Nº 85-558-XIF au catalogue

Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police

Centre canadien de la statistique juridique

Statistique Canada Statistics Canada

Canada

Comment obtenir d'autres renseignements

Toute demande de renseignements au sujet du présent produit ou au sujet de statistiques ou de services connexes doit être adressée à : Centre canadien de la statistique juridique, appel sans frais 1 800 387-2231 ou (613) 951-9023, Statistique Canada, Ottawa, Ontario, K1A 0T6.

Pour obtenir des renseignements sur l'ensemble des données de Statistique Canada qui sont disponibles, veuillez composer l'un des numéros sans frais suivants. Vous pouvez également communiquer avec nous par courriel ou visiter notre site Web.

Service national de renseignements	**1 800 263-1136**
Service national d'appareils de télécommunications pour les malentendants	**1 800 363-7629**
Renseignements concernant le Programme des bibliothèques de dépôt	**1 800 700-1033**
Télécopieur pour le Progamme des bibliothèques de dépôt	**1 800 889-9734**
Renseignements par courriel	**infostats@statcan.ca**
Site Web	**www.statcan.ca**

Renseignements sur les commandes et les abonnements

Le produit no 85-558-XIF au catalogue est gratuit sur Internet. Les utilisateurs sont priés de se rendre à www.statcan.ca.

Normes de service à la clientèle

Statistique Canada s'engage à fournir à ses clients des services rapides, fiables et courtois, et ce, dans la langue officielle de leur choix. À cet égard, notre organisme s'est doté de normes de service à la clientèle qui doivent être observées par les employés lorsqu'ils offrent des services à la clientèle. Pour obtenir une copie de ces normes de service, veuillez communiquer avec Statistique Canada au numéro sans frais 1 800 263-1136.

Statistique Canada
Centre canadien de la statistique juridique

Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police

Document produit par Melanie Kowalski

Publication autorisée par le ministre responsable de Statistique Canada

Décembre 2002

Nº 85-558-XIF au catalogue
ISBN 0-662-88107-9

Périodicité : occasionnel

Ottawa

This publication is available in English upon request (Catalogue no. 85-558-XIE).

Note de reconnaissance

Le succès du système statistique du Canada repose sur un partenariat bien établi entre Statistique Canada et la population, les entreprises, les administrations canadiennes et les autres organismes. Sans cette collaboration et cette bonne volonté, il serait impossible de produire des statistiques précises et actuelles.

TABLE DES MATIÈRES

Page

SOMMAIRE 5

REMERCIEMENTS 5

INTRODUCTION 6

PARTIE I QU'EST-CE QUE LA CYBERCRIMINALITÉ? 6

PARTIE II LÉGISLATION CANADIENNE DE LA CYBERCRIMINALITÉ 7

PARTIE III ACTIVITÉS DE LUTTE CONTRE LA CYBERCRIMINALITÉ AUX ÉTATS-UNIS, AU ROYAUME-UNI ET AU CANADA 8
États-Unis 9
Royaume-Uni 9
Canada 10

PARTIE IV ACTIVITÉS DE COLLECTE DE DONNÉES AUX ÉTATS-UNIS, AU ROYAUME-UNI ET AU CANADA 11
États-Unis 11
Royaume-Uni 14
Canada 15

PARTIE V RÉSULTATS DES CONSULTATIONS DE LA POLICE 18

PARTIE VI POSSIBILITÉS DE COLLECTE DE DONNÉES AUPRÈS DE LA POLICE 23

PARTIE VII CONCLUSION 26

BIBLIOGRAPHIE 27

ANNEXE A 29

ANNEXE B 31

ANNEXE C 32

SOMMAIRE

Par cybercriminalité, on entend généralement les infractions criminelles ayant l'ordinateur pour objet ou pour instrument de perpétration principal. Le présent rapport jette un premier regard sur les enjeux, les sources de données et la faisabilité d'une collecte de données statistiques sur la cybercriminalité auprès de la police. Tout au long de cette étude, nous examinerons les possibilités de mise en place d'un mécanisme de collecte permanente, ainsi que la nature et l'ampleur du « cybercrime » au Canada.

Certains pays dans le monde sont actuellement en quête de moyens de garantir que la cybercriminalité fera l'objet d'une enquête et d'une déclaration appropriées. Ainsi, aux États-Unis, le « National Incident-Based Reporting System » (NIBRS) du « Uniform Crime Reporting System » comprend une catégorie qui met en évidence les crimes informatiques. Par le NIBRS, on peut ainsi indiquer si l'ordinateur a été l'objet d'un acte criminel ou si des délinquants se sont servis de matériel informatique pour perpétrer un crime.

Tout comme les recherches, les consultations menées auprès de la police canadienne montrent que les milieux policiers ne se sont pas entendus sur une définition uniforme de la cybercriminalité. Sur les 11 grands corps policiers consultés, 8 disposaient d'un service spécialisé d'enquête sur les cybercrimes pour lequel ils avaient élaboré des définitions, des politiques et des procédures. Sur ces 8 corps, 6 disposaient d'un système de collecte de données et autres renseignements sur les activités relevant de la cybercriminalité. Ceux qui ne recueillaient pas encore une telle information ont dit que la mise en place d'un mécanisme de collecte n'aurait pas pour effet d'accroître le fardeau de réponse outre mesure.

À la suite des consultations de la police, on a dégagé deux possibilités de collecte de données de cybercriminalité auprès des services de police du pays. La première serait de réaliser une étude spéciale où l'on recueillerait des renseignements détaillés auprès des services de polices qui observent statistiquement aujourd'hui le phénomène de la cybercriminalité. La deuxième consisterait à modifier le Programme DUC 2 (Programme de déclaration de la criminalité fondé sur l'affaire). Il s'agirait notamment d'ajouter un élément d'information permettant de reconnaître les actes criminels ayant l'ordinateur pour objet ou comme instrument de perpétration. On recommande que ces deux possibilités soient mises en œuvre pour répondre aux besoins en information à court et à long termes des organismes d'application de la loi, des décideurs et des législateurs.

REMERCIEMENTS

Le Centre canadien de la statistique juridique (CCSJ) apprécie l'aide et les services du Comité de l'information et de la statistique policières (CISP) de l'Association canadienne des chefs de police, ainsi que la collaboration des divers services de police canadiens qui ont participé à la démarche de consultation.

INTRODUCTION

La cybercriminalité est un problème national et international qui a une sérieuse incidence sur les organismes d'application de la loi à tous les échelons. Récemment, elle a eu droit à une attention accrue de la part des gouvernements fédéral, provinciaux et territoriaux et des milieux policiers. Nous ne disposons pas à ce jour de données nationales sur cette importante question. Dans la présente étude, nous examinerons la faisabilité d'une collecte de données sur la cybercriminalité auprès de la police en examinant les différentes méthodes actuellement employées aux États-Unis et au Royaume-Uni, ainsi que celles qu'appliquent certains corps policiers au Canada qui réunissent et stockent des données sur les « cybercrimes ». Nous nous attacherons aux définitions de la cybercriminalité, aux lois en place au Canada et à l'étranger, aux données qui existent, aux résultats des consultations de certains services de police et aux possibilités de collecte de données de cybercriminalité auprès des corps policiers.

PARTIE I – QU'EST-CE QUE LA CYBERCRIMINALITÉ?

Il n'y a pas encore de définition unique de la cybercriminalité à laquelle se reportent la majorité des services de police. Voici une définition de travail qui est de plus en plus acceptée par les organismes canadiens d'application de la loi. *« La cybercriminalité est la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale »*[1].

Généralement parlant, si on considère la définition élaborée par le Collège canadien de police et d'autres sources de données de recherche (Carter, 1995; Davis et Hutchison, 1997), il y aurait deux grandes catégories de cybercrimes. La première serait celle où l'ordinateur est l'instrument de perpétration. Elle comprendrait les crimes que les organismes de maintien de l'ordre ont combattus dans le monde matériel, mais combattent aussi aujourd'hui de plus en plus dans le monde virtuel d'Internet, qu'il s'agisse de pornographie enfantine, de harcèlement criminel, de fraude, de violation de la propriété intellectuelle ou de vente de substances ou de produits illicites.

La seconde catégorie est celle où l'ordinateur est l'objet du crime. Cette cybercriminalité consiste en crimes précis liés aux ordinateurs et à des réseaux. Ce sont de nouveaux actes criminels qui sont expressément liés à la technologie informatique et à Internet. À titre d'exemple, citons le piratage ou l'utilisation illicite de systèmes informatiques, la défiguration de sites Web ou la création et la propagation malveillante de virus informatiques.

Outre les cybercrimes, il y a les crimes favorisés par l'ordinateur dont les auteurs utilisent l'informatique pour la communication et le stockage de documents et de données. Ce genre de criminalité ne relève pas de la définition de la cybercriminalité que nous employons dans le présent rapport.

Lorsqu'il est question de sources d'information policières et d'autres sources, les termes « criminalité informatique », « crimes favorisés par ordinateur », « crimes technologiques », « cybercriminalité » et « criminalité par Internet » sont souvent interchangeables.

[1] *C'est la définition qu'offre le Collège canadien de police où les policiers sont formés à l'application des techniques informatiques d'enquête criminelle.*

PARTIE II – LÉGISLATION CANADIENNE DE LA CYBERCRIMINALITÉ

Pour les organismes d'application de la loi, une des difficultés de l'heure est justement d'appliquer les lois en place aux actes criminels mettant les nouvelles technologies en jeu. À la suite des engagements récemment créés par la Convention sur la cybercriminalité du Conseil de l'Europe, on s'efforcera d'arrêter des définitions internationales communes de certains actes criminels liés à l'utilisation des nouvelles technologies (on trouvera à la partie III un complément d'information sur cette convention).

Le Canada a été un des premiers pays à se doter de lois pénales dans le domaine de la criminalité informatique (Convention sur la cybercriminalité, 2001). D'après une étude réalisée par un réseau à parrainage onusien de responsables des politiques Internet, le Canada devance près des deux tiers des 52 pays observés pour ce qui est de la promulgation de lois destinées à combattre la cybercriminalité (Chu, 2000). Par des modifications apportées en 1985 au *Code criminel*, il a donné force de loi à ce qui était généralement considéré à l'époque comme tout un train de modificatifs portant sur la criminalité informatique : articles 342.1 (Utilisation non autorisée d'ordinateur), 430.(1.1) (Méfait concernant des données), 327 (Possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunication) et 326 (Vol de service de télécommunication). En 1997, il a apporté diverses modifications à son code pénal, ce qui comprend l'article 342.2 (Possession de moyens permettant d'utiliser un service d'ordinateur), par la Loi visant à améliorer la législation pénale.

Dans certains cas, les actes criminels traditionnels ont tout simplement évolué pour s'adapter à la nouvelle technologie. Par conséquent, le système de justice pénale doit aussi s'adapter. En outre, le Canada a créé des lois pour punir d'autres « crimes informatiques » comme la fraude et la contrefaçon informatiques. Dans d'autres situations, il a fallu apporter de légères modifications à la législation pénale pour s'assurer que les infractions sont définies de manière à tenir compte des nouveaux aspects technologiques de la criminalité et à autoriser les interventions nécessaires des organismes d'application de la loi. Ainsi, la possession de pornographie enfantine est déjà interdite par la loi au Canada; toutefois, les lois ont été modifiées afin de proscrire le téléchargement et la visualisation d'une telle pornographie sur Internet.

La loi C-15A, qui a reçu la sanction royale le 10 juin 2002, comprend des dispositions des lois canadiennes en matière de pornographie enfantine qui visent à prévenir la prolifération de cette dernière dans Internet et par d'autres technologies avancées de communication. Elle fait une infraction des activités de transmission et de mise à disposition de la pornographie enfantine ainsi que du fait d'y accéder. Elle fait de même pour l'activité consistant à faciliter un acte criminel contre un enfant. Elle confère enfin aux juges canadiens le pouvoir d'interdire les sites de pornographie enfantine au pays et d'ordonner la confiscation des contenus ou des ordinateurs employés à cette fin.

