Web site: www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 12 March 2008 T-CY (2008) INF 02 F

COMITE DE LA CONVENTION SUR LA CYBERCRIMINALITE (T-CY)

Document d'information concernant l'Opinion du Comité d'experts sur le Terrorisme (CODEXTER) sur la cybercriminalité et l'utlilisation d'Internet à des fins terroristes

Note du Secrétariat
établie par
la Direction générale des droits de l'Homme et des affaires juridiques

Décision adoptée par le Comité des Ministres lors de leur 1019e réunion, 27-28 février 2008

10.2 Comité d'experts sur le terrorisme (CODEXTER)

b. Avis du CODEXTER sur le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes

Les Délégués

1. prennent note de l'avis du Comité d'experts sur le terrorisme (CODEXTER) concernant le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes, tel qu'il figure dans le document CM(2007)177, Annexe 2, et décident de le transmettre au Comité européen pour les problèmes criminels (CDPC) et au Comité de la Convention cybercriminalité (T-CY) pour information ;

Avis du Comité d'experts sur le terrorisme (CODEXTER) à l'attention du Comité des Ministres
concernant le cyberterrorisme et l'utilisation de l'internet à des fins terroristes

Le 11 juillet 2005, le Comité des Ministres a transmis la Recommandation 1706 (2005) de l'Assemblée parlementaire - Médias et terrorisme, au Comité d'experts sur le terrorisme (CODEXTER) pour information et commentaires éventuels, en lui demandant de communiquer ceux-ci avant le 31 octobre 2005.

Le Bureau du CODEXTER a tenu une réunion extraordinaire les 17 et 18 octobre 2005 au cours de laquelle il a, comme demandé par le Comité des Ministres, examiné cette recommandation en se concentrant sur les questions jugées relever du mandat du CODEXTER, et a ensuite formulé un certain nombre de commentaires.

Lors de sa 9e réunion (8-10 novembre 2005), le CODEXTER a examiné ces commentaires dans le cadre de son activité destinée à identifier les lacunes dans le droit international et l'action internationale contre le terrorisme ; il a ainsi considéré que le cyberterrorisme pourrait être un domaine d'action future du Conseil de l'Europe.

Le CODEXTER est convenu d'intégrer la question du cyberterrorisme dans l'évaluation générale de l'application de la Convention sur la cybercriminalité (STE n° 185) et a demandé à être tenu informé des faits nouveaux en la matière.

Le CODEXTER est parvenu à la conclusion que, sans préjuger des autres propositions qui pourraient être présentées sur cette question, les attaques graves contre les infrastructures informatiques semblaient déjà couvertes par la Convention sur la cybercriminalité. Il a par ailleurs pris note des propositions de mesures pratiques destinées à combattre et empêcher l'utilisation de systèmes informatiques à des fins terroristes.

Il avait en outre été décidé que le CODEXTER reviendrait sur cette question sur la base des propositions soumises par les délégations. La question du cyberterrorisme a de surcroît été reprise dans le rapport d'avancement du CODEXTER sur les futurs domaines prioritaires pour les activités du Conseil de l'Europe en matière de lutte contre le terrorisme, rapport qu'il a soumis au Comité des Ministres.

Le 20 janvier 2006, le Comité des Ministres a pris note dudit rapport d'avancement, l'a transmis à un certain nombre de comités pertinents du Conseil de l'Europe, et est convenu d'y revenir à un stade ultérieur sur la base d'informations complémentaires.

En 2006, le Conseil de l'Europe a commandité au Professeur Ulrich Sieber, Directeur de l'Institut Max Planck de droit pénal international de Fribourg (Allemagne), un rapport d'expert sur « l'utilisation de l'Internet (englobant également d'autres moyens de communication analogues comme les téléphones portables de troisième génération) à des fins terroristes et le cyberterrorisme ».

Au cours de ses 10e (juin 2006), 11e (décembre 2006) et 12e (avril 2007) réunions, le CODEXTER a poursuivi l'examen du problème posé par l'utilisation de l'Internet à des fins terroristes et de la notion de cyberterrorisme, sur la base des observations soumises par les délégations et de deux échanges de vues avec le Professeur Sieber (lors des 11e et 12e réunions).

* * *

Le Comité mène actuellement une enquête sur la situation dans les Etats membres et observateurs du Conseil de l'Europe, à partir d'un questionnaire concernant le droit et la pratique au niveau national en matière d'utilisation du cyberespace à des fins terroristes.

A la lumière des travaux qu'il a menés, le CODEXTER considère que les notions de cyberterrorisme et d'utilisation de l'Internet à des fins terroristes incluent divers éléments :

a. les attaques via l'Internet qui portent atteinte non seulement aux systèmes essentiels de communication électronique et aux infrastructures informatiques, mais aussi à d'autres infrastructures, systèmes et intérêts légaux, y compris la vie humaine ;

b. la diffusion de contenus illicites, et notamment les menaces d'attaques terroristes, les incitations, la promotion et l'apologie du terrorisme, la collecte de fonds et le financement du terrorisme, l'entraînement au terrorisme, le recrutement à des fins de terrorisme ; ainsi que

c. d'autres utilisations logistiques des systèmes informatiques par les terroristes, telles que la communication interne, l'acquisition d'informations et l'analyse de cibles.

