www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

Comité de la Convention Cybercrime (T-CY)

Note d'orientation #11 du T-CY (PROJET)
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.[1]

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. »

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

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 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)[2], 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 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.

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