Loi C-15A

Pour une meilleure protection de l'enfance contre l'exploitation sexuelle :

- elle crée une infraction pour l'activité consistant à utiliser Internet pour détourner et exploiter les enfants à des fins sexuelles;
- elle fait un acte criminel de l'activité consistant à transmettre, à mettre à disposition, à exporter et à intentionnellement diffuser de la pornographie enfantine dans Internet;
- elle permet aux juges d'ordonner la confiscation de tout matériel ou ordinateur servant à la perpétration d'un acte de pornographie enfantine;
- elle rend les juges plus capables de garder les délinquants sexuels connus loin des enfants par des ordonnances d'interdiction, des désignations en surveillance de longue durée ou des ordonnances de bonne conduite d'un an à l'égard des infractions liées à la pornographie enfantine et à Internet;
- elle modifie la loi promulguée en 1997 sur le tourisme sexuel contre les enfants en simplifiant la procédure de judiciarisation des Canadiens commettant des actes d'agression sexuelle contre les enfants dans d'autres pays.

Source : *Ministère de la Justice Canada, 2002.*

PARTIE III – ACTIVITÉS DE LUTTE CONTRE LA CYBERCRIMINALITÉ AUX ÉTATS-UNIS, AU ROYAUME-UNI ET AU CANADA

Internet est aujourd'hui accessible dans plus de 200 pays et, comme ce système ne connaît pas de frontières, des crimes peuvent se commettre par des communications acheminées par un certain nombre de pays (President's Working Group on Unlawful Conduct on the Internet, 2000). Une des grandes difficultés avec le phénomène de la cybercriminalité est que le criminel peut commettre son crime à partir de tout pays, s'attaquer à ses victimes partout dans le monde, dissimuler son identité en faisant passer ses communications par des systèmes informatiques situés dans un grand nombre de pays étrangers et stocker en des lieux éloignés les données relatives à ses agissements. La capacité de contrôler les communications qui passent par une diversité de réseaux informatiques dans une diversité de pays est un facteur critique de prévention, d'enquête et de pénalisation en matière de cybercriminalité (Groupe de travail fédéral-provincial-territorial sur le contenu illégal et offensant dans Internet, 2001). On ne s'étonnera donc pas que les mesures destinées à combattre la cybercriminalité fassent largement appel à la coopération internationale.

C'est l'Organisation de coopération et de développement économiques qui, dans les années 1970, y est allée des premiers efforts concertés sur le plan international en vue de s'attaquer aux problèmes de la criminalité informatique. Elle s'est considérablement efforcée de préciser ce qu'on devait entendre par criminalité informatique et d'élaborer des directives pour une meilleure harmonisation des lois portant sur cette criminalité. Elle jugeait cette harmonisation nécessaire pour une répression efficace de ce qui constituait une activité criminelle internationale dans une large mesure.

Tout récemment en 2001, le Canada et 29 autres pays ont signé la Convention sur la cybercriminalité du Conseil de l'Europe. Toutefois, la plupart des pays, y compris de Canada, n'ont pas encore ratifié le premier instrument multilatéral qui a pour objet d'aborder les problèmes causés par la propagation de l'activité criminelle par les réseaux informatiques (Convention sur la cybercriminalité, 2001). Cette convention exige des parties signataires qu'elles adoptent des lois contre la cybercriminalité, veillent à ce que les organismes d'application de la loi aient, en matière de procédure, les pouvoirs nécessaires d'enquête et de poursuites contre les cybercriminels et, par la collaboration internationale, appuient les autres parties dans leur lutte contre la criminalité informatique.

La Convention sur la cybercriminalité est le premier traité international portant en général sur les crimes par Internet et les autres réseaux informatiques et en particulier sur les violations de la propriété intellectuelle, les fraudes informatiques, la pornographie enfantine et les atteintes à la sécurité des réseaux. On y trouve en outre un ensemble de pouvoirs et de procédures de fouille et d'interception dans les réseaux informatiques, par exemple.

Ajoutons que les efforts du Groupe des Sept, puis du Groupe des Huit depuis 1996 illustrent l'engagement pris par la communauté internationale de s'attaquer aux questions multinationales qui se posent dans le domaine de la cybercriminalité. Ainsi, le sous-groupe de la criminalité technologique du groupe Lyon (anciennement le groupe d'experts sur la criminalité transnationale organisée) s'intéresse aux questions technologiques internationales. Il essaie d'amener les pays à se concerter dans la lutte internationale contre la criminalité informatique.

Lors de la réunion des ministres de la justice et de l'intérieur des pays du Groupe des Huit qui a eu lieu au Mont Tremblant en mai 2002, les ministres ont entériné les recommandations révisées du Groupe des Huit sur la criminalité transnationale; les recommandations sur le dépistage de communications acheminées par réseau entre les pays dans le cadre d'enquêtes criminelles et terroristes ainsi qu'un certain nombre d'autres documents qui aideraient les gouvernements à lutter contre le problème de la criminalité technologique.

États-Unis

Les États-Unis ont pris leurs premières mesures dans le dossier de la cybercriminalité en 1984 lorsqu'ils ont adopté une première loi (la *Computer Fraud and Abuse Act* [18 U.S.C. 1030]), portant directement sur les attaques de systèmes informatiques. En 1991, le Département de la Justice créait un service spécialisé dans les questions de criminalité informatique. La Computer Crime and Intellectual Property Section évalue ainsi ces problèmes, propose des solutions par les lois et les politiques et poursuit les délinquants.

En 2001, le Département de la Justice a proposé d'instituer neuf services spécialisés de poursuites contre les cybercriminels. Les nouvelles équipes appelées « Computer Hacking and Intellectual Property Units » auront pour point de mire les crimes technologiques par piratage informatique, les vols d'ordinateurs et autres appareils de haute technologie, les fraudes et violations de propriété intellectuelle et commerciale, les divulgations de secrets commerciaux et l'espionnage économique. À ce jour, cinq de ces services sont en activité sur le territoire américain.

Le Federal Bureau of Investigation (FBI) a aussi pris diverses mesures de lutte à la cybercriminalité. En février 1998, il chargeait un National Infrastructure Protection Center de combattre, par détection, évaluation et enquête, les menaces et les actes de détournement importants contre les infrastructures essentielles. En cours d'enquête, on devait de plus en plus constater dans ce cas que l'acte d'infiltration n'était en fait que le premier pas dans une démarche criminelle plus traditionnelle ayant pour objet la fraude ou l'obtention irrégulière d'un gain financier (Kubic, 2001). C'est ce qui s'était passé dans de nombreux cas de pénétration illicite dans les bases de données de sociétés émettrices de cartes de crédit, d'institutions financières, etc.; le but était d'y recueillir des données de carte de crédit ou d'autres données d'identité et par la suite de s'en servir pour escroquer des particuliers ou des entrepreneurs. Mentionnons enfin que le FBI continue à créer et à déployer des équipes de lutte contre la cybercriminalité qui se composent d'enquêteurs et de personnes-ressources des autres organismes fédéraux, des organismes des États et des organismes locaux. Dans le domaine de la cybercriminalité, les États-Unis ont également participé avec enthousiasme aux réunions des ministres de la justice et de l'intérieur des pays du Groupe des Huit et à la réunion du Conseil de l'Europe concernant la Convention sur la cybercriminalité.

Royaume-Uni

En juin 1999, un « Internet Crime Forum » voyait le jour au Royaume-Uni avec des représentants du gouvernement, des organismes d'application de la loi et de l'industrie Internet. Le but général était d'établir et d'entretenir des relations de travail entre l'industrie des fournisseurs de services Internet et les services de maintien de l'ordre au Royaume-Uni, de sorte que les enquêtes criminelles puissent se mener en tout respect de la loi et en toute rapidité et efficience, mais aussi avec le souci de sauvegarder la confidentialité des communications légitimes et de nuire le moins possible aux affaires de l'industrie (Internet Crime Forum, mars 2001).

Il n'y a pas que les questions indiquées au Forum, puisqu'on a conçu, en matière de criminalité technologique, une stratégie nationale comportant une évaluation des risques stratégiques (Project Trawler), exercice que le National Criminal Intelligence Service a rendu public en 1999. Le « Projet Trawler » a permis de déceler des lacunes importantes dans les capacités d'enquête au double palier local et national et de renseigner les décideurs sur la menace que pouvait représenter la criminalité technologique. C'est en réaction à la constatation de ces lacunes que la première « National Hi-Tech Crime Unit » est entrée en activité en avril 2001.

On a vu dans des services téléphoniques grand public, comme l'Internet Watch Foundation du Royaume-Uni, un mécanisme efficace de réception des plaintes au sujet du contenu du World Wide Web et des « groupes de discussion » Usenet. Ces services créeront aussi un réseau de liaison avec les corps policiers de l'étranger dans le sens même des engagements pris par le Royaume-Uni lors de la réunion des ministres de la justice et de l'intérieur des pays du Groupe des Huit qui a eu lieu au Mont Tremblant en mai 2002 et du travail qu'il a réalisé lors de la réunion du Conseil de l'Europe concernant la Convention sur la cybercriminalité.

Canada

Le Canada est activement présent dans divers organismes internationaux comme le groupe d'experts sur la criminalité transnationale organisée du Groupe des Huit, le Comité d'experts sur la criminalité dans le cyberespace du Conseil de l'Europe et le groupe des experts gouvernementaux sur la cybercriminalité de l'Organisation des États américains.

Le gouvernement canadien accueille des sommets mondiaux et réalise des études internationales. Il a également prêté main-forte à l'élaboration de la Convention sur la cybercriminalité au Conseil de l'Europe. L'Association canadienne des fournisseurs Internet partage l'information avec les fournisseurs Internet en Europe et collabore avec les autres pays à la recherche de solutions internationales.

En 2001, le gouvernement fédéral a créé le Bureau de protection de l'infrastructure essentielle et de la protection civile (BPIEPC), qui ressemble au programme américain précité de sécurité des infrastructures. À l'échelle nationale, le BPIEPC oriente les activités servant à protéger l'infrastructure critique du Canada — qu'il s'agisse des dimensions physique ou cybernétique — sans tenir compte de l'origine des menaces et des vulnérabilités. Le BPIEPC travaille en collaboration avec plusieurs ministères, en particulier avec le Solliciteur général Canada, afin d'élaborer une approche globale pour protéger notre infrastructure critique et prendre des mesures à l'égard des incidents.

On compte diverses autres grandes initiatives en place pour les questions de contenu Internet illégal ou offensant. En 1997, un groupe de travail fédéral-provincial-territorial du même nom a été chargé de l'examen de tout ce qui est utilisation illicite des nouvelles technologies des communications. Il était plus particulièrement question d'Internet et de son rôle dans la distribution de matériel illégal ou offensant, qu'il s'agisse de pornographie enfantine, de contenu obscène ou de propagande haineuse. Dans le cadre de cette initiative, le groupe de travail sur la cybercriminalité s'est intéressé au phénomène du détournement commercial par Internet qui, sous certaines de ses formes, peut être considéré comme une activité criminelle, et de la communication avec des enfants aux fins de l'exploitation sexuelle. Son point de mire est le droit pénal et les nouvelles technologies. Il s'agit entre autres de procurer aux organismes d'application de la loi les instruments et le cadre législatif pouvant leur permettre de lutter contre la cybercriminalité — en particulier la pornographie enfantine sur Internet.

Il existe une stratégie interministérielle fédérale appelée « Stratégie canadienne pour promouvoir l'utilisation sécuritaire, prudente et responsable d'Internet » qui offre à l'utilisateur final un modèle de lutte contre les activités illicites qui s'exercent dans Internet. L'objectif est de faire l'éducation des Canadiens dans tout ce qui est contenu Internet offensant ou illégal et de leur donner les moyens d'intervenir dans leur propre foyer. C'est aussi une stratégie qui a amené le gouvernement canadien et le secteur privé à étudier les coûts et les avantages de la création d'un service téléphonique canadien auquel serait signalé tout contenu Internet illégal.

Le Comité fédéral-provincial-territorial sur les mesures liées à la consommation a constitué un Groupe de travail sur les consommateurs et le commerce électronique et lui a confié le mandat d'examiner les questions de cybercommerce et les possibilités d'éducation du consommateur, d'autoréglementation de l'industrie et de protection des consommateurs par le législateur.

