couvertes par les articles 2-12 de la Convention dans la promotion du terrorisme peuvent être réalisées par des personnes morales qui seraient tenues comme responsable sous l'article 12.
Article 13 – Sanctions	Les infractions couvertes par la Convention peuvent constituer une menacesà l'égard des individus et de la société, en particulier lorsqu'elles visent des systèmes critiques au quotidien – par exemple, les systèmes bancaires ou les hôpitaux. Les conséquences seront variables dans chaque pays en fonction du degré d'interconnectivité et de la dépendance à de tels systèmes. Une Partie peut prévoir dans son droit interne une sanction par trop clémente pour les actes liés au terrorisme en lien avec les articles 2 à 11, ou encore ne pas prévoir de circonstances aggravantes en cas de tentative ou de complicité. Des Parties pourraient avoir à envisager de modifier leur droit interne. En vertu de l'article 13 de la Convention, les Parties doivent veiller à ce que les infractions pénales liées à de tels actes « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté. » Les Parties peuvent aussi envisager de faire jouer des circonstances aggravantes, par exemple si de tels actes affectent un nombre significatif de systèmes ou causent des dégâts considérables, notamment des morts ou des blessés, ou endommagent des infrastructures critiques.

D'autres infractions couvertes par la Convention mais qui ne sont pas mentionnées spécifiquement ci-dessus, notamment la production de matériel lié à l'exploitation des enfants ou le trafic de piratage de propriété intellectuelle, peuvent aussi être commises en lien avec le terrorisme.

Pour les Parties à la Convention de Budapest qui sont Parties au Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE 189)[16], deux articles de ce dernier sont pertinents puisque ces phénomènes peuvent contribuer à la radicalisation et à l'extrémisme violent menant au terrorisme : l'article 4 couvrant les menaces avec une motivation raciste ou xénophobe et

[16] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

l'article 6 couvrant la négation, la minimisation grossière, l'approbation ou la justification du génocide ou des crimes contre l'humanité.

3 Déclaration du T-CY

Le T-CY convient que les infractions matérielles visées par la Convention peuvent constituer des actes de terrorisme tel que défini dans le droit applicable.

Plus généralement, les infractions matérielles visées par la Convention peuvent être commises pour faciliter le terrorisme, le soutenir – y compris financièrement – ou le préparer.

Les outils procéduraux et d'entraide judiciaire internationale prévus dans la Convention peuvent servir aux enquêtes sur des faits de terrorisme, leur facilitation, le soutien ou des actes préparatoires au terrorisme.

3.7 List of participants

1. Bureau members

Version 15 November 2016

COUNTRY	NAME	INSTITUTION
NETHERLANDS (T-CY Chair)	Erik PLANKEN Cloud Evidence Group member (T-CY Representative)	Senior Policy Advisor Cybercrime Law Enforcement Department Ministry of Justice
ROMANIA (T-CY Vice-chair)	Cristina SCHULMAN Cloud Evidence Group member (T-CY Representative)	Legal adviser Department for International Law and Judicial Cooperation Ministry of Justice
CANADA	Gareth SANSOM Cloud Evidence Group member (T-CY Representative)	Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice Canada
DOMINICAN REPUBLIC	Claudio PEGUERO Cloud Evidence Group member (T-CY Representative)	Advisor to the chief of Police in ICT National Police
ESTONIA	Markko KÜNNAPU Cloud Evidence Group member (T-CY Representative)	Adviser on EU Affairs Ministry of Justice
MAURITIUS	Karuna Devi GUNESH-BALAGHEE Cloud Evidence Group member (T-CY Representative)	Assistant Solicitor General
NORWAY	Mr Eirik TRØNNES HANSEN Cloud Evidence Group member (T-CY Delegate)	Prosecutor Kripos
PORTUGAL	Pedro VERDELHO Cloud Evidence Group member (T-CY Representative)	Public Prosecutor General Prosecutor's Office of Lisbon Procuradoria Geral da Republica
SRI LANKA	Jayantha FERNANDO Cloud Evidence Group member (T-CY Representative)	Director ICTA
SWITZERLAND	Andrea CANDRIAN Cloud Evidence Group member (T-CY Representative)	Stv. Chef, International Criminal Law Unit Federal Office of Justice

COUNTRY	NAME	INSTITUTION
UKRAINE	Oleksii TKACHENKO Cloud Evidence Group member (T-CY Representative)	International Relations officer Cyber Department, SBU

