



Douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale

Salvador (Brésil), 12-19 avril 2010



› Fiche d'information 8

Pour information seulement — document sans caractère officiel

UNE COOPÉRATION INTERNATIONALE INSUFFISANTE PERMET AUX CYBERCRIMINELS DE S'EN TIRER À BON COMPTE

La rapide évolution et la nature changeante des technologies de l'information jumelée avec la rapide expansion de la Toile (WWW) au cours des dix dernières années ajoutées à la croissance exponentielle de la rapidité de l'échange des renseignements ont rendu la réalisation des enquêtes sur la cybercriminalité particulièrement difficile. À la fin 1997, seulement 1,7 % de la population mondiale, soit 70 millions de personnes, avait utilisé l'Internet. En 2009, le nombre des utilisateurs était passé à environ 1,9 milliards de personnes, soit 26 % de la population mondiale, selon les derniers chiffres publiés par l'Union internationale des télécommunications (UIT).

Pourtant, malgré un demi-siècle de débats, l'abus de la technologie sous forme de cybercriminalité constaté au cours des récentes années continue à poser un grave problème au personnel de détection et de répression ainsi qu'aux législateurs. Par comparaison avec la coopération internationale qui a lieu au sujet des crimes dits traditionnels, celle qui existe pour faire face à la criminalité électronique et informatique est notablement sous-développée étant donné son importance.

› Nature et étendue du problème

Le fait que les services électroniques soient disponibles dans le monde entier signifie que la cybercriminalité possède une dimension transnationale. Même pour quelque chose d'aussi simple que l'envoi d'un courrier électronique à un destinataire dans le même pays, il existe un élément transnational si l'une des personnes utilise un service de courrier électronique exploité à partir de l'étranger. Certains services de courrier électronique populaires sont utilisés par des millions de personnes dans le monde, ce qui donne une idée de l'ampleur que peut prendre la cybercriminalité transnationale.

Il est essentiel, pour qu'une enquête porte ses fruits, que les pays coopèrent en temps voulu et efficacement car, contrairement au cas des enquêtes criminelles traditionnelles, la durée pendant laquelle un enquêteur peut agir au sujet d'un cybercrime est très restreinte. Il ne faut que quelques minutes pour télécharger des fichiers de grande taille! Bien que certains accords d'entraide judiciaire soient en place, il

est vital d'établir des procédures pour agir rapidement et pour assurer la coopération internationale.

Malgré un consensus presque universel sur le fait que la cybercriminalité est une question urgente qui exige une réponse immédiate et coordonnée de la part de tous les pays, il est difficile de quantifier son ampleur, et encore plus de suivre ses myriades d'avatars changeants. Même les statistiques nationales de base sur la criminalité ne consacrent pas toujours une catégorie distincte à la cybercriminalité. Par conséquent, les renseignements fiables concernant les arrestations, poursuites et condamnations sont fréquemment difficiles, voire impossible, à rassembler.

Il est fréquent que la cybercriminalité ne fasse l'objet d'aucun rapport, et ce pour diverses raisons. Ainsi, les victimes du secteur financier comme les banques pourraient ne pas la signaler par crainte de l'atteinte à leur réputation si elles faisaient état d'attaques de pirates informatiques.

› Importance d'un réseau d'intervention mondial et rapide

Parce qu'un cybercrime peut être perpétré même lorsque les criminels et les victimes visées ne se trouvent pas dans le même lieu, il est essentiel que les nations élaborent un système de collaboration bien coordonné. Cependant, les différences régionales au niveau du droit peuvent constituer un obstacle en matière de cybercriminalité; un contenu réputé illégal dans un pays peut être légalement affiché sur un serveur dans un autre. La plus grande partie de l'entraide judiciaire est fondée sur la double incrimination ce qui implique que les enquêtes portent sur des actes incriminés dans tous les pays touchés, d'où des problèmes lorsque les législations ne convergent pas.

La prévention des sanctuaires pour les criminels constitue donc un défi essentiel de la prévention de la cybercriminalité. Les sanctuaires permettent aux criminels de réaliser leurs activités et gênent le déroulement des enquêtes. On peut citer pour exemple le ver informatique "Love Bug" développé aux Philippines en 2000 et qui a affecté des millions d'ordinateurs dans le monde.

› Liens entre la criminalité organisée et la cybercriminalité

La nature de la participation de la criminalité organisée dans la cybercriminalité est double: l'utilisation de la technologie de l'information par les groupes traditionnels du monde de la criminalité organisée et les groupes du même monde qui se spécialisent dans la perpétration de cybercrimes.

Selon les informations dont on dispose, la tendance serait à l'implication des groupes organisés traditionnels dans la criminalité informatique tels que le piratage de logiciels, la pornographie impliquant des enfants et le vol d'identité.

› Quelles sont les mesures prises, et ce qui n'est pas fait

Plusieurs initiatives régionales ont été mises en place pour tenter d'élaborer et de normaliser la législation. Il s'agit notamment des suivantes.

La Commonwealth Model Law on Computer and Computer Related Crime contient des dispositions sur le droit pénal et procédural ainsi que sur la coopération internationale. Cependant, sa portée est limitée aux pays du Commonwealth.

L'Union européenne (UE) a également adopté plusieurs approches, y compris la Directive sur le commerce électronique, la Directive relative à la conservation des données et la Modification de la décision-cadre du Conseil relative à la lutte contre le terrorisme. Les 27 États membres sont tenus de mettre ces instruments en œuvre.

Le Conseil de l'Europe a élaboré trois instruments principaux pour harmoniser la législation sur la cybercriminalité. La plus connue est la Convention sur la cybercriminalité, élaborée entre 1997 et 2001. Elle contient des dispositions sur le droit pénal matériel, le droit procédural et la coopération internationale. Un premier Protocole additionnel à la Convention sur la cybercriminalité a été introduit en 2003.

En 2007, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels a été ouverte à la signature. Elle contient des dispositions particulières qui criminalisent l'échange de pornographie impliquant des enfants ainsi que l'obtention d'un accès, au moyen des technologies de communication, à cette forme de pornographie.

Il existe en outre plusieurs initiatives scientifiques telles que la Stanford Draft International Convention (CISAC), qui a été élaborée à titre de suivi d'une conférence accueillie par la Stanford University aux États-Unis en 1999, et l'ITU Cybercrime Legislation Toolkit (boîte à outils de l'UIT concernant la législation sur la cybercriminalité), qui a été élaboré par l'American Bar Association et autres experts. Cependant, l'impact mondial de ces approches est limité car elles ne sont applicables qu'à leurs États membres. Signée par 46 États et ratifiée par 26, la Convention sur la cybercriminalité du Conseil de l'Europe bénéficie de la portée la plus vaste.

Avec le nouveau phénomène de sécurité publique de l'Internet tel que l'utilisation de l'Internet par les terroristes à des fins de propagande, le financement du terrorisme au moyen de paiements liés à l'Internet et la collecte de renseignements au sujet d'une cible potentielle, il est plus urgent que jamais que les nations agissent collectivement.

Pour obtenir de plus amples renseignements, veuillez consulter les sites:

www.unis.unvienna.org

www.unodc.org

www.crimecongress2010.com.br

Les débats seront diffusés en direct sur le site:

www.un.org/webcast/crime2010