Le Conseil de l'Europe et la cybercriminalité

La cybercriminalité – les faits

L'Internet a un impact sociétal considérable dans le monde entier. En 1999, on comptait 300 millions d'internautes. Il y en avait 600 millions en 2002 (chiffres de l'INSEAD/ Forum économique mondial : The Network Readiness Index 2003 – 2004).

Le commerce électronique est en train de décoller. Selon l'Economist (15 mai 2004), les achats en ligne des Américains devraient représenter, (en 2004) plus de 200 milliards de dollars ; et les Européens commencent à leur emboîter le pas.

L'Internet rend possible la mondialisation des marchés. Il suffit d'actionner une touche pour se constituer une clientèle potentielle dans le monde entier. Il en va de même pour le militant anti-mondialisation : il peut trouver des sympathisants par l'intermédiaire du Net.

La place importante prise par l'Internet rend les sociétés vulnérables. Le principal danger est celui de la cybercriminalité.

Les menaces quotidiennes vont des spams à la maltraitance des enfants, en passant par les virus, le piratage, le vol d'identité et la fraude.

Au nombre des menaces potentielles figure le cyber-terrorisme : on stoppe des infrastructures essentielles ou l'on utilise les ordinateurs comme des armes – on désactive des systèmes vitaux ou l'on menace des populations entières.

Les technologies de l'information et de la communication fournissent au crime organisé de nouveaux outils pour pratiquer le crime organisé (traditionnel), et de nouveaux outils pour de nouveaux types de criminalité.

Les groupes qui pratiquent le crime organisé utilisent l'Internet pour la fraude et le vol à grande échelle. Ils exploitent les différences entre les législations des divers pays.

L'Internet permet de blanchir plus facilement l'argent qui provient de la criminalité classique ; les méthodes utilisées sont, entre autres, la surfacturation ou la sous-facturation et les cyber-ventes aux enchères. Grâce à la banque électronique et à l'utilisation de l'argent électronique, il est plus facile de faire circuler l'argent sale.

L'Internet facilite les opérations anonymes et le travail en réseau avec d'autres criminels.

La cybercriminalité menace chacun d'entre nous – et pas seulement les internautes :

- Personnes physiques et personnes morales peuvent être victimes de fraude en utilisant l'Internet.

- Les pirates peuvent « voler » des informations bancaires en détournant des systèmes légitimes – par exemple en insérant des pages où le client est invité à communiquer des informations personnelles qui permettront d'accéder à ses liquidités.
- Les enfants deviennent des victimes de pédophiles.
- Les pirates mettent aussi en danger la vie des affaires – et la vie tout court – s'ils désactivent des systèmes par des attaques du type « refus de service ».

Le spam (publicité non sollicitée) n'est pas seulement une gêne ; il peut comporter un danger mortel s'il bloque le fonctionnement de systèmes essentiels dans les hôpitaux ou dans des centres de secours ; et il peut entraîner, pour les milieux d'affaires, des pertes se chiffrant par millions d'euros.

Des racistes et des fascistes diffusent leurs tracts haineux et fanatiques au moyen de leurs sites web ou de leurs spams.

Même si 99.9 % des 600 millions d'internautes utilisaient Internet pour la bonne cause, il resterait encore 600 000 délinquants potentiels.

Une poignée d'individus peut faire des ravages sur l'Internet ; des virus comme Sasser et I-love-you ont désactivé des systèmes essentiels dans le monde entier.

Selon le Internet Fraud Complaints Centre (Centre de réclamations concernant les fraudes par Internet) (chiffres de novembre 2003), le montant des dommages occasionnés par les cybercriminels en 2003 serait de l'ordre de 150 à 200 milliards d'euros.

La cybercriminalité pose de nombreux défis aux systèmes de police et aux systèmes de justice pénale.

Avec l'Internet, il est facile d'opérer à partir d'un espace judiciaire étranger, et en particulier à partir d'un espace où la réglementation et les moyens d'exécution sont faibles.

Les données circulent très rapidement et sont difficiles à pister.

Les autorités de police elles-mêmes peuvent être accusées de cybercriminalité. Des agents du FBI qui avaient utilisé des techniques de piratage pour démasquer deux « hackers» en Russie, ont dû eux-mêmes répondre d'infractions relevant de la cybercriminalité.