2. Parties

COUNTRY	NAME	INSTITUTION
ALBANIA	Bledar DERVISHAJ (T-CY Representative)	Legal adviser Ministry of Justice
ALBANIA	Lysien ALI (T-CY Delegate)	Senior Expert IT Department Ministry of Justice
ALBANIA	Hergis JICA	Commissioner, Cybercrime Unit Albanian State Police
ALBANIA	Arqilea KOÇA	Prosecutor (chef of the sector) Cybercrime Sector Task –Force Department General Prosecution Office of Albania
ALBANIA	Aida VEIZAJ	Head of sector for money laundering State police directory
ARMENIA	Armen ABRAHAMYAN (T-CY Delegate)	Officer Fight Against High-tech Crimes, General Department of Struggle Against Organized Crime
ARMENIA	Armenuhi HARUTYUNYAN	Head of Department Legal Mutual Assistance Ministry of Justice
AUSTRALIA	Susan WHITAKER	Principal Legal Officer Australian Attorney-General's Department
AUSTRIA	Andrea ROHNER (T-CY Representative)	Prosecutor at the Ministry of Justice
AZERBAIJAN	Javid HUMBATOV	Ministry of National Security
BELGIUM	Frederik DECRUYENAERE (T-CY Representative)	Attaché au Service des Infractions et Procédures Particulières Service Public Fédéral Justice
BELGIUM	Nathalie CLOOSEN	Office of European Criminal Law of the Ministry of Justice
BOSNIA AND HERZEGOVINA	Branka BANDUKA (T-CY Representative)	Expert Adviser for combating organized crime Sector for combating terrorism, organized crime, corruption, war crimes and misuse of narcotics
BOSNIA AND HERZEGOVINA	Nedžad DILBEROVIĆ	Adviser, Section NBC Interpol, Directorate for Coordination of Police Bodies of Bosnia and Herzegovina

COUNTRY	NAME	INSTITUTION
BOSNIA AND HERZEGOVINA	Nedžad ĆATIĆ	Head of the Department for the fight against cybercrime, Ministry of the Interior of the Federation of Bosnia and Herzegovina
BOSNIA AND HERZEGOVINA	Darko CULIBRK	Investigator in Hi-Tech Crime Department Ministry of Interior of Republic of Srpska
BULGARIA	Vasil PETKOV T-CY Delegate	Inspector Cybercrime, IPR and Gambling Section, General Directorate Combating Organized Crime Ministry of Interior
CANADA	Erin MCKEY	Senior Counsel International Assistance Group Department of Justice Government of Canada
CANADA	Gareth SANSOM T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Director Technology and Analysis Criminal Law Policy Section Department of Justice Canada
CANADA	Dominic ARPIN	Cybercrime Coordinator Crime and Terrorism Division (IDT) Global Affairs Canada Government of Canada
CANADA	Cyndy NELSON	Legal Officer Criminal, Security and Diplomatic Law Division (JLA) Global Affairs Canada
CROATIA	Ivan MIJATOVIĆ	High-tech Crime Department National Police
CYPRUS		
CZECH REPUBLIC	Lenka HABRNÁLOVÁ (T-CY Representative)	International Cooperation and EU Department Ministry of Justice
DENMARK	Selina ROSENMEIER	Head of Section Criminal Law Division The Ministry of Justice
DOMINICAN REPUBLIC	Claudio PEGUERO T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Advisor to the chief of Police in ICT National Police

COUNTRY	NAME	INSTITUTION
DOMINICAN REPUBLIC	César MOLINE	Attorney in charge of Competition Defense Encargado Defensa de la Competencia Dominican Institute of Telecommunications (Instituto Dominicano de las Telecomunicaciones - INDOTEL)
DOMINICAN REPUBLIC	Miguel JAZMIN	Member of the National Parliament Chairman of the National Commission for ICT House of Representatives, National Congress
DOMINICAN REPUBLIC	Thelma ALVAREZ	Legal Advisor / DICAT National Police
ESTONIA	Markko KÜNNAPU T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Adviser on EU Affairs Ministry of Justice
FINLAND	Janne KANERVA (T-CY Representative)	Counsellor of Legislation Legislative Affairs Ministry of Justice
FINLAND	Karl LINDERBORG	Senior Detective Superintendent, Legal Advisor, Deputy Head of Cybercrime Center National Bureau of Investigation Criminal Investigation, Cybercrime Center
FINLAND	Tiina FERM	Councellor in Legislative Affairs Police Department Ministry of the Interior
FRANCE	Sylvain BRUN (T-CY Delegate)	Adjoint au chef de OCLCTIC (National Cybercrime Unit) Sous-direction de la lutte contre la cybercriminalité Direction centrale de la police judiciaire Direction générale de la police nationale Ministère de l'Intérieur
FRANCE	Raphaele BAIL	Judge DACG
GEORGIA	Giorgi TIELIDZE (T-CY Representative	Senior Adviser Department of Internal Security and Public Order
GEORGIA	Givi BAGDAVADZE	