PARTIE IV – ACTIVITÉS DE COLLECTE DE DONNÉES AUX ÉTATS-UNIS, AU ROYAUME-UNI ET AU CANADA

États-Unis

Voici certains des moyens nationaux de collecte de données sur la criminalité informatique aux États-Unis :

1) « National Incident-Based Reporting System » (NIBRS) dans le cadre du système américain UCR de déclaration uniforme de la criminalité;
2) enquête nationale sur les victimes d'actes criminels (« National Victimization Survey »);
3) enquête sur la criminalité et la sécurité informatiques (« Computer Crime and Security Survey »);
4) centre des plaintes pour fraude dans Internet (« Internet Fraud Complaint Center »);
5) autres programmes planifiés.

1. Système national de déclaration uniforme de la criminalité fondé sur l'affaire (NIBRS-UCR)

Le système américain NIBRS-UCR recueille des données sur les affaires et les arrestations criminelles qui viennent des dossiers des organismes d'application de la loi (cette enquête ressemble au Programme DUC 2 canadien). Le NIBRS comprend une catégorie de données qui appréhende les affaires relevant de la criminalité informatique.

Les responsables du programme national UCR pensent que la criminalité informatique consiste en réalité en crimes habituels de vol, de détournement de fonds, de violations de propriété, qui se commettent aujourd'hui par un nouvel instrument, l'ordinateur. Si les vols, détournements de fonds et violations de propriété par l'ordinateur devaient être déclarés dans une nouvelle catégorie appelée « criminalité informatique », les séries chronologiques courantes du programme national UCR qui portent sur ces actes criminels s'en trouveraient déformées.

C'est pour prévenir une telle déformation que le NIBRS prévoit la capacité d'indiquer si l'ordinateur a été l'objet d'un crime ou en a été l'instrument de perpétration (voir l'encadré « Le NIBRS et la criminalité informatique » dans le texte). Par un tel élément d'information, on dirait si, dans une affaire, un délinquant est soupçonné d'avoir utilisé un ordinateur, un terminal ou un autre produit informatique pour perpétrer son crime (voir la formule de déclaration des affaires à l'annexe A).

Sur les 45 950 crimes informatiques signalés par le NIBRS en l'an 2000[2], 5 744 mettaient en cause l'ordinateur comme instrument et 40 211, comme objet. Pour l'une et l'autre des définitions, le crime le plus courant était le vol. Le tableau 1 ventile les actes criminels indiqués par le NIBRS dont l'ordinateur a respectivement été l'instrument de perpétration et l'objet.

2. Enquête nationale sur les victimes d'actes criminels

Les enquêtes sur les victimes d'actes criminels sont un autre moyen de se renseigner sur les affaires et les actes criminels. Par les soins du Bureau of Justice Statistics, le département de la Justice des États-Unis se renseigne, dans le cadre de l'enquête nationale sur les victimes d'actes criminels (National Crime Victimization Survey [NCVS]), sur les actes criminels dont sont victimes les personnes et les ménages et constate si ceux-ci ont été dénoncés ou non à la police. Dans son questionnaire de 2001 sur les affaires, la NCVS interroge les enquêtés sur la criminalité informatique,

[2] *En l'an 2000, le NIBRS rendait compte de 13 % des services de police aux États-Unis et, par ces services, de 16 % de la population américaine.*

Le NIBRS et les crimes informatiques :

Le NIBRS permet d'indiquer si l'ordinateur a été l'objet ou l'instrument de perpétration d'un crime.

1. Ordinateur comme objet du crime :

Élément d'information 15 — **DESCRIPTION DES BIENS** — entrer 07 = Matériel informatique/logiciels, par quoi on entend les ordinateurs, des périphériques comme les unités de bande ou de disque et les imprimantes et des supports de stockage comme les bandes magnétiques ou les disques magnétiques ou optiques.

2. Ordinateur comme instrument de perpétration du crime :

Élément d'information 8 — **DÉLINQUANT SOUPÇONNÉ D'UTILISER** — entrer C = Matériel informatique

Par exemple, 1) un pirate informatique s'est servi de son micro-ordinateur et d'un modem pour pénétrer dans l'ordinateur d'une entreprise et voler des données confidentielles; on devrait alors entrer C = Matériel informatique; 2) un domicile a été cambriolé et un micro-ordinateur y a été volé avec d'autres articles; on ne doit pas entrer C = Matériel informatique, parce que l'ordinateur n'a pas servi à la perpétration du crime, bien qu'en étant un des produits.

Source : *Federal Bureau of Investigation, 2000.*

Tableau 1
Crimes informatiques selon la nature, 2000, États-Unis[1]

	Ordinateur comme :	
	Instrument	Objet
Voie de fait	878	282
Agression sexuelle	73	15
Enlèvement ou rapt	12	32
Agression sexuelle avec consentement	5	0
Meurtre ou homicide involontaire sans négligence	0	1
Crimes contre la personne	**968**	**330**
Narcotiques	605	606
Armes à feu	36	52
Pornographie ou obscénité	108	1
Jeux de hasard	6	4
Prostitution	9	0
Crimes contre la société	**764**	**663**
Vol	1 589	19 950
Destruction détérioration ou vandalisme	485	2 990
Vol avec effraction	373	14 174
Fraude	756	595
Faux et usage de faux	525	293
Vol de véhicule automobile	110	386
Détournement de fonds	84	277
Vol qualifié	37	220
Vol de biens	31	283
Incendie volontaire	10	39
Extorsion ou chantage	7	10
Corruption	5	1
Crimes contre les biens	**4 012**	**39 218**
Total	**5 744**	**40 211**

[1] *Il y a 69 organismes qui ont produit des données où le délinquant était soupçonné d'avoir utilisé du matériel informatique; 102 organismes ont produit des données où le matériel informatique/logiciel était l'objet du crime en l'an 2000. Le NIBRS rend compte de 13 % des services de police aux États-Unis et, par là, de 16 % de la population américaine.*

Source : *« National Incident-Based Reporting System », Federal Bureau of Investigation, département de la Justice des États-Unis.*

pose notamment des questions sur l'utilisation d'ordinateurs et s'enquiert de l'expérience vécue de la cybercriminalité (voir les détails à l'annexe B). Une fois disponibles, ces résultats nous éclaireront sur la nature des crimes qui se commettent par Internet.

3. Enquête sur la criminalité et la sécurité informatiques

Le Computer Security Institute réalise tous les ans à titre de service public l'enquête sur la sécurité et la criminalité informatiques avec le concours du service d'enquête sur le piratage informatique des bureaux de San Francisco du Federal Bureau of Investigation. Il s'agit d'aider à sensibiliser les gens aux questions de sécurité et de juger de l'ampleur de la criminalité informatique sur le territoire américain. On s'intéresse à l'importance et à la nature de cette criminalité et fait le bilan des prévisions de pertes pécuniaires des enquêtés qui se prêtent à l'exercice. Les résultats de l'enquête de 2001 indiquent (par les réponses obtenues de 538 praticiens du domaine de la sécurité informatique) que 91 % des organismes gouvernementaux et des grandes sociétés aux États-Unis ont constaté dans la dernière année des violations de cette sécurité (Power, 2001).

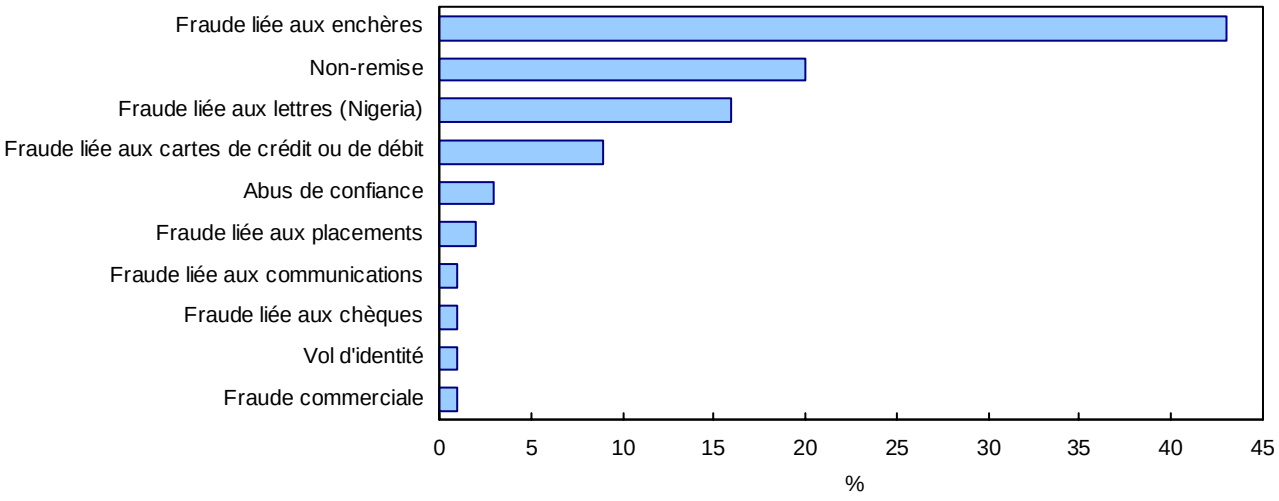
4. Centre des plaintes pour fraude dans Internet

En mai 2001, l'« Internet Fraud Complaint Center » (IFCC), créé par le FBI et le National White Collar Crime Center (organisme sans but lucratif financé par le Congrès), a établi un service en ligne. Il se veut un centre de réception des plaintes pour fraude dans Internet et se sert des indications reçues pour quantifier les tendances du phénomène et fournir des données statistiques à jour sur les tendances dégagées (voir dans l'encadré qui suit une description des principaux types de fraudes Internet dénoncés).

En 2001, l'IFCC a reçu 49 711 plaintes à son site Web pour des questions de piratage, de courrier électronique non sollicité ou de pornographie enfantine. L'infraction qui était le plus fréquemment déclarée était la fraude d'enchères dans Internet, qui représentait 43 % des plaintes reçues (voir la figure 1).

Figure 1

Plaintes liées aux fraudes dans Internet les plus fréquemment signalées, États-Unis, 2000



Source : *Internet Fraud Complaint Center, 2001.*

Principaux types de fraudes Internet déclarés à l'IFCC

Enchères et ventes au détail en ligne — On incite les victimes à envoyer de l'argent pour obtenir les articles promis, mais on ne leur expédie rien ensuite ou seulement un article de moindre valeur que celui qui avait été promis (marchandises contrefaites ou dénaturées, par exemple).

Offre en ligne d'une activité commerciale ou d'un travail à la maison — Il s'agit d'ordinaire d'exiger un paiement d'un particulier, mais sans pour autant lui remettre les produits ou lui communiquer les renseignements qui permettraient de faire de ce travail à la maison une activité viable.

Abus de confiance — Abus de la discrétion et/ou de la confiance qui cause une perte pécuniaire.
Vol et fraude de données d'identité — Obtention et utilisation illicites de données personnelles en vue d'une fraude ou d'une tromperie, d'ordinaire pour un gain économique.

Sollicitation en ligne de placements — Pratiques trompeuses visant à un placement dans des instruments qui produisent un revenu ou dans des entreprises plus risquées devant mener à un gain en capital.

Fraude de carte de crédit — Obtention illicite de numéros de carte de crédit pour des commandes de biens ou de services en ligne.

Source : *Internet Fraud Complaint Center, 2001.*

5. Autres programmes prévus

En complément aux sources de données que nous venons de décrire, le Bureau of Justice Statistics (BJS) a entrepris en l'an 2000 de mettre au point une stratégie d'élaboration d'un programme statistique destiné à mesurer l'évolution de la fréquence, de l'ampleur et des conséquences de la criminalité électronique ou cybercriminalité. On a proposé d'appréhender par ces statistiques les crimes tant contre la personne que contre les biens, depuis les menaces et le harcèlement par courrier électronique jusqu'au détournement ou à l'utilisation illicite de réseaux en vue d'une fraude ou d'un vol (Bureau of Justice Statistics, 2002). Le BJS, le Census Bureau et des représentants du monde des affaires et des milieux universitaires étudieront les questions qui se posent et concevront un programme de collecte de données statistiques sur la cybercriminalité.

Actuellement, le Census Bureau mène une enquête-pilote sur la criminalité informatique au sein des entreprises. Si cette enquête-pilote se révèle un succès, l'enquête réelle sera réalisée auprès d'environ 36 000 entreprises dès l'automne 2003 afin d'évaluer la nature et l'étendue des crimes informatiques contre les entreprises. Cette enquête servira à recueillir de l'information sur la fréquence et les types de crimes informatiques qui ont été commis, sur les frais liés à la sécurité informatique et sur les pertes financières subies (U.S. Census Bureau, 2002).

