NATIONS UNIES
Office contre la drogue et le crime

www.unodc.org
www.11uncongress.org

Onzième Congrès des Nations Unies
pour la prévention du crime et la justice pénale
18-25 avril 2005, Bangkok (Thaïlande)

Fiche d'information 6

DÉLINQUANCE INFORMATIQUE

Les technologies de l'information et de la communication (TIC) apportent des changements dans les sociétés partout dans le monde: elles améliorent la productivité des industries traditionnelles, révolutionnent les méthodes de travail et remodèlent les flux de transfert des capitaux en les accélérant. Or cette croissance rapide a également rendu possibles de nouvelles formes de criminalité liées à l'utilisation des réseaux informatiques.

Il est difficile de bien saisir ou de conceptualiser où commence la criminalité liée à l'informatique. On considère souvent qu'elle constitue une conduite proscrite par la législation et/ou la jurisprudence et qui nécessite l'utilisation des technologies numériques dans la commission du délit; qui est dirigée contre les technologies de traitement des données et de communications elles-mêmes; ou qui fait intervenir l'utilisation accessoire d'ordinateurs en vue de la perpétration d'autres délits.

Les types de délits liés à l'informatique

- Nombreux types de délits liés à l'informatique visant les TIC elles-mêmes, comme les serveurs et les sites Web, les virus informatiques à diffusion mondiale engendrant des dégâts considérables dans les réseaux tant d'affaires que de grande consommation.
- Le vandalisme électronique et la fabrication professionnelle de faux ou de contrefaçons.
- Le vol ou la fraude, par exemple les attaques contre les systèmes électroniques des banques ou les systèmes financiers, et la fraude comportant des transferts de fonds électroniques.
- L'utilisation d'ordinateurs pour faciliter une large gamme de pratiques de démarchage à distance et des fraudes à l'investissement faisant intervenir des pratiques trompeuses.
- Le "*phishing*" ou l'envoi en masse de messages non sollicités contenant des liens avec des sites Web falsifiés pour apparaître authentiques aux consommateurs. Des millions de ces courriers frauduleux sont diffusés et prétendent provenir de banques, de sites de vente aux enchères en ligne ou d'autres sites légitimes à la seule fin de duper des utilisateurs et d'obtenir d'eux qu'ils répondent en confiant leurs coordonnées financières, personnelles ou leurs mots de passe.
- La diffusion de matériel illégal et nocif. Ces dernières années, l'Internet a été utilisé aux fins commerciales par l'industrie légitime du "divertissement pour adulte". Toutefois, l'Internet est maintenant de plus en plus utilisé pour la diffusion de matériel considéré comme juridiquement obscène dans plusieurs pays. Un autre sujet de préoccupation est la pornographie enfantine. Depuis la fin des années 80, les matériels sont de plus en plus diffusés via une gamme de réseaux informatiques, sous le couvert de différents services Internet, y compris des sites Web. Une part non négligeable de la diffusion de matériels de pornographie enfantine est liée à la criminalité transnationale organisée.
- Outre le fait que l'Internet est utilisé pour diffuser de la propagande haineuse et des messages xénophobes, il s'avère qu'il sert aussi à faciliter le financement des groupes terroristes et à diffuser la propagande terroriste.

La fracture numérique et la criminalité liée à l'informatique

La diffusion des TIC dans le monde n'est pas uniforme. Il existe des différences énormes dans le type et l'avancée des progrès technologiques entre les différentes régions du monde. Ce que l'on appelle la fracture numérique a été reconnue

comme telle dans la Déclaration du millénaire en 2000, qui formule huit objectifs de développement visant à réaliser des améliorations mesurables dans la vie de la plus grande partie de la population mondiale. L'un de ces objectifs, pour lequel il est appelé à renforcer les partenariats mondiaux pour le développement, appelle également à la coopération avec le secteur privé pour mettre à la disposition du plus grand nombre les avantages des nouvelles technologies — en particulier des TIC. Dans le même temps, à mesure que ces avantages commencent à se diffuser, il est nécessaire de mieux faire prendre conscience au plus grand nombre des menaces et des vulnérabilités liées à la criminalité informatique.

La Déclaration de principes adoptée par le Sommet mondial sur la société de l'information constate qu'aujourd'hui les avantages de la révolution des technologies de l'information sont inégalement distribués entre pays développés et pays en développement comme à l'intérieur de la société. Cette déclaration exprime aussi l'engagement à transformer cette fracture numérique en une perspective numérique pour tous, en particulier pour ceux qui risquent d'être laissés pour compte et, plus gravement encore, marginalisés.

Par-delà les frontières: criminalité transfrontière et investigation informatique

L'investigation des crimes liés à l'informatique n'est pas chose facile, vu que la majeure partie des indices sont intangibles et transitoires. Les enquêteurs en matière de cybercriminalité doivent rechercher des traces numériques qui sont souvent volatiles et de courte durée de vie. Les obstacles juridiques se dressent aussi en raison de questions de territorialité des juridictions. L'investigation et la poursuite des crimes liés à l'informatique mettent bien en relief l'importance et l'intérêt de la coopération internationale.

Solutions offertes par la coopération internationale

La densité croissante des TIC accroît également la fréquence des délits informatiques sur le territoire national, ce qui doit conduire les États à se doter d'une législation propre. Des lois nationales adaptées à la cybercriminalité peuvent être nécessaires pour répondre efficacement aux demandes d'assistance étrangères ou pour obtenir de l'aide d'un autre pays. La compatibilité avec les lois des autres États doit être un objectif essentiel dans l'élaboration de la législation; une coopération internationale est nécessaire en raison du caractère international et transfrontières de cette forme de criminalité. Des mécanismes internationaux officiels sont aussi nécessaires pour respecter les droits souverains des États et faciliter la coopération internationale. Pour qu'un régime d'entraide juridique fonctionne avec succès, les délits et les pouvoirs de procédure dans une juridiction donnée doivent être équivalents à ce qu'ils sont dans les autres juridictions.

Diverses initiatives ont été prises pour mieux faire prendre conscience de la problématique et promouvoir la coopération internationale dans la lutte contre la criminalité liée à l'informatique, notamment avec les actions menées par le Conseil de l'Europe, l'Union européenne, le Groupe des huit, l'Organisation de coopération et de développement économiques et l'Organisation des Nations Unies. Avec l'atelier qu'il consacrera à ce sujet, il est escompté que le Congrès offre une occasion privilégiée de discuter de manière détaillée des défis et des enjeux de la cybercriminalité et des mesures permettant de stimuler la coopération internationale pour la combattre.

Pour plus d'informations, veuillez consulter les sites Internet suivants:

www.unodc.org et www.unis.vienna.org

V.05-82112