COUNTRY	NAME	INSTITUTION
GERMANY	Stefan ZIMMERMANN	Staff Counsel Division for Criminal Law Suppression of Economic Crime, Computer Crime, Corruption-related Crime and Environmental Crime Federal Ministry of Justice and Consumer Protection
HUNGARY	Zsuzsa PETHŐ (T-CY Representative)	Department of European Cooperation Ministry of Interior
ICELAND	Sigurður Emil PÁLSSON (T-CY Delegate)	Senior Advisor Civil Protection, Cyber Security, Critical Infrastructures, Technical and Strategic Issues Department of Public Security Ministry of the Interior
ISRAEL	Haim WISMONSKY (T-CY Representative)	Director, Cybercrime Department Israeli State Attorney's Office
ISRAEL	Naomi Elimelech Shamra (T-CY delegate)	Treaties Department Deputy Director Ministry of Foreign Affaires
ITALY	Francesco CAJANI Cloud Evidence Group member (T-CY Representative)	Deputy Public Prosecutor High Tech Crime Unit Court of Law in Milan
ITALY	Gianluigi UMETELLI	Chief Inspector Italian National Police
JAPAN	Yuri HAYASHI Cloud Evidence Group member	International Safety and Security Cooperation Division Foreign Policy Bureau Ministry of Foreign Affairs
JAPAN	Mayumi TSUBOI	Attorney Criminal Affairs Bureau Ministry of Justice
JAPAN	Fumitake MASUKAWA	Superintendent, Cybersecurity Office National Police Agency of JAPAN
LATVIA	Aleksandra TUKISA (T-CY Delegate)	International Cooperation Bureau
LATVIA	Uldis ĶINIS	Vice Presidents of Constitutional court/ professor Constitutional court of Latvia

COUNTRY	NAME	INSTITUTION
LITHUANIA	Lilija OMELJANČUK (T-CY Representative)	Chief Investigator of the 1st Division of Cybercrime Investigation Board of the Lithuanian Criminal Police Bureau Vilnius
LIECHTENSTEIN	Dominic SPRENGER (T-CY Representative)	Office for Foreign Affairs
LUXEMBOURG	Catherine TRIERWEILER (T-CY Representative) APOLOGISED	Attachée d'administration au Ministère de la Justice à Luxembourg
MALTA		
MAURITIUS	Karuna Devi GUNESH-BALAGHEE Bureau and Cloud Evidence Group member (T-CY Representative)	Assistant Solicitor General
MAURITIUS	Mary Jane LAU YUK POON Cloud Evidence Group member	Assistant Solicitor General Attorney General's Office
MAURITIUS	Divi SEWPAL	State Counsel
MAURITIUS	Pravin HARRAH	Principal State Counsel Office of the Director of Public Prosecutions
MAURITIUS	Michael Clint Kervin Juanito PUDMAN	Police Officer Mauritius Police Force
MOLDOVA	Veaceslav SOLTAN (T-CY Representative)	Prosecutor Chief of Department on Information Technology and Cybercrime Investigation
MOLDOVA	Irina CUCIUC	
MONTENEGRO	Jakša BACKOVIĆ	Head of Unit for Anti-High Tech Crime in the Department for the fight against organised crime and corruption, Ministry of Interior - Police Directorate
MONTENEGRO	Ognjen MITROVIC (T-CY Representative)	Adviser Directorate for International Legal Cooperation and EU Integration Ministry of Justice
MONTENEGRO	Aleksandra RUBEŽIĆ	Independent advisor – coordinator of Analytics Department Administration for the Prevention of Money Laundering and Terrorism Financing of Montenegro