Royaume-Uni

L'outil principal de collecte de données sur la criminalité par Internet est la British Crime Survey (BCS) qui s'adresse aux victimes d'actes criminels. Celle-ci mesure l'ampleur de la criminalité en Angleterre et au pays de Galles en s'enquérant auprès des gens des actes criminels dont ils ont pu être victimes dans la dernière année. Dans la reprise 2001 de cette enquête, on a ajouté des questions sur les aspects suivants :

- utilisation de cartes de crédit et lieux de cette utilisation (notamment dans Internet);
- degré d'inquiétude des gens au sujet de chacun des lieux d'utilisation de cartes de crédit;
- fraudes liées à des cartes de crédit ou à des cartes bancaires;
- recours à Internet pour l'achat de marchandises;
- précautions prises au moment d'acheter des marchandises dans Internet;
- souci des attaques par virus et des pénétrations illicites dans des fichiers (au travail comme au foyer);
- expérience vécue des attaques par virus;
- préoccupations au sujet de la transmission par Internet de contenus pornographiques ou offensants sans le consentement du destinataire;
- réception de matériel pornographique ou offensant.

Grâce aux réponses à ces questions, on comprendra mieux le phénomène de la cybercriminalité au R.-U.

Un autre moyen auquel le Royaume-Uni a recours pour rendre compte de tout contenu illégal dans Internet est l'Internet Watch Foundation (IWF), organisme qui évalue les contenus signalés par la population pour ensuite aviser les fournisseurs de services et la police. Les seuls objets de son attention sont toutefois la pornographie enfantine, les contenus pour adultes qui vont à l'encontre de l'*Obscene Publication Act* et les contenus racistes pénalisables. Les statistiques les plus récentes indiquent qu'en 1999, l'IWF a signalé 19 710 cas de contenu illicite; il s'agissait presque invariablement de cas de pornographie enfantine (99 %).

Canada

À l'heure actuelle, le Canada n'a pas de méthode uniforme de collecte de données semblables. Bien que de portée restreinte, le Programme DUC 2.1 (Déclaration uniforme de la criminalité), qui est fondé sur l'affaire, et l'Enquête sur les tribunaux de juridiction criminelle pour adultes renseignent sur quelques infractions au *Code criminel* qui relèvent de la cybercriminalité. Ajoutons que les enquêtes auprès des ménages de Statistique Canada et le sondage « Les enfants du Canada dans un monde branché » du Réseau Éducation-Médias que finance le gouvernement fédéral (étude élaborée par l'Environics Research Group) s'attachent aux tendances de l'utilisation d'Internet dans les familles canadiennes.

1. Enquête sociale générale 2000

Dans le cadre de l'Enquête sociale générale 2000 (ESG)[3], on a recueilli des données détaillées sur l'usage que font les particuliers de la technologie. Il ne s'agissait pas dans cette enquête de se renseigner expressément sur la cybercriminalité, mais on y a obtenu des indications sur les questions de contenu offensant et de sécurité dans Internet (voir « Mesure de la cybercriminalité par l'ESG » à l'annexe C).

En 2000, 53 % des Canadiens âgés de 15 ans et plus ont dit avoir utilisé Internet à la maison, au travail ou ailleurs dans les 12 derniers mois. C'était considérablement plus (53 % contre 18 %) qu'en 1994 (Statistique Canada, mars 2001).

Tout ce qui est contenu offensant — ce qui comprend l'obtention et la distribution de matériel à caractère d'obscénité, de propagande haineuse ou de pornographie — continue à inquiéter tant les organismes chargés de la justice pénale que les parents de jeunes enfants. Voici dans leurs grandes lignes les résultats de l'ESG 2000 :

- 6 % des parents ont dit que leur enfant avait été mis en présence d'un contenu offensant dans Internet;
- 49 % (la moitié environ) des Canadiens ont rencontré des sites Web qui présentaient de la pornographie et, sur ce nombre, 83 % l'ont fait par accident et 46 % ont jugé ce contenu offensant;
- 13 % des utilisateurs d'Internet avaient été mis en présence d'un contenu qui incitait à la haine ou à la violence contre un groupe en particulier;
- 8 % des Canadiens utilisateurs d'Internet ont subi des menaces ou un harcèlement par courrier électronique.

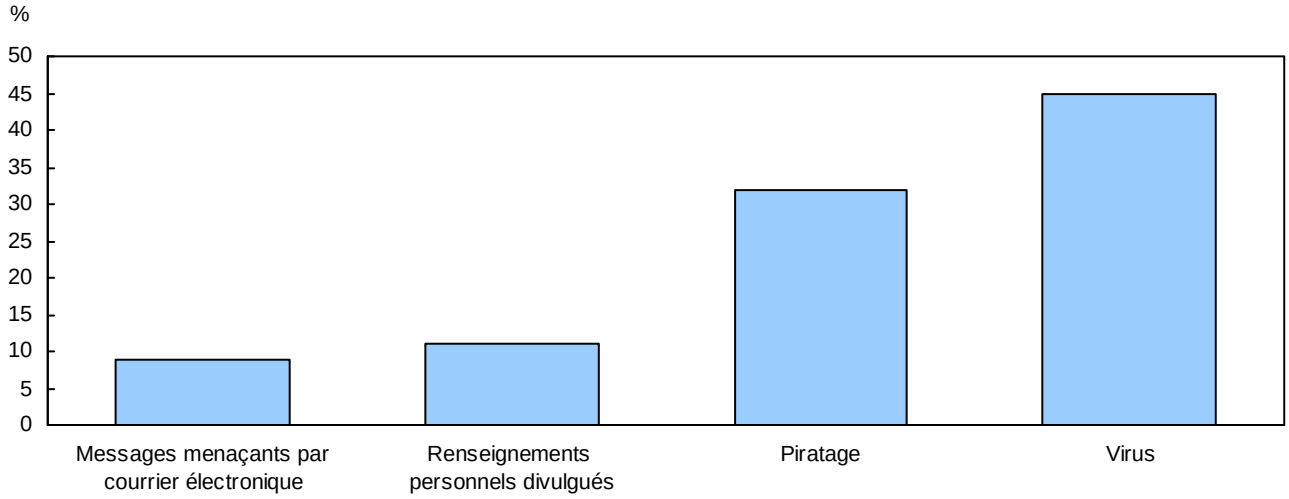
D'après les résultats de l'ESG, 5 % des Canadiens qui ont utilisé Internet dans la dernière année ont connu des problèmes de sécurité. Il y a 45 % des répondants qui ont évoqué des problèmes de virus; 32 % ont mentionné le piratage de comptes de courrier électronique ou de fichiers informatiques, 11 % une divulgation de renseignements personnels et 9 % des menaces par courrier électronique (voir la figure 2; se reporter à la question 4 de « Mesure de la cybercriminalité par l'ESG » à l'annexe C).

---

[3] *L'ESG est une enquête annuelle par sondage téléphonique auprès de la population de 15 ans et plus de toutes les provinces sans les pensionnaires d'établissement. Le volet de cette enquête qui porte sur la technologie est réalisé tous les cinq ans. Les données de la reprise 2000 de cette enquête ont été recueillies sur les 12 mois compris entre janvier et décembre 2000. L'échantillon représentatif comptait 25 090 personnes et le taux de réponse s'est établi à 81 %.*

Figure 2

Problèmes de sécurité dans Internet, Canada, 2000



Source : *Enquête sociale générale, cycle 14, 2000.*

2. Enquête auprès des ménages sur l'utilisation d'Internet

Dans cette enquête de Statistique Canada auprès d'un sous-échantillon de ménages de l'Enquête sur la population active, on s'enquiert de l'usage que font d'Internet les ménages canadiens. Les données les plus récentes issues de cette enquête indiquent que l'utilisation d'Internet par un membre du ménage (que ce soit à la maison, au travail ou à l'école) a monté de 51 % en 2000 à 60 % en l'an 2001. Ces personnes ont plus souvent accès à Internet et y ont des séances de consultation plus longues, bien que la protection des renseignements personnels demeure un sujet d'inquiétude pour la majorité des répondants. Près de 60 % des utilisateurs ont dit nourrir de telles inquiétudes à propos d'Internet. Les répondants qui ont déclaré être des utilisateurs réguliers au foyer ont précisé s'inquiéter des contenus que risquaient de visualiser les enfants à la maison, et notamment des contenus pornographiques (80 %) (Statistique Canada, juillet 2002).

3. Les enfants du Canada dans un monde branché : le point de vue des parents

Le sondage national Les enfants du Canada dans un monde branché mené en l'an 2000 par le Réseau Éducation-Médias — financé par Industrie Canada en collaboration avec Santé Canada et Développement des ressources humaines Canada — a révélé que 51 % des parents utilisateurs d'Internet s'inquiètent le plus, dans l'utilisation d'Internet par leurs enfants, de ce que ceux-ci soient mis en présence de contenus fâcheux (incluant la pornographie, la violence et la propagande haineuse). De plus, 18 % des parents ont dit se préoccuper le plus de communications interactives comme le clavardage et 23 % ont déclaré en revanche n'avoir pas du tout d'inquiétudes (Réseau Éducation-Médias et Environics Research Group, 2000).

4. Enquête sur les tribunaux de juridiction criminelle pour adultes (ETJCA)

L'ETJCA renseigne sur les accusations d'infraction aux lois fédérales devant les tribunaux pénaux pour adultes et les cours supérieures des provinces et des territoires. Les données englobent sept provinces et un territoire et, à l'échelle nationale, elles représentent 80 % des causes soumises aux tribunaux pour adultes. Voici les infractions au *Code criminel* qui sont actuellement visées dans le domaine de la criminalité technologique (voir le code pénal pour plus de détails) :

– utilisation non autorisée d'ordinateur — article 342.1;
– possession de moyens permettant d'utiliser un service d'ordinateur — article 342.2;
– possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunication — article 327;

– méfait concernant des données — article 430. (1.1);
– vol de service de télécommunication — article 326.

Le tableau 2 ne dégage de tendance uniforme de 1995 à 2001 pour aucune de ces cinq infractions. La troisième et la cinquième sont plus fréquentes que les autres crimes technologiques énumérés.

Tableau 2
Infractions relatives à la technologie[1], nombre d'accusations, Canada, 1995/1996 à 2000/01

Infraction au Code criminel	1995/1996	1996/1997	1997/1998	1998/1999	1999/2000	2000/01
Méfait contre des données	64	19	61	20	15	16
Vol de télécommunication	433	443	520	396	301	270
Possession d'un appareil permettant d'accéder à un service ou à des installations de télécommunication	357	220	262	238	599	133
Utilisation illicite d'un ordinateur	25	26	57	113	43	58

[1] *Aucune accusation n'a été signalée pour la possession d'un appareil permettant d'obtenir des services informatiques de 1995/96 à 2000/01.*

Note: *Les données de l'Enquête sur les tribunaux de juridiction criminelle pour adultes proviennent de sept provinces et d'un territoire, soit 80 % du nombre de causes des tribunaux pour adultes à l'échelle du pays.*

Source: *Enquête sur les tribunaux de juridiction criminelle pour adultes, Centre canadien de la statistique juridique, Statistique Canada.*

5. Programme de déclaration uniforme de la criminalité fondé sur l'affaire (DUC 2)

Il existe actuellement deux versions du Programme DUC 2. Il n'y a que la version la plus récente (DUC 2.1) qui comprenne un élément d'information « Type de fraude » permettant de déclarer toute fraude comportant l'utilisation d'un ordinateur sans autorisation ou à des fins illicites. En 2001, 32 corps policiers ont répondu à l'enquête DUC 2.1 qui rendait compte de 27 % des actes criminels qui se commettent au pays. Ils ont déclaré cette année-là 100 affaires de fraude informatique, et notamment de piratage et d'usage illicite de codes d'utilisateur ou de mots de passe.

Comme dans le NIBRS, les infractions au *Code criminel* pour fraude ou vol, par exemple, sont regroupées avec les crimes technologiques correspondants (voir ci-dessus la section sur l'Enquête sur les tribunaux de juridiction criminelle pour adultes). Le NIBRS peut servir de base à l'adoption d'une méthode semblable de collecte de données sur la cybercriminalité dans le cadre du Programme DUC 2 canadien.