La cybercriminalité est parfois un concept mal défini, qui n'a pas la même signification dans toutes les sociétés. Cela ne facilite pas la coopération internationale.

La Convention du Conseil de l'Europe sur la cybercriminalité

Quelques faits

La Convention du Conseil de l'Europe sur la cybercriminalité, entrée vigueur le 1er juillet 2004, est le seul traité international contraignant existant à ce jour dans ce domaine. Elle sert de ligne directrice à tout Etat qui souhaite développer une législation nationale complète contre la cybercriminalité et de cadre à la coopération internationale entre les Etats Parties à la Convention.

Elle n'est pas limitée à l'Europe; d'autres pays y adhèreront probablement. Le Canada, le Japon, l'Afrique du Sud et les Etats-Unis ont signé la Convention. Les Etats-Unis l'ont également ratifiée.

A ce jour (12 mars 2007) elle a été signée par 43 pays (y compris cinq Etats non membres du Conseil de l'Europe) et ratifiée par 19.

La Convention est complétée par un Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (1er mars 2006). Trente et un pays ont signé ce protocole et 10 l'ont ratifié.

La Convention et son Protocole sont suivis par le Comité de la Convention sur la Cybercriminalité (T-CY).

Le Conseil de l'Europe aide les pays à ratifier et à mettre en œuvre ces traités à travers le Projet sur la cybercriminalité.

Pourquoi est-ce la bonne solution ?

Les sociétés ont besoin d'être protégées contre la cybercriminalité ; mais il faut qu'on puisse utiliser et développer comme il convient les technologies de l'information et de la communication ; et il faut que les gens aient la garantie de pouvoir s'exprimer librement.

S'il y a un crime qui requiert la coopération internationale, c'est bien la cybercriminalité. Les cybercriminels exploitent la possibilité de se jouer des frontières et d'exploiter les différences entre les législations nationales.

Il faut donner aux services de police et aux autorités de la justice pénale les moyens de prévenir et de combattre la cybercriminalité.

Les mesures de lutte contre la cybercriminalité doivent se fonder sur la loi ; et il est nécessaire que les lois soient harmonisées, ou du moins compatibles, pour permettre la coopération.

La Convention répond à ces besoins.

Elle offre un concept clair de la cybercriminalité en invitant les pays à criminaliser quatre types d'infractions, dans le souci de promouvoir une approche harmonisée :

- Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques – y compris l'accès illégal à un système informatique, l'interception illégale, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et l'abus de dispositifs.
- Les infractions informatiques – y compris la falsification informatique et la fraude informatique.
- Les infractions liées au contenu – à savoir, la pornographie enfantine (le Protocole à la Convention ajoute le racisme et la xénophobie).
- Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

Elle met en place des procédures pour rendre les enquêtes plus efficaces.

- En assurant la conservation immédiate des données informatiques.
- En habilitant les autorités à demander la communication de données informatiques spécifiées.
- En autorisant les enquêteurs à collecter les données relatives au trafic et à intercepter le contenu en temps réel.

Elle met en place des procédures et des systèmes grâce auxquels la coopération internationale fonctionne plus efficacement. Par exemple :

- Elle crée un réseau qui fonctionne 24 h sur 24, 7 jours sur 7, afin de pouvoir aider les enquêteurs à tout moment.
- Elle facilite l'extradition et les échanges d'informations spontanées.
- Elle aide les autorités d'un pays à collecter des données dans un autre pays, et elle facilite l'entraide judiciaire internationale.

La Convention se fonde sur les principes de la Convention européenne des Droits de l'Homme. Elle est soumise à plusieurs conditions et garanties. Ainsi, le droit d'expression des individus et leur droit à la vie privée ne seront pas sacrifiés.

La cybercriminalité est l'un des grands défis auxquels la société moderne est confrontée. Le Conseil de l'Europe est convaincu que la Convention est un moyen idéal, pour les gouvernements, d'anticiper les problèmes et de les résoudre, dans un effort commun pour sécuriser la population, en Europe et ailleurs.

www.coe.int/cybercrime et www.coe.int/economiccrime
Plus d'informations au : +33 3 88 41 25 60

COUNCIL OF EUROPE CONSEIL DE L'EUROPE