COUNTRY	NAME	INSTITUTION
NETHERLANDS	Erik PLANKEN T-CY Chair and Cloud Evidence Group member (T-CY Representative)	Senior Policy Advisor Cybercrime Law Enforcement Department
NETHERLANDS	MAAS E.M.	Ministry Security and Justice
NORWAY	Eirik TRØNNES HANSEN T-CY Bureau and Cloud Evidence Group member (T-CY Delegate)	Prosecutor Kripos
PANAMA		
POLAND	Michał ZALEWSKI	Wydział dw. z Cyberprzestępczością Biuro Służby Kryminalnej Komendy Głównej Policji
PORTUGAL	Pedro VERDELHO T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Public Prosecutor General Prosecutor's Office of Lisbon Procuradoria Geral da Republica
ROMANIA	Ioana ALBANI Cloud Evidence Group member (T-CY Delegate)	Deputy Chief-Prosecutor Directorate for Investigating Organised Crime and Terrorism Prosecutor's Office attached to the High Court of Cassation and Justice
ROMANIA	Cristina SCHULMAN T-CY Vice-Chair and Cloud Evidence Group member (T-CY Representative)	Legal adviser Department for International Law and Judicial Cooperation Ministry of Justice
SERBIA	Branko STAMENKOVIC (T-CY Representative)	Special Prosecutor for High-Tech Crime of Serbia
SERBIA	Jovana MIHAILOVIC	Legal Specialist Ministry of Justice
SERBIA	Dragan JOVANOVIC	Deputy Head of Department Service for Combating Organized Crime Department for Cyber Crime
SERBIA	Vlatko BOZOVIC	Head of Department for Financial Investigation Ministry of Interior
SLOVAKIA	Branislav KADLECIK (T-CY Representative)	General State Counsellor Office of the Minister Human Rights Divisin Ministry of Justice
SLOVENIA	Tomaž JAKSE	Senior Criminal Police Inspector – Specialist Computer Investigation Centre

COUNTRY	NAME	INSTITUTION
SPAIN	Maria Elvira TEJADA DE LA FUENTE (T-CY Representative)	Head Cybercrime Prosecutor's Office
SPAIN	Angel SANCHEZ FRAILE	Spanish National Police High Tech Unit
SPAIN	Jose DURAN	Guardia Civil Criminal Police Branch Criminal Intelligence Unit – High Tech Crime Group
SRI LANKA	Jayantha FERNANDO Bureau and Cloud Evidence Group member (T-CY Representative)	Director ICTA
SRI LANKA	Dharshika KUMARI	Woman Assistance Superintendent of Police Criminal Investigation Department
SRI LANKA	Roshan Chandraguptha GALABADA LIYANAGE	Principal Information Security Engineer
SRI LANKA	Hon. E.A.G.R. AMARASEKARA	High Court Judge, Commercial High Court Colombo
SWITZERLAND	Andrea CANDRIAN T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Stv. Chef, International Criminal Law Unit Federal Office of Justice
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Vladimir MILOSHESKI (T-CY Representative)	Public Prosecutor Basic Public Prosecutor's Office
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Aleksander RISTOVSKI	IT Officer Financial Police Department Ministry of Finance
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Maja JOVANOVA	Head of IT Unit Department for Financial Intelligence
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Marjan STOILKOVSKI	Head of the Sector for Computer Crime and Digital Forensics
TURKEY	Kürşad Başaran BASOGLU	Captain Cybercrime Prevention Division Cybercrime Department Turkish National Police
TURKEY	Ömer Artun AKTİMUR	Financial Intelligence Unit (FIU) Financial Crimes Investigation Board Ministry of Finance

COUNTRY	NAME	INSTITUTION
TURKEY	Tamer SOYSAL	Judge Department of Justice
TURKEY	Meral GÖKKAYA	Investigating Judge Ministry of Justice
UKRAINE	Oleksii TKACHENKO T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	International Relations officer Cyber Department, SBU
UKRAINE	Tetiana SHORSTKA	Deputy Head of Department-Head of the Division on Mutual Legal Assistance in Criminal Matters Ministry of Justice
UNITED KINGDOM	Faiza TAYAB-JONES APOLOGISED	Cyber Crime, Fraud, Interventions & Partnerships Unit Strategic Centre for Organised Crime Office for Security and Counter Terrorism
USA	Albert C. REES JR.	Senior Counsel, International Programs Computer Crime & Intellectual Property Section United States Department of Justice