6. Centre téléphonique national PhoneBusters

PhoneBusters a été établi en janvier 1993 par la direction des manœuvres frauduleuses de la Police provinciale de l'Ontario pour recevoir les plaintes sur le télémarketing frauduleux, pour partager les preuves avec d'autres organismes d'application de la loi et pour renseigner le public à propos de l'escroquerie par télémarketing. En juin 2001, PhoneBusters est devenu un organisme d'envergure nationale avec la participation de la Gendarmerie royale du Canada. Les efforts concertés de ces deux organismes favoriseront la collecte et l'analyse des données afin de déceler les tendances nationales et de fournir l'aide nécessaire aux enquêtes sur le télémarketing frauduleux aux échelons national et international (Gendarmerie royale du Canada, juin 2001).

7. Cyberaide.ca

En septembre 2002, le gouvernement du Canada a alloué des fonds à l'organisme Child Find Manitoba pour subventionner la ligne d'aide et le site Web Cyberaide.ca, qui vise à prévenir l'exploitation sexuelle en ligne des enfants. Au moyen d'un formulaire de rapport en ligne, le site Cyberaide.ca offre à la population un mécanisme pour signaler tout contenu illégal sur Internet, tel que la pornographie enfantine ou les tentatives d'entraîner un enfant vers des activités illicites. Le rapport est ensuite examiné et mis à la disposition des organismes d'application de la loi (Canada Newswire, 2002).

PARTIE V – RÉSULTATS DES CONSULTATIONS DE LA POLICE

Définitions, politiques et procédures policières en matière de cybercriminalité

Au Canada, il n'y a pas de mandat national par lequel les services de police sont tenus de dénombrer les infractions qui se commettent à l'aide d'Internet ou d'un ordinateur, mais il y a des corps policiers qui le font de leur propre chef. Pour pouvoir constater les besoins d'information et juger de la faisabilité d'une collecte de données de cybercriminalité auprès de la police, le CCSJ s'est mis en rapport avec 11 grands services policiers canadiens en 2002 :

Police de Halifax;
Service de police de la Communauté urbaine de Montréal (SPCUM);
Sûreté du Québec (SQ);
Service de police d'Ottawa;
Gendarmerie royale du Canada (GRC);
Police provinciale de l'Ontario (PPO);
Police de Toronto;
Police de Winnipeg;
Police d'Edmonton;
Police de Calgary;
Police de Vancouver.

Constatations générales

Dans la collecte de données policières sur la cybercriminalité, une difficulté à laquelle on se heurte est l'absence de définition uniforme de cette criminalité : cinq corps policiers appliquent une définition officielle, trois disposent d'une définition officieuse et trois n'ont aucune définition du tout.

L'absence de définition policière normalisée rend difficile toute collecte uniforme de données sur la cybercriminalité. Le problème fondamental est que, dans plusieurs services de police, on ne distingue pas les crimes par Internet des simples crimes par ordinateur.

Tableau3
Récapitulation des réponses des services de police

Corps policiers	Service spécialisé	Politique ou procédure	Définition	Données
Halifax	√	√ Officieuse	√ Officielle	√
MUC	√	√ Officieuse	√ Officieuse	√
SQ	√	√ Officielle	√ Officielle	√
Ottawa	√	√ Officieuse	√ Officieuse	√
GRC	√	√ Officielle	√ Officielle	√
PPO	√	√ Officieuse	√ Officieuse	√
Toronto	√	√ Officieuse	Non	Non
Winnipeg	Non	Non	Non	Non
Edmonton	Non	Non	Non	Non
Calgary	Non	Non	√ Officielle	Non
Vancouver	√	√ Officieuse	√ Officielle	Non

La plupart des services spécialisés dans les crimes technologiques enquêtent sur les crimes ayant l'ordinateur pour objet. Si l'ordinateur est l'instrument de perpétration, ce sont d'autres services qui interviennent. Ainsi, s'il se commet une fraude par Internet, le service des fraudes prendra l'affaire en charge. Dans ce cas, il incombera au service spécialisé dans les crimes technologiques de lui prêter main-forte le cas échéant.

Il y a des corps policiers qui se sont dotés de politiques et de procédures en matière de cybercriminalité, mais la plupart ne disposent que de procédures officieuses, c'est-à-dire n'ont pas de directives expresses. Des 11 services policiers interrogés, la GRC et la SQ étaient les seuls à appliquer des politiques et des procédures officielles.

Sur les huit corps ayant des services d'enquête sur la cybercriminalité, six recueillent, stockent et assemblent des données sur cette criminalité. L'information est versée sur support électronique dans des systèmes d'information directement conçus pour la collecte et l'analyse de renseignements criminels. La plupart des services policiers indiquent avoir ajouté à leur système de gestion de dossiers un élément d'information permettant de préciser si l'infraction était commise à l'aide de l'ordinateur ou d'Internet. Dans les corps policiers qui étaient en mesure de fournir les données recherchées, les infractions les plus fréquentes à l'aide d'un ordinateur étaient la fraude, la pornographie enfantine, les menaces et le harcèlement.

Un grand nombre de corps policiers qui n'étaient pas en mesure de communiquer ces renseignements ont dit qu'il serait faisable d'ajouter un élément d'information à leur système de gestion de dossiers et que cette mesure n'ajouterait pas grandement au fardeau de réponse. Il y aurait donc bel et bien une possibilité de collecte de telles données.

Indications des divers corps policiers

Nota : Les corps policiers d'Edmonton et de Winnipeg n'ont pas de service directement chargé de faire enquête sur les cybercrimes.

1. Police de Halifax

Le service de police de Halifax définit ainsi la cybercriminalité : « toute communication envoyée ou reçue par ordinateur par laquelle il y a tentative de perpétration d'un crime ».Ce corps policier fait enquête sur la cybercriminalité par son service des enquêtes générales sauf dans les affaires de pornographie enfantine. Dans ce service, il y a quatre personnes formées aux enquêtes sur les crimes par Internet. De plus, la sous-section scientifique des crimes informatiques de la section du soutien technique travaille à divers dossiers de piratage, de prostitution ou de pornographie par Internet, de fraude, de menaces, de pornographie enfantine, etc.

Sans disposer de politique officielle, la police de Halifax juge qu'une affaire relève de la criminalité informatique s'il y a eu des messages envoyés, acheminés ou reçus à l'aide d'un système informatique.

Il y a à Halifax un système en place de collecte de données sur la cybercriminalité. En 2001, 41 cybercrimes ont été signalés, souvent dans les domaines de la pornographie enfantine (8) et de la fraude (5). Le reste de ces 41 actes criminels consistaient en « autres » infractions au *Code criminel*.

2. Service de police de la Communauté urbaine de Montréal (SPCUM)

Au SPCUM, il n'y a pas de définition officielle de la cybercriminalité. La section dite du support tactique et spécialisé comprend un module des crimes technologiques qui fait enquête sur la cybercriminalité et qui est expressément chargé d'aider les autres services dans les affaires de crime informatique. Le nombre des affaires où ce module a apporté son aide a diminué de 23 % de 2000 à 2001, passant de 275 à 213.

Le Service de police de Montréal est en train d'élaborer des politiques et des procédures officielles concernant les enquêtes sur les crimes qui se commettent par ordinateur ou par Internet.

3. Sûreté du Québec (SQ)

La SQ définit la cybercriminalité comme « l'ensemble des crimes commis par Internet ». Le Module de la cybersurveillance et de la vigie, mis sur pied en décembre 2001, est le service spécialisé de ce corps policier qui fait enquête sur les crimes

cybernétiques et qui assure leur surveillance. Les membres de cette division analysent et évaluent chaque acte criminel afin de déterminer si le crime est lié à Internet. Ils effectuent aussi des vérifications préliminaires des banques de renseignements criminels, des activités du suspect sur Internet, des activités d'infiltration sur Internet, de la pornographie enfantine, etc. Les employés rédigent et exécutent les mandats, puis acheminent le dossier à l'unité appropriée au service de police concerné. En outre, le personnel expérimenté et hautement qualifié supporte et forme les membres de la SQ ainsi que des employés d'autres organismes collaborateurs. Entre janvier et septembre 2002, la Division a prêté main forte dans 309 affaires, dont 185 avaient trait à des crimes contre les bonnes mœurs, 99, des crimes économiques et 99, des crimes contre la personne.

4. Service de police d'Ottawa

Le Service de police d'Ottawa n'a pas de définition officielle de la cybercriminalité ou de politique officielle sur les enquêtes liées à la criminalité informatique. Il existe toutefois des politiques officielles pour certains types d'enquêtes qui sont liées à Internet, comme celles sur la pornographique enfantine et la fraude. En 1999, il a créé l'Escouade d'intervention contre la criminalité technologique (EICT) pour s'occuper de ces crimes.

Voici les responsabilités de l'EICT :

- Elle enquête sur les crimes ayant l'ordinateur pour objet (piratage informatique) par opposition aux crimes où l'ordinateur est l'instrument de perpétration (cas de fraude, de menaces ou de harcèlement) et dont s'occupent les services d'enquête compétents.
- Elle fait aussi enquête sur la pornographie enfantine dans Internet par opposition aux agressions sexuelles contre les enfants dont s'occupe la Section des agressions sexuelles et de la violence faite aux enfants (ASVE).
- Elle fait de l'analyse judiciaire de systèmes informatiques; la responsabilité des enquêtes est généralement confiée à la section concernée (voir plus haut) et l'EICT apporte une aide technique à leurs enquêteurs, qu'il s'agisse de biens volés récupérés ou d'enquêtes sur des décès, pour ne citer que ces exemples.
- Elle apporte enfin une aide technique aux autres services d'enquête pour ce qui est d'Internet, qu'il s'agisse d'enquêtes à la suite de plaintes pour conditions d'incitation à suicide dans Internet ou de détection de crimes de courrier électronique, pour ne citer que ces exemples.

Dans le système de gestion de dossiers d'Ottawa, on se sert de codes internes pour mettre en évidence les crimes commis à l'aide de l'ordinateur.

Statistiques du Service de police d'Ottawa sur la criminalité par Internet, 2000 et 2001

	2000	2001
Menaces	63	76
Menaces à un associé	1	2
Pornographie enfantine	31	26
Fraude de plus de 5 000 $	7	6
Fraude de 5 000 $ au plus	31	28
Méfaits concernant des données	10	17
TOTAL	**143**	**155**

Source: *Service de police d'Ottawa.*

5. Gendarmerie royale du Canada (GRC)

Le Programme de lutte contre les délits informatiques de la GRC définit la cybercriminalité par deux catégories générales, celles des crimes informatiques et des crimes facilités par ordinateur.

Le crime informatique est tout acte criminel ayant un ordinateur ou son contenu pour objet. Sont visées les infractions au *Code criminel* consistant en une « utilisation non autorisée d'ordinateur » ou en un « méfait concernant des données ». Il peut aussi s'agir des agissements des pirates informatiques, c'est-à-dire de ceux qui, par accès illicite à des systèmes informatiques, font un usage abusif des données qu'ils renferment.

Les crimes facilités par ordinateur comprennent des infractions au *Code criminel* avec usage d'ordinateur, qu'il s'agisse de trafic de drogue, de fraude ou de distribution de pornographie enfantine, pour ne citer que ces exemples. L'ordinateur est alors l'instrument qui vient faciliter la perpétration du crime.

Pour être le plus efficace possible, la GRC a réuni ses ressources de lutte contre la criminalité technologique sous la Direction de la criminalité technologique. Cette direction est chargée de la recherche et du développement, des politiques et des normes, et du soutien aux enquêtes dans le domaine de la criminalité technologique. Une des tâches spécialisées de cette direction est de faire enquête sur les actes criminels ayant des systèmes informatiques ou leur contenu pour objet. Cela inclut les enquêtes sur les cas d'usage abusif de systèmes de télécommunication, plus particulièrement dans un contexte interprovincial ou international. La Direction de la criminalité technologique a également pour tâche spécialisée de fournir un soutien informatique aux enquêtes, incluant la perquisition, la saisie et l'analyse des éléments de preuve électroniques à l'appui des enquêtes criminelles assistées par ordinateur, comme celles liées au crime organisé, à la sécurité nationale, aux produits de la criminalité et à la criminalité économique.