Analyse des recommandations de l'expert indépendant

Le CODEXTER a discuté des analyses et recommandations suivantes contenus dans le rapport d'expert qui, à son avis, méritent un examen approfondi par les instances compétentes.

Les conventions internationales existantes, de même que d'autres instruments contribuant à l'harmonisation des règles substantielles et procédurales du droit interne et à la coopération internationale, sont applicables face à ces usages dévoyés de l'Internet à des fins terroristes. La question essentielle à laquelle il faut répondre est celle de l'existence de lacunes « spécifiques au terrorisme » dans les conventions « spécifiques à l'informatique » et de lacunes « spécifiques à l'informatique » dans les conventions « spécifiques au terrorisme ». L'expert a estimé à cet égard que de telles lacunes n'existent pas pour ce qui concerne la mise en œuvre des conventions.

Cependant il pourrait y avoir des lacunes générales, par exemple, des lacunes qui ne sont pas propres à l'utilisation de l'Internet à des fins terroristes dans des instruments « spécifiques à l'informatique » et « spécifiques au terrorisme »:

a. Un grave problème, commun à la plupart des instruments internationaux, est le nombre insuffisant d'Etats parties. Cette remarque vaut particulièrement pour la Convention sur la cybercriminalité et la Convention pour la prévention du terrorisme, qui sont les instruments internationaux les plus importants dans le domaine de la lutte contre le cyberterrorisme et les autres utilisations de l'Internet à des fins terroristes. Aussi faut-il encourager la signature, la ratification et la mise en œuvre de ces deux conventions, et faire en sorte que les initiatives nouvelles prises en la matière ne retardent ni ne perturbent ce processus.

b. La Convention sur la cybercriminalité pourrait être évaluée davantage au regard de sa capacité à prendre en considération des avancées techniques apparues ou évoquées depuis peu, notamment dans le domaine des techniques d'investigation judiciaire (telles que les perquisitions en ligne ou l'utilisation d'enregistreurs de touches). Dans le contexte technique de la cybercriminalité où tout évolue rapidement, il est absolument normal de procéder à de telles évaluations - qui entraînent souvent révisions et mises à jour -, surtout face à des risques aussi grands que ceux posés par le terrorisme.

Cependant, l'ajout d'une disposition portant sur les attaques visant des infrastructures informatiques ou générales n'est pas indispensable. Il suffirait aux Etats de s'assurer que leurs textes de loi relatifs aux atteintes à l'intégrité des données et des systèmes prévoient des sanctions appropriées en cas d'attaques terroristes dirigées contre des systèmes informatiques. De telles « sanctions effectives, proportionnées et dissuasives » sont du reste déjà requises par la Convention sur la cybercriminalité, et l'on pourrait laisser aux législateurs nationaux le soin d'y veiller, en réglementant les peines encourues, en aggravant la qualification des infractions pour atteinte à l'intégrité des données ou en créant des infractions pour atteinte aux infrastructures.

c. Les mesures répressives et préventives, à la fois efficaces et respectueuses des libertés publiques, qui auraient pour cible la diffusion de contenus illicites sur l'Internet pourraient être examinées. Une possibilité pour ce faire serait de mettre plus particulièrement l'accent sur les contenus terroristes illicites ; une autre solution, plus générale, serait d'y inclure d'autres types de contenus illicites. Sur le plan du droit substantiel, cela pourrait impliquer la réflexion sur la responsabilité des fournisseurs de services Internet qui pourraient ensuite venir appuyer des procédures internationales de repérage et de démantèlement.

Avis du CODEXTER

Le CODEXTER considère que le nombre insuffisant d'Etats parties à la Convention sur la Cybercriminalité et la Convention pour la prévention du terrorisme constitue un grave problème. Il invite le Comité des Ministres à réitérer sa position sur ce problème et à encourager les Etats à signer, ratifier et mettre en œuvre les conventions pertinentes.

Il souligne par ailleurs qu'à ce stade, il faudrait tout d'abord s'attacher à garantir la mise en œuvre effective de la Convention sur la cybercriminalité et de la Convention pour la prévention du terrorisme, l'ouverture de nouvelles négociations risquant d'hypothéquer leurs effets de plus en plus marqués sur la lutte internationale contre la cybercriminalité et le terrorisme.

La mise en oeuvre effective de la Convention sur la cybercriminalité permettrait de s'assurer que les législations nationales prévoient des sanctions appropriées en cas de graves attaques – y compris celles à caractère terroriste - dirigées contre des infrastructures informatiques ou générales. De même, la mise en œuvre effective de la Convention du Conseil de l'Europe pour la prévention du terrorisme permettrait de prendre pour cible la diffusion de contenus terroristes illicites sur l'Internet.

Le CODEXTER propose également d'examiner plus avant la question de la responsabilité des fournisseurs d'accès à l'Internet.