3. Observer States

COUNTRY	NAME	INSTITUTION
ANDORRA	Azahara CASCALES RUIZ APOLOGISED	Juge d'instruction
ARGENTINA	Marcos SALT (T-CY representative)	Prof. Criminal Law University of Buenos Aires Academic Director National Program on computer Related Crime Ministry of Justice
CHILE	Pablo CASTRO (T-CY Representative)	Subdirector para Seguridad Internacional Ministerio de Relaciones Exteriores Dirección de Seguridad Internacional y Humana
COLOMBIA	Angel JUANITA NAVARRO	Crime Prevention Division Department of Political Multilateral Affairs Ministry of Foreign Affairs
COSTA RICA	Adalid MEDRANO (T-CY Delegate)	Abogado & Consultor en Nuevas Tecnologías
GHANA	Yvonne ATAKORA OBUOBISA	Ag. Director of Public Prosecutions Division
GHANA	Kwabena ADU-BOAHEN	Office of the National Security Coordinator
GHANA	Margaret ABBA-DONKOR	Manager Engineering National Communications Authority
GREECE		
IRELAND		
MEXICO	Santiago OÑATE LABORDE	Observateur Permanent du Mexique auprès du Conseil de l'Europe
MEXICO	Diego Sandoval PIMENTEL	Adjoint à l'Observateur Permanent du Mexique auprès du Conseil de l'Europe
MONACO	Gabriel REVEL	Adjoint au Représentant Permanent Représentation Permanente de Monaco auprès du Conseil de l'Europe
MONACO	Jacques DOREMIEUX	Public Prosecutor (General) Justice Parquet Général

COUNTRY	NAME	INSTITUTION
MOROCCO	Layla EZZOUINE	Chef de Service de lutte contre la criminalité liée aux nouvelles technologies Direction générale de la Sûreté nationale
MOROCCO	Abdeljalil TAKI (T-CY representative)	Ministère de l'Intérieur DGST
MOROCCO	Mina JAMIL	Magistrat Ministère de la Justice et des Libertés
PARAGUAY	María Soledad MACHUCA APOLOGISED	Head of Cybercrime Unit Deputy Attorney General
PERU	Milagros CASTANON SEANE APOLOGISED	Ministra SDR Directora de la Direccion de Ciencia Y tecnología DAE
PHILIPPINES	Wendell BENDOVAL	Prosecutor National Prosecution Service Department of Justice
PHILIPPINES	Antonio KHO	Undersecretary / Deputy Minister Department of Justice
PHILIPPINES	Jed Sherwin UY T-CY Representative	Director Office of Cybercrime Department of Justice
RUSSIAN FEDERATION	Konstantin KOSORUKOV	First Secretary, Legal Department of the Ministry of Foreign Affairs of the Russian Federation
RUSSIAN FEDERATION	Yulia TOMILOVA	Third Secretary, Department of New Threats and Challenges of the Ministry of Foreign Affairs of the Russian Federation
RUSSIAN FEDERATION	Anton MARKOVSKIY	Deputy to the Permanent Representative of the Russian Federation to the Council of Europe
SAN MARINO		
SENEGAL	Papa Assane TOURE	Secrétaire général Adjoint du Gouvernement Primature du Sénégal
SENEGAL	Samba SALL	Magistrat Doyen des juges d'instruction au tribunal de grande instance hors classe de Dakar
SENEGAL	Issa DIACK	Commandant Section Recherches de la Gendarmerie nationale

COUNTRY	NAME	INSTITUTION
SOUTH AFRICA	Zoyisile MSHUNQANE (T-CY Representative)	State Security Agency
SOUTH AFRCA	Rhulani Luckson MIHLANGA	Third Secretary Permanent mission of South Africa in Austria
SWEDEN	Mikael KULLBERG APOLOGISED	Rättssakkunnig Åklagarenheten Justitiedepartementet
TONGA	Adi Talanaivini MAFI	Legal Officer Ministry of Justice
TONGA	Aminiasi KEFU (T-CY Representative)	Solicitor General Attorney General Office

