OCTOPUS CONFERENCE 2013
Strasbourg, 4 – 6 December 2013

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Version 6 décembre 2013

Messages clés

Près de 300 experts de la cybercriminalité provenant de plus de 80 pays, 17 organisations et initiatives internationales et 45 acteurs issus du secteur privé, de la société civile ou du monde universitaire étaient réunis à Strasbourg du 4 au 6 décembre 2013 pour améliorer la coopération contre la cybercriminalité à tous les niveaux.

Voici certains des principaux messages qui ressortent des débats tenus lors des séances plénières et des ateliers :

1 La menace croissante que représente la cybercriminalité est un défi majeur pour les sociétés du monde entier. D'importantes mesures ont été prises au sein des secteurs public et privé de nombreux pays pour prévenir et combattre cette menace. Des efforts supplémentaires s'imposeront, notamment pour renforcer les cadres juridiques, les capacités du système judiciaire pénal et la coopération plurilatérale. En ce qui concerne les mesures de justice pénale applicables, la Convention de Budapest fait référence en Afrique, dans les Amériques, en Asie-Pacifique et en Europe.

2 Les gouvernements ont l'obligation positive de protéger les personnes contre la criminalité. Les mesures de justice pénale prévues notamment dans la Convention sur la cybercriminalité s'appliquent dans le cas de certaines enquêtes bien précises et sont soumises aux garanties de l'Etat de droit visant à protéger les droits des personnes. Il est rappelé que les pays se dotant de lois relatives à la cybercriminalité sont nombreux à adopter en parallèle une législation en matière de protection des données. Actuellement en pleine refonte, la Convention du Conseil de l'Europe n° 108 pour la protection des données sert de référence et est ouverte à l'adhésion des pays tiers.

3 Les mesures de justice pénale relatives à la cybercriminalité doivent être distinguées de celles relatives à la sécurité nationale. La frontière floue qui existe entre le champ de la justice pénale et celui de la sécurité nationale constitue une menace pour l'Etat de droit. Certains rapports concernant des activités de surveillance de masse menées par des institutions nationales de sécurité laissent craindre que les conditions nécessaires ne soient pas réunies pour protéger le droit au respect de la vie privée et d'autres droits fondamentaux ou pour prévenir les abus de pouvoir de l'Etat. Il convient de prendre des mesures pour restaurer la confiance. Les institutions nationales de sécurité doivent opérer dans le cadre de l'Etat de droit.

4 Le nombre croissant d'organisations internationales ayant placé la cybercriminalité et la cybersécurité à leur ordre du jour témoigne également des inquiétudes grandissantes que suscite cette question. Il est essentiel que les organisations internationales coopèrent afin de mieux servir les sociétés. La Conférence a été l'occasion d'exposer une série de bonnes pratiques à cet égard.

5 A noter parmi les points encourageants, l'évolution de la législation en Afrique, dans les Amériques, en Asie-Pacifique et en Europe ainsi que le degré croissant d'harmonisation

avec les normes de la Convention de Budapest. Un soutien bienvenu peut être apporté aux initiatives allant en ce sens notamment par l'Union européenne, par le Commonwealth, par l'Organisation des Etats américains et par la Conférence des ministres de la Justice des pays ibéro-américains (COMJIB).

6 Vu les réformes législatives déjà menées ou en cours dans de nombreux pays, la priorité devrait à présent être donnée au renforcement des capacités, comme indiqué lors des précédentes conférences Octopus. Il est encourageant de voir que, d'une part, la communauté internationale, y compris au niveau des Nations Unies, s'accorde dans l'ensemble à dire que le renforcement des capacités est une réponse efficace et que, d'autre part, cet accord politique se traduit actuellement par des projets de coopération spécifiques. De bonnes pratiques relatives aussi bien à ces projets qu'à des outils ou à des matériels peuvent être diffusées. Les organisations elles-mêmes devraient se donner davantage de moyens pour mettre en place des projets de renforcement des capacités. A cet effet, le Conseil de l'Europe est sur le point d'ouvrir un Bureau de programme sur la cybercriminalité (C-PROC) à Bucarest (Roumanie).

7 La cybercriminalité est un défi complexe auquel il convient de faire face en s'appuyant sur des approches multipartites et sur un éventail d'acteurs variés. Il est nécessaire de favoriser une certaine diversité dans les initiatives de lutte contre la cybercriminalité, et en particulier une plus importante participation des femmes.

8 Une coopération internationale efficace est essentielle compte tenu de la dimension transnationale que présentent la cybercriminalité et les preuves électroniques. Une série de solutions peuvent être envisagées pour optimiser la coopération entre services de police, l'entraide judiciaire et le fonctionnement du réseau 24/7 de points de contact. Il est rappelé que les dispositions d'entraide judiciaire de la Convention de Budapest font actuellement l'objet d'un examen du Comité de la Convention Cybercriminalité (T-CY).

9 Etant donné les innovations technologiques et les techniques utilisées dans le cadre de la cybercriminalité, les démarches, les voies et les moyens traditionnels de coopération internationale ne sont pas toujours applicables. Il peut être nécessaire de disposer d'un accès transfrontalier direct aux données pour certaines enquêtes judiciaires spécifiques. Cependant, il est essentiel d'établir des garanties pour protéger les droits des personnes, les intérêts des tierces parties et les intérêts des Etats. La Conférence encourage les parties prenantes concernées à coopérer pour trouver des solutions acceptables qui soient compatibles avec l'Etat de droit, les droits de l'homme et la protection des données.

10 La protection des enfants contre la violence sexuelle sur internet requiert une approche globale alliant prévention, protection, poursuites judiciaires et autonomisation. Les organisations non gouvernementales et internationales jouent un rôle important, en particulier concernant la prévention, la protection et la promotion d'une utilisation plus sécurisée des technologies de l'information par les enfants. L'application de la loi et l'exercice de poursuites sont au centre de la réponse. La mise en œuvre des critères de droit pénal énoncés dans les Conventions de Budapest et de Lanzarote facilite les opérations internationales de détection et de répression visant à sauver des enfants et à poursuivre les auteurs en justice.

11 Encore une fois, coopérez et ne vous attaquez pas à de faux problèmes.

Composante du Projet global sur la cybercriminalité, la Conférence Octopus a été rendue possible grâce aux contributions volontaires de l'Estonie, de l'Allemagne, du Japon, de Monaco, de la Roumanie, du Royaume-Uni et de Microsoft ainsi qu'à des fonds du budget du Conseil de l'Europe.

www.coe.int/cybercrime