La GRC dispose, dans le cadre de son Système des rapports statistiques sur les opérations (système RSO), d'un système de collecte de données sur la cybercriminalité. En 1997, elle a mis en application un codage d'enquête permettant d'établir si Internet était intervenu en tout ou en partie dans la perpétration d'un crime. Le nombre de cybercrimes a monté de 1997 à 2001 de 54 à 768 affaires. En 2001, les cybercrimes le plus fréquemment déclarés était les méfaits concernant des données (376), les cas de pornographie enfantine (110) et les cas d'utilisation illicite d'un ordinateur (58).

6. Police provinciale de l'Ontario (PPO)

La PPO n'a pas de définition officielle de la cybercriminalité aux fins de la déclaration de données. Elle range un acte criminel dans la catégorie de la criminalité informatique s'il s'agit d'une infraction substantielle à l'article 342.1 « Utilisation non autorisée d'ordinateur » ou à l'article 430. (1.1) « Méfait concernant des données » du *Code criminel*.

La PPO fait enquête sur les cybercrimes et soutient les activités de fouille et de saisie électroniques de l'équipe d'enquête sur l'utilisation frauduleuse du système de santé de la Section de la lutte contre l'escroquerie du Bureau des enquêtes, et ce, par la Section de la répression de la criminalité informatique créée en 1999.

La PPO n'a pas de politique écrite sur la manière dont les enquêtes sur la cybercriminalité sont menées; toutefois, la PPO dispose de politiques et de procédures écrites concernant les activités de fouille et de saisie de preuves numériques. Une enquête sur un crime traditionnel ayant un élément informatique (Internet ou une preuve électronique) est menée de la même façon que tout autre acte criminel, c'est-à-dire que l'enquêteur principal pourrait venir de la région où le crime a été commis ou du bureau central; toutefois, il peut obtenir de l'aide facilement par l'intermédiaire de la Section de la répression de la criminalité informatique. La Section de la répression de la criminalité informatique offre, sur demande, de l'expertise aux détachements de la PPO, aux bureaux centraux de la PPO, aux organismes gouvernementaux et à d'autres organismes municipaux.

L'objectif de l'équipe de répression de la criminalité informatique est de fournir de l'expertise technologique dans le domaine des recherches judiciaires informatisées, d'offrir un soutien aux enquêtes sur les actes criminels traditionnels ayant un système informatique pour objet, de tenir des enquêtes liées à la criminalité informatique telle que définie par le *Code criminel* et de jouer le rôle d'experts-conseils dans les situations où l'on utilise la technologie pour faciliter des activités criminelles.

La Section de la répression de la criminalité informatique de la PPO dispose dans son système de gestion de dossiers d'un système de collecte de données sur la criminalité par Internet. En 2001, la Section a reçu au total 191 demandes de service, dont 70 % étaient liées à Internet. Les actes criminels le plus fréquemment déclarés en ce qui concerne Internet

sont les fraudes (19), les menaces (16), les méfaits concernant des données (10), la pornographie enfantine (9), les agressions sexuelles (9) et le harcèlement criminel (6).

La PPO a aussi une Section de la répression de la pornographie enfantine qui traite uniquement des enquêtes sur la pornographie enfantine commise à l'aide d'Internet et d'ordinateurs. La Section de la répression de la pornographie enfantine dispose dans son système de gestion de dossiers d'un sous-système de collecte de données d'enquêtes criminelles où Internet est en cause. En 2001, la Section a mené 410 enquêtes, a exécuté 91 mandats de perquisition et a porté 75 accusations contre 37 personnes.

7. Police de Toronto

Dans ce corps policier, il n'y a pas de définition fonctionnelle de la cybercriminalité, mais le service policier torontois enquête sur cette dernière par ses sections de l'exploitation sexuelle et du soutien technique.

La section de l'exploitation sexuelle, qui fait partie de l'escouade d'enquête sur les agressions sexuelles, a en partie pour mandat de faire enquête sur les cas d'exploitation sexuelle par Internet. À l'heure actuelle, ce service de police affecte six personnes aux enquêtes de pornographie enfantine par Internet. Il propose un projet sur deux ans qui répondra à la demande croissante d'enquêtes sur la pornographie enfantine, ce qui aurait pour effet de porter à 10 le nombre d'agents de la section de l'exploitation sexuelle.

Ajoutons que la section du soutien technique aide les autres services dans les affaires de crime à l'aide de l'ordinateur. Cette section compte actuellement deux agents d'enquête scientifique sur les ordinateurs et l'extraction de renseignements électroniques. À l'issue de ce projet de deux ans, six autres agents seraient spécialisés dans ce type d'enquête.

Jusqu'à présent, le service policier torontois ne dispose pas, dans le cadre de son système de gestion de dossiers, d'un mécanisme de collecte de données sur la cybercriminalité.

8. Police de Calgary

Le service de police de Calgary définit ainsi la criminalité technologique-informatique : « toute infraction à toute loi où un système informatique ou un autre dispositif technologique est en cause, que celui-ci soit l'objet du crime, un instrument de perpétration ou le lieu où sont stockées les données relatives à un acte criminel ».

Dans ce corps policier, le service d'enquête sur la criminalité technologique fait partie du service d'enquête sur les crimes commerciaux. Jusqu'à maintenant, on n'y applique pas de méthode officielle de repérage et de collecte de données statistiques sur la cybercriminalité. La sous-section de la criminalité technologique en est seulement aux premiers stades de l'édification d'une base d'information à la fois sur les crimes comportant l'utilisation d'ordinateurs et sur la cybercriminalité proprement dite.

9. Police de Vancouver

Le service de police de Vancouver emploie la définition de la cybercriminalité du Collège canadien de police. Il caractérise ces crimes par les deux articles du *Code criminel* qui traitent de l'utilisation criminelle d'ordinateurs et/ou des données qu'ils renferment. Il y a crime informatique lorsqu'un ordinateur sert à sa perpétration par importation, exportation, transfert ou stockage de données. La section des crimes financiers de ce corps policier est appelée à faire enquête sur toute infraction au *Code criminel* ayant trait à Internet.

Le service de police de Vancouver ne dispose pas encore d'un système de collecte de données statistiques sur la cybercriminalité, mais la constatation des crimes par Internet ou par ordinateur ne devrait poser aucun problème dans toute collecte future de données.

PARTIE VI – POSSIBILITÉS DE COLLECTE DE DONNÉES AUPRÈS DE LA POLICE

D'après les résultats des consultations menées par le Centre canadien de la statistique juridique auprès des services de police et l'examen des autres méthodes de collecte de données employées aux États-Unis et au Royaume-Uni, deux possibilités se dégagent pour ce qui est de la collecte future de données de cybercriminalité auprès des corps policiers : mener une étude spéciale et modifier le Programme de déclaration uniforme de la criminalité fondé sur l'affaire. Les exemples d'enquêtes-ménages cités à la partie IV illustrent les sources disponibles d'information complémentaire. Dans la présente question, il sera question des éléments d'information dans une collecte de données de déclaration policière de la cybercriminalité.

Possibilité 1 : Étude spéciale

Une possibilité serait de réaliser une étude spéciale où l'on recueillerait des renseignements détaillés auprès des services de police qui réunissent des données statistiques sur la cybercriminalité. À mesure que les services policiers spécialisés deviennent plus outillés pour faire enquête sur la cybercriminalité, les méthodes de collecte de données pourront s'améliorer dans les services de police canadiens. On compte actuellement au moins six de ces services qui font une telle collecte statistique. Jusqu'à ce que le Programme DUC 2 puisse être modifié, une étude spéciale permettrait à la police de communiquer les renseignements qu'elle recueille actuellement sur cette criminalité.

Avantages :

- Disponibilité des données — Une partie de l'information est disponible dès maintenant auprès des services de police.
- Progrès — Ce serait un pas en avant dans la définition du cadre d'élaboration d'un nouvel élément d'information pour le Programme DUC 2.
- On pourrait disposer de données avant même que le Programme DUC 2 ne soit révisé.

Inconvénients :

- Il n'y a actuellement aucune définition de la cybercriminalité qui soit officielle. Les données émanant des différents corps policiers pourraient ne pas mesurer le même concept.
- Il serait coûteux de mettre en place une enquête et un système de collecte et d'en analyser et diffuser les données.

Selon le nombre de services de police qui participeraient, le champ de l'étude, les questions posées, les coûts de système et les produits, une étude spéciale coûterait au moins 100 000 $ sur une période d'un à deux ans.

Possibilité 2 : Modification du Programme de déclaration uniforme de la criminalité fondé sur l'affaire (DUC 2)

On pourrait aussi ajouter un élément d'information au Programme DUC 2, comme on l'a fait dans le NIBRS américain afin d'établir si une infraction au *Code criminel* est liée à Internet ou aux ordinateurs. Ainsi, le préposé coderait l'infraction selon l'élément d'information qui existe actuellement pour les infractions au *Code criminel* (fraudes, par exemple) et se servirait du nouvel élément d'information pour indiquer si cet acte criminel est lié ou non à Internet ou aux ordinateurs. Voici un élément d'information possible pour le Programme DUC 2 :

ÉLÉMENT D'INFORMATION 1a.

Désignation : cybercriminalité
Enregistrement : niveau de l'affaire

Définition générale : *Infraction au* Code criminel *ayant un ordinateur pour objet, ou un ordinateur comme instrument de perpétration de la composante matérielle de l'infraction (Collège canadien de police).*

Éléments possibles de codage :

(i) Non, l'affaire n'est liée ni à Internet ni au matériel informatique
(ii) Oui, l'affaire est liée aux ordinateurs ou à Internet — si oui, passer à l'élément d'information 1b
(iii) Inconnu
(iv) Sans objet

ÉLÉMENT D'INFORMATION 1b.

Désignation : cybercriminalité
Enregistrement : niveau de l'affaire

Définition générale : *Cet élément d'information définit différents modes de perpétration d'un acte criminel à l'aide d'Internet ou de l'ordinateur. Dans ces méthodes criminelles, l'ordinateur est l'instrument de perpétration ou l'objet. La pornographie enfantine, le harcèlement criminel, la violation de la propriété intellectuelle et la vente de substances ou de marchandises illicites sont autant d'exemples d'actes criminels où l'ordinateur est l'instrument de perpétration. Par ailleurs, le piratage, la défiguration de sites Web et la création et la propagation malveillante de virus informatiques sont des exemples d'actes criminels ayant l'ordinateur pour objet.*

Éléments possibles de codage :

(i) Objet du crime (piratage)
(ii) Instrument de perpétration du crime (fraude ou pornographie enfantine)
(iii) Inconnu
(iv) Sans objet

Avantages :

- On pourrait recueillir des données détaillées non seulement sur les affaires, mais aussi sur les accusés et les victimes (pour les crimes contre la personne seulement).
- Le Programme DUC 2 existe déjà; une fois cet élément d'information ajouté, il n'y aura pas de grand surcroît de frais à prévoir.
- On pourrait produire des données annuelles sur la fréquence des cybercrimes.
- Il y a des services de police qui recueillent actuellement des données sur la cybercriminalité dans le cadre de leur système de gestion de dossiers.
- Un grand nombre de corps policiers qui ne réunissent pas pour l'instant de données sur la cybercriminalité ont dit que, en ajoutant un élément d'information à leur système de gestion de dossiers, ils ne se trouveraient pas à alourdir outre mesure le fardeau de réponse.

Inconvénients :

- Le temps nécessaire à la mise en œuvre — Il faudra attendre encore quelques années pour qu'une nouvelle version de l'enquête avec ces modifications et d'autres puissent être envisagée.
- Ce ne sont pas tous les services de police qui fournissent des données au Programme DUC 2; à l'heure actuelle, la couverture est de 60 % de la criminalité nationale.

Modifier le Programme DUC 2 est un exercise long et coûteux. Cependant, une fois les modifications mises en place, les coûts totaux seraient inferieurs à ceux d'études spéciales futures visant à saisir et analyser les données sur la cybercriminalité.

RECOMMANDATIONS

Nous recommandons d'exploiter les deux possibilités pour faciliter la collecte future de données statistiques sur la cybercriminalité. Idéalement, à court terme, l'étude spéciale (possibilité 1) pourrait servir à faire enquête auprès de tous les grands corps policiers canadiens afin d'examiner leurs méthodes actuelles de collecte de données. C'est ainsi qu'on pourrait étudier la qualité de l'information et fournir de l'aide pour établir conjointement des définitions, politiques, procédures et méthodes de collecte communes parmi les services de police. Les résultats obtenus au moyen de cette option pourraient alors servir à remanier le Programme DUC 2 (possibilité 2), ce qui constituerait un objectif à long terme.

PARTIE VII – CONCLUSION

L'attention récemment prêtée par les gouvernements fédéral, provinciaux et territoriaux et les milieux policiers à la cybercriminalité a amené le Centre canadien de la statistique juridique à s'attacher à la faisabilité d'une collecte de données de déclaration policière sur la criminalité dans Internet. Dans le présent rapport, nous jetons un premier regard sur les perspectives de collecte de telles données statistiques et énonçons des possibilités dans ce domaine.

La collecte de données sur l'activité criminelle sur Internet représente un grand défi, car les questions abondent en ce qui concerne la disponibilité et la fiabilité de l'information en question. L'absence d'une seule définition pour tous les services de police, l'absence de politiques et de procédures officielles dans les unités spécialisées et le manque de ressources des services d'enquêtes spéciaux sur les crimes commis à l'aide d'Internet ou d'ordinateurs sont autant d'obstacles à la collecte de statistiques exactes sur la cybercriminalité.

Les nouveaux défis qui sont particuliers à la cybercriminalité contribuent au nombre de crimes cybernétiques qui ne sont ni signalés à la police ni mis sous enquête par elle. En effet, la cybercriminalité pourrait constituer la forme de comportement criminel la moins déclarée puisque la victime ignore souvent qu'une infraction a même eu lieu. De plus, dans le cas d'entreprises, les victimes hésitent à signaler de telles infractions de peur de perdre la confiance des consommateurs. Le perfectionnement des techniques, les capacités de stockage des réseaux informatiques et la diffusion mondiale de l'information ajoutent à la difficulté de déceler les crimes cybernétiques. La documentation à ce sujet laisse entendre que la majorité des affaires de cybercriminalité pourraient ne pas être signalées à la police.

Ces défis comprennent les suivants :

1. Il existe des difficultés d'ordre technique qui nuisent à la capacité des responsables de l'application de la loi de découvrir et de poursuivre les criminels qui exercent leur activité en ligne.
2. Il existe des difficultés d'ordre juridique qui tiennent à la désuétude de certaines lois. De plus, les instruments juridiques nécessaires aux enquêtes sur la cybercriminalité accusent un retard sur l'évolution des technologies, des structures et de la société.
3. Il y a des difficultés d'ordre opérationnel à aplanir si on entend s'assurer que les agents des organismes d'application de la loi seront bien formés et bien outillés pour collaborer, même au-delà les frontières nationales.
4. Les auteurs des actes criminels visés sont très difficiles à identifier, car souvent ils se servent de fausses identités en ligne et font usage de services de retour anonymes.
5. Il est difficile de déterminer le lieu précis du crime. Il s'agit de crimes qui peuvent se commettre à partir de tout lieu où il y a le téléphone, qu'il s'agisse de postes publics Internet dans les aérodromes, les gares routières, les bibliothèques, les cybercafés ou les dépanneurs, pour ne citer que quelques exemples.

Il importe toutefois de recueillir des données statistiques sur la cybercriminalité à l'échelle nationale pour pouvoir en évaluer l'incidence sur la société. Les gouvernements et les services de police s'appuient sur cette information pour mieux appliquer leurs politiques et leurs procédures, ainsi que pour affecter des ressources aux activités d'enquête et de prévention qui pourront rendre les cybercrimes moins fréquents au pays.

Ce rapport présente deux possibilités de collecte de données sur la cybercriminalité au Canada. L'option à court terme consisterait en une étude spéciale visant à recueillir de l'information détaillée auprès des services de police qui réunissent ce genre de données. Dans l'option à long terme, il faudrait ajouter un élément d'information au Programme DUC 2 afin de repérer les infractions au *Code criminel* pour lesquelles Internet ou un ordinateur est l'objet du crime ou l'instrument utilisé pour le commettre.

BIBLIOGRAPHIE

Bureau of Justice Statistics. *Office of Justice Prosecutions,* département de la Justice des États-Unis, 2002. Adresse Internet : www.ojp.usdoj.gov/ (consulté le 4 novembre 2002).

Canada Newswire. *Child Online Safety Gets a Boost with Launch of Cybertip.ca,* 2002.
Adresse Internet : www.newswire.ca/releases/September2002/26/c5173.html (consulté le 4 novembre 2002).

Carter, D. « Computer crime categories: How techno-criminals operate », *FBI Law Enforcement Bulletin,* vol. 64, nº 7, 1995, p. 21.

Chu, S. *Canada lags in cyber-crime laws,* le 14 décembre 2000. Adresse Internet : globetechnology.com/servlet/GAMArticleHTML (consulté le 4 novembre 2002).

Convention on Cyber-Crime. *The Convention on Cyber-Crime, a unique instrument for international co-operation,* Budapest, Conseil de l'Europe, 2001. Adresse Internet : conventions.coe.int/treaty/EN/projets/projets.htm:2001 (consulté le 4 novembre 2002).

Davis, R, et S. Hutchison. *Computer Crime in Canada,* Toronto, Thomson Canada Limited, 1997.

Enquête sociale générale, cycle 14. *Accès et utilisation des technologies de l'information et des communications*, Ottawa, Statistique Canada, 2000.

Federal Bureau of Investigation. *National Incident-Based Reporting System, Volume 1: Data Collection Guidelines,* Virginie occidentale, département de la Justice des États-Unis, FBI, 2000.

Finkelhor, D., K.J. Mitchell et J. Wolak. *Online Victimization: A Report of the Nations's Youth,* Washington, D.C., National Center for Missing and Exploited Children, 2000.

Gendarmerie royale du Canada. *Le lancement du nouveau Centre national d'appels PhoneBusters,* juin 2001. Adresse Internet : www.rcmp-grc.gc.ca/news/cm-01-09.htm (consulté le 4 novembre 2002).

Groupe de travail fédéral-provincial-territorial sur le contenu illégal et offensant dans Internet. *Rapport au Comité de coordination des hauts fonctionnaires*. Ottawa, ministère de la Justice Canada, juin 2002.

Internet Crime Forum. *Internet Crime Forum,* mars 2001. Adresse Internet : www.internetcrimeforum.org.uk (consulté le 4 novembre 2002).

Internet Fraud Complaint Center. *IFCC 2001 Internet fraud report,* 2001. Adresse Internet : www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf (consulté le 4 novembre 2002).

Kubic, T. *The FBI's Perspective on the Cyber Crime Problem,* juin 2001. Adresse Internet : www.FBI.GOV//CONGRESS/Congress01/kubic06/201.htm (consulté le 4 novembre 2002).

Ministère de la Justice Canada. *Des mesures en vue de mieux protéger les Canadiens et les enfants des cybercriminels,* Ottawa, ministère de la Justice Canada, juin 2002. Adresse Internet : canada.justice.gc.ca/http://strategis.ic.gc.ca/pics/sff/finalreportfr.pdf (consulté le 4 novembre 2002).

Power, R. « 2001 CSI/FBI computer crime and security survey », *Computer Security Issues & Trends,* San Francisco, Computer Security Institute, vol. 7, nº 1, 2001.

PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET. *The electronic frontier: The challenge of unlawful conduct involving the use of the Internet,* Washington, D.C., département de la Justice des États-Unis, mars 2000. Adresse Internet : www.usdoj.gov/criminal/cybercrime/unlawful.htm (consulté le 4 novembre 2002).

RÉSEAU ÉDUCATION-MÉDIAS et ENVIRONICS RESEARCH GROUP. *Les enfants du Canada dans un monde branché — le point de vue des parents,* Ottawa, Gouvernement du Canada, mars 2000. Adresse Internet : strategis.ic.gc.ca/pics/sff/finalreportfr.pdf (consulté le 4 novembre 2002).

RÉSEAU ÉDUCATION-MÉDIAS et ENVIRONICS RESEARCH GROUP. *Jeunes canadiens dans un monde branché — la perspective des élèves,* Ottawa, Gouvernement du Canada, octobre 2000. Adresse Internet : www.connect.gc.ca/cyberaverti/pdf/wired_f.pdf (consulté le 4 novembre 2002).

STATISTIQUE CANADA. *Aperçu : accès et utilisation des technologies de l'information et des communications,* Division des statistiques sociales, du logement et des familles, mars 2001. Adresse Internet : www.statcan.ca/français/IPS/Data/56-505-XIF/free_f.htm (consulté le 4 novembre 2002).

STATISTIQUE CANADA. « Enquête sur l'utilisation d'Internet par les ménages », *Le Quotidien,* juillet 2002. Adresse Internet : www.statcan.ca/Daily/Français/020725/ d020725a.htm (consulté le 4 novembre 2002).

US CENSUS BUREAU. *Computer Security Survey,* 2002, Adresse Internet : www.census.gov/eos/www/css/css.html (consulté le 4 novembre 2002).

ANNEXE A: Incident Report : enquête NIBRS (États-Unis)[1]

ORI #:

INCIDENT #:

REPORT TYPE: ❑ INITIAL REPORT ❑ SUPPLEMENT

INCIDENT REPORT
(EXAMPLE)

INCIDENT STATUS: ❑ UNFOUNDED ❑ CLEARED BY ARREST ❑ CLEARED EXCEPTIONALLY
A ❑ DEATH OF OFFENDER
B ❑ PROSECUTION DECLINED
C ❑ EXTRADITION DECLINED
D ❑ REFUSED TO COOPERATE
E ❑ JUVENILE, NO CUSTODY
N ❑ NOT APPLICABLE

EXCEPTIONAL CLEARANCE DATE:

COMPLAINANT : (Last, First, Middle)

PHONE: (Home) ( ) (Business) ( )

ADDRESS: (Street, City, State, Zip)

LOCATION OF INCIDENT : (Address Or Block No.)

OFFENSE:	(Check If Bias Motivated)	OFFENDER:
1.	1. ❑	1.
2.	2. ❑	2.
3.	3. ❑	3.

UCR OFFENSE CODE: 1. 2. 3.

DATE(S) OF INCIDENT :

TIME(S) OF INCIDENT :

BIAS MOTIVATION : (Check one for Offense #1)

RACIAL
11 ❑ ANTI - WHITE
12 ❑ ANTI - BLACK
13 ❑ ANTI - AMERICAN INDIAN / ALASKAN NATIVE
14 ❑ ANTI - ASIAN / PACIFIC ISLANDER
15 ❑ ANTI - MULTI - RACIAL GROUP

ETHNICITY / NATIONAL ORIGIN
31 ❑ ANTI - ARAB
32 ❑ ANTI - HISPANIC
33 ❑ ANTI - OTHER ETHNICITY / NATIONAL ORIGIN

RELIGIOUS
21 ❑ ANTI - JEWISH
22 ❑ ANTI - CATHOLIC
23 ❑ ANTI - PROTESTANT
24 ❑ ANTI - ISLAMIC (MOSLEM)
25 ❑ ANTI - OTHER RELIGION
26 ❑ ANTI - MULTI - RELIGIOUS GROUP
27 ❑ ANTI - ATHEISM / AGNOSTICISM

SEXUAL
41 ❑ ANTI - MALE HOMOSEXUAL (GAY)
42 ❑ ANTI - FEMALE HOMOSEXUAL (LESBIAN)
43 ❑ ANTI - HOMOSEXUAL (GAYS AND LESBIANS)
44 ❑ ANTI - HETEROSEXUAL
45 ❑ ANTI - BISEXUAL

ENTER BIAS MOTIVATION **CODE** IF DIFFERENT FROM OFFENSE #1
#2 ❑❑
#3 ❑❑

OFFENSE STATUS: (Check Only One Per Offense)
1. A ❑ ATTEMPTED C ❑ COMPLETED
2. A ❑ ATTEMPTED C ❑ COMPLETED
3. A ❑ ATTEMPTED C ❑ COMPLETED

OFFENDER(S) USED: (Check As Many As Apply) A ❑ ALCOHOL C ❑ COMPUTER EQUIP D ❑ DRUGS N ❑ NOT APPLICABLE

(For Burglary Only)
NUMBER OF PREMISES ENTERED: _____
METHOD OF ENTRY : F ❑ FORCIBLE N ❑ NO FORCE

LOCATION OF OFFENSE: (Check Only One) (Enter Code Number for Offense #2_____#3 _____)
01 ❑ AIR / BUS / TRAIN TERMINAL
02 ❑ BANK / SAVINGS & LOAN
03 ❑ BAR / NIGHT CLUB
04 ❑ CHURCH / SYNAGOGUE / TEMPLE
05 ❑ COMMERCIAL / OFFICE BUILDING
06 ❑ CONSTRUCTION SITE
07 ❑ CONVENIENCE STORE
08 ❑ DEPARTMENT / DISCOUNT STORE
09 ❑ DRUG STORE / DR'S OFFICE / HOSPITAL
10 ❑ FIELD / WOODS
11 ❑ GOVERNMENT / PUBLIC BUILDINGS
12 ❑ GROCERY / SUPERMARKET
13 ❑ HIGHWAY / ROAD / ALLEY
14 ❑ HOTEL / MOTEL / ETC.
15 ❑ JAIL / PRISON
16 ❑ LAKE / WATERWAY
17 ❑ LIQUOR STORE
18 ❑ PARKING LOT / GARAGE
19 ❑ RENTAL / STORAGE FACILITY
20 ❑ RESIDENCE / HOME
21 ❑ RESTAURANT
22 ❑ SCHOOL / COLLEGE
23 ❑ SERVICE / GAS STATION
24 ❑ SPECIALTY STORE (TV, FUR, ETC.)
25 ❑ OTHER / UNKNOWN

TYPE CRIMINAL ACTIVITY : (Check Up To Three)
B ❑ BUYING / RECEIVING
C ❑ CULTIVATING / MANUFACTURING / PUBLISHING
D ❑ DISTRIBUTING / SELLING
E ❑ EXPLOITING CHILDREN
O ❑ OPERATING / PROMOTING / ASSISTING
P ❑ POSSESSING / CONCEALING
T ❑ TRANSPORTING / TRANSMITTING / IMPORTING
U ❑ USING / CONSUMING

TYPE WEAPON / FORCE INVOLVED: (Check Up To Three) (Enter A In Box If Automatic)
11 ❑ FIREARM (type not stated)
12 ❑ HANDGUN
13 ❑ RIFLE
14 ❑ SHOTGUN
15 ❑ OTHER FIREARM
20 ❑ KNIFE / CUTTING INSTRUMENT
30 ❑ BLUNT OBJECT
35 ❑ MOTOR VEHICLE
40 ❑ PERSONAL WEAPONS
50 ❑ POISON
60 ❑ EXPLOSIVES
65 ❑ FIRE / INCENDIARY
70 ❑ NARCOTICS / DRUGS
85 ❑ ASPHYXIATION
90 ❑ OTHER
95 ❑ UNKNOWN
99 ❑ NONE

VICTIM # 1: (Last, First, Middle)

PHONE: (Home)

ADDRESS: (Street, City, State, Zip)

TYPE OF VICTIM: (Check Only One)
I ❑ INDIVIDUAL
B ❑ BUSINESS
F ❑ FINANCIAL
G ❑ GOVERNMENT
R ❑ RELIGIOUS
S ❑ SOCIETY / PUBLIC
O ❑ OTHER
U ❑ UNKNOWN

RACE:
W ❑ WHITE
B ❑ BLACK
I ❑ INDIAN
A ❑ ASIAN
U ❑ UNKNOWN

SEX:
M ❑ MALE
F ❑ FEMALE
U ❑ UNKNOWN

AGE:

DOB:

NO. OF VICTIMS:

RESIDENT STATUS:
R ❑ RESIDENT
N ❑ NONRESIDENT
U ❑ UNKNOWN

ETHNICITY :
H ❑ HISPANIC
N ❑ NON - HISPANIC
U ❑ UNKNOWN

AGGRAVATED ASSAULT / HOMICIDE CIRCUMSTANCES: (Check Up to Two)
01 ❑ ARGUMENT
02 ❑ ASSAULT ON LAW OFFICER
03 ❑ DRUG DEALING
04 ❑ GANGLAND
05 ❑ JUVENILE GANG
06 ❑ LOVERS' QUARREL
07 ❑ MERCY KILLING
08 ❑ OTHER FELONY INVOLVED
09 ❑ OTHER CIRCUMSTANCES
10 ❑ UNKNOWN CIRCUMSTANCES

INJURY TYPE: (Check Up to Five)
N ❑ NONE
B ❑ BROKEN BONES
I ❑ POSS. INT. INJURIES
L ❑ SEVERE LACERATION
M ❑ MINOR INJURY
O ❑ MAJOR INJURY
T ❑ LOSS OF TEETH
U ❑ UNCONSCIOUSNESS

VICTIM CONNECTED TO OFFENSE NUMBER ABOVE:
1. ❑
2. ❑
3. ❑

RELATIONSHIP OF VICTIM TO OFFENDER: (For multiple offender relationships enter offender number[s] in space)
SE ____ SPOUSE
CS ____ COMMON - LAW SPOUSE
PA ____ PARENT
SB ____ SIBLING
CH ____ CHILD
GP ____ GRANDPARENT
GC ____ GRANDCHILD
IL ____ IN-LAW
SP ____ STEPPARENT
SC ____ STEPCHILD
SS ____ STEPSIBLING
OF ____ OTHER FAMILY
AQ ____ ACQUAINTANCE
FR ____ FRIEND
NE ____ NEIGHBOR
BE ____ BABYSITTEE (baby)
BG ____ BOY / GIRL FRIEND
CF ____ CHILD OF "BG" ABOVE
HH ____ HOMOSEXUAL REL.
XS ____ EX-SPOUSE
EE ____ EMPLOYEE
ER ____ EMPLOYER
OK ____ OTHERWISE KNOWN
ST ____ STRANGER
VO ____ VICTIM WAS OFFENDER
RU ____ RELATIONSHIP UNKNOWN

Page _____ of _____

PROPERTY

TYPE PROPERTY LOSS / ETC.	CODE	QUANTITY	PROPERTY DESCRIPTION INCLUDE MAKE, MODEL, SIZE, TYPE, SERIAL #, COLOR, ETC.	VALUE	DATE RECOVERED Month / Day / Year
1 ❑ NONE					
2 ❑ BURNED					
3 ❑ COUNTERFEITED / FORGED					
4 ❑ DAMAGED / DESTROYED					
5 ❑ RECOVERED					
6 ❑ SEIZED					
7 ❑ STOLEN					
8 ❑ UNKNOWN					

PROPERTY DESCRIPTION CODE TABLE:
(Enter Number In Code Column Above)

01 AIRCRAFT
02 ALCOHOL
03 AUTOMOBILES
04 BICYCLES
05 BUSES
06 CLOTHES / FURS
07 COMPUTER HARDWARE / SOFTWARE
08 CONSUMABLE GOODS
09 CREDIT / DEBIT CARDS
10 DRUGS / NARCOTICS
11 DRUG / NARCOTIC EQUIPMENT
12 FARM EQUIPMENT
13 FIREARMS
14 GAMBLING EQUIPMENT
15 HEAVY CONSTRUCTION / INDUSTRIAL EQUIPMENT
16 HOUSEHOLD GOODS
17 JEWELRY / PRECIOUS METALS
18 LIVESTOCK
19 MERCHANDISE
20 MONEY
21 NEGOTIABLE INSTRUMENTS
22 NONNEGOTIABLE INSTRUMENTS
23 OFFICE-TYPE EQUIPMENT
24 OTHER MOTOR VEHICLES
25 PURSES / HANDBAGS / WALLETS
26 RADIOS / TVs / VCRs
27 RECORDINGS - AUDIO / VISUAL
28 RECREATIONAL VEHICLES
29 STRUCTURES - SINGLE OCCUPANCY DWELLINGS
30 STRUCTURES - OTHER DWELLINGS
31 STRUCTURES - OTHER COMMERCIAL / BUSINESS
32 STRUCTURES - INDUSTRIAL / MANUFACTURING
33 STRUCTURES - PUBLIC / COMMUNITY
34 STRUCTURES - STORAGE
35 STRUCTURES - OTHER
36 TOOLS - POWER / HAND
37 TRUCKS
38 VEHICLE PARTS / ACCESSORIES
39 WATERCRAFT
77 OTHER
88 PENDING INVENTORY
99 (_____)

OFFENDER

NUMBER OF OFFENDERS: _____

1.
ADDRESS: (Street, City, State, Zip)

AGE:	SEX: M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN	RACE: W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN	HEIGHT: ____ feet ____ inches	WEIGHT:	EYES:	HAIR:	CLOTHING:

2.
ADDRESS:

AGE:	SEX: M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN	RACE: W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN	HEIGHT: ____ feet ____ inches	WEIGHT:	EYES:	HAIR:	CLOTHING:

3.
ADDRESS:

AGE:	SEX: M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN	RACE: W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN	HEIGHT: ____ feet ____ inches	WEIGHT:	EYES:	HAIR:	CLOTHING:

ARRESTEE

NUMBER OF ARRESTEES: _____ **MULTIPLE CLEARANCE INDICATOR:** M ❑ MULTIPLE C ❑ COUNT ARRESTEE N ❑ NOT APPLICABLE

ARRESTEE #1:(Last, First, Middle) **ADDRESS:** (Street, City, State, Zip)

AGE:	SEX: M ❑ MALE F ❑ FEMALE	RACE: W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN	DOB:	ARRESTEE ETHNICITY: H ❑ HISPANIC N ❑ NON-HISPANIC U ❑ UNKNOWN	RESIDENT STATUS: R ❑ RESIDENT N ❑ NONRESIDENT U ❑ UNKNOWN

ARRESTEE WAS ARMED WITH: (Check Up To Two) (Enter A In Box If Automatic)
01 ❑ UNARMED
11 ❑ FIREARM (type not stated)
12 ❑ HANDGUN
13 ❑ RIFLE
14 ❑ SHOTGUN
15 ❑ OTHER FIREARM
16 ❑ LETHAL CUTTING INSTRUMENT (e.g. Switchblade Knife, etc.)
17 ❑ CLUB / BLACKJACK / BRASS KNUCKLES

TYPE OF ARREST:
O ❑ ON-VIEW
S ❑ SUMMONED / CITED
T ❑ TAKEN INTO CUSTODY

DISPOSITION OF ARRESTEE UNDER 18:
H ❑ HANDLED WITHIN DEPARTMENT
R ❑ REFERRED TO OTHER AUTHORITY

HEIGHT: ____ feet ____ inches	WEIGHT:	EYES:	HAIR:	ARREST NUMBER:	ARREST DATE:	UCR ARREST OFFENSE CODE:

WITNESS

NAME: (Last, First, Middle)	ADDRESS: (Street, City, State, Zip)	RESIDENTIAL PHONE:	BUSINESS PHONE:
#1			
#2			

NARRATIVE

❑ continued on supplement

[1] *Indisponible en français*

ANNEXE B : National Victimization Survey (États-Unis)[1]

FORM **NCVS-1**
(5-10-2001)

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

ACTING AS COLLECTING AGENT FOR THE
BUREAU OF JUSTICE STATISTICS
U.S. DEPARTMENT OF JUSTICE

NATIONAL CRIME VICTIMIZATION SURVEY

NCVS-1 BASIC SCREEN QUESTIONNAIRE

HOUSEHOLD RESPONDENT'S COMPUTER CRIME SCREEN QUESTIONS

FIELD REPRESENTATIVE – *Read introduction.*

INTRO: **The next series of questions are about YOUR use of a computer. Please include ALL computers, laptops, or access to WebTV used at home, work, or school for PERSONAL USE *or* for operating a home business.**

45c. **During the last 6 months, have YOU used a computer, laptop, or WebTV for the following purposes** *(Read answer categories 1–4) –*

Mark (X) all that apply.

100 *
1 ☐ **For personal use at home?**
2 ☐ **For personal use at work?**
3 ☐ **For personal use at school, libraries, etc.?**
4 ☐ **To operate a home business?**