4. Ad-hoc country observers

COUNTRY	NAME	INSTITUTION
BELARUS	Aleksandr SUSHKO	
BELARUS	Zmicier BRYLOU	
CABO VERDE	Franklin Afonso FURTADO	Deputy Public Prosecutor General Prosecutor's Office of Cabo Verde Procuradoria Geral da República Praia
KOREA	In Gi LEE	Investigator Cybercrime investigation FSID of SPO (Forensic Science Investigation Department of Supreme Prosecutor's Office)
KOREA	Seong Su AN	Chief Prosecutor Deputy Chief of FSID FSID of SPO (Forensic Science Investigation Department of Supreme Prosecutor's Office
KOREA	Gwi il KIM	Senior Investigator Cybercrime investigation FSID of SPO (Forensic Science Investigation Department of Supreme Prosecutor's Office)
KOREA	Do Wook SHIN	Prosecutor / International Criminal Affairs International Criminal Affairs Division of Ministry of Justice
SINGAPORE	Kannan GNANASIHAMANI	Senior State Counsel Deputy Public Prosecutor Senior Director Technology Crime Unit Financial & Technology Crime Division Attorney-General's Chambers
SINGAPORE	Suhas MALHOTRA	Attorney-General's Chambers
TUNISIA	Mohamed MESSAI	Conseiller à la Cour d'Appel de Tunis

5. Observer Organisations

ORGANISATION	NAME	POSITION
AFRICAN UNION COMMISSION (AUC)		
COMMONWEALTH	Emma THWAITE	Assistant Legal Officer, Rule of Law Division Commonwealth Secretariat
EUROPEAN COMMISSION HOME AFFAIRS	Tjabbe Bos	Policy Officer European Commission DG Migration and Home Affairs Unit D2 – Fight against organised crime
EUROPEAN COMMISSION	Barbara MENTRÉ	Legislative Officer
EUROPEAN UNION EUROPOL (EC3)	Gregory MOUNIER APOLOGISED	Head of Outreach and Support
EUROPEAN UNION ENISA	Silvia PORTESI	Research and Analysis Expert ENISA European Union Agency for Network and Information Security
EUROPEAN UNION EUROJUST		
EUROPEAN UNION EUROJUST	Daniela BURUIANA	Chair of the Task Force on cybercrime Eurojust National member for Romania
G7 Group's High-Tech Crime Subgroup		
INTERPOL	John BARRY	ICT Law Programme Manager Data Protection and Programmes
INTERPOL	Sabine BERGHS	Legal Officer
INTERPOL	Christophe DURAND	Head of Strategy and Outreach IGCI
International Telecommunication Union (ITU)		
ORGANIZATION OF AMERICAN STATES (OAS)	Belisario CONTRERAS	Cyber Security Program Manager Inter-American Committee against Terrorism
ORGANIZATION OF AMERICAN STATES (OAS)	Rodolfo ORJALES	President, Group of Experts on Cybercrime
OECD		
OSCE	Margaret LAZYAN	Politico/Military Senior Assistant OSCE Office in Yerevan
UNODC		

6. Council of Europe experts

ORGANISATION	NAME	POSITION
Consultant	Betty SHAVE	Consultant

7. Council of Europe Committees

COMMITTEES	NAME	POSITION
CDMSI (Steering Committee on Media and Information Society)		
CDPC (European Committee on Crime Problems)		
PC-OC		
T-PD		

8. Council of Europe Secretariat

Name	Details
Jan KLEIJSSEN	Director of Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Patrick PENNINCKX	Head of Media, Information Society, Data Protection and Cybercrime Department Information Society and Action against Crime Directorate, Directorate General Human Rights and Rule of Law
Alexander SEGER	Executive Secretary of the Cybercrime Convention Committee Head of Cybercrime Division Head of Cybercrime Programme Office (C-PROC) Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Alexandru FRUNZA	Programme Officer Data Protection and Cybercrime Division Information Society and Action against Crime Directorate Directorate General of Human Rights and Rule of Law
Pierluigi PERRI	Programme Officer Data Protection and Cybercrime Division Information Society and Action against Crime Directorate Directorate General of Human Rights and Rule of Law
Marie AGHA-WEVELSIEP	Programme Officer Cybercrime Division Information Society and Action against Crime Directorate Directorate General of Human Rights and Rule of Law
Ana ELEFTERESCU	Project Officer Cybercrime Programme Office (C-PROC) Bucharest Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Sinziana HANGANU	Project assistant Cybercrime Programme Office (C-PROC) Bucharest Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Valérie SCHAEFFER	Project Assistant Cybercrime Division Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Alexandra-Adina TRANDAFIR	Project assistant Cybercrime Programme Office (C-PROC) Bucharest Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law

9. Interpreters

Julia TANNER
Christopher TYCZKA
Sylvie BOUX

Derrick WORSDALE
Sergio ALVAREZ
Hans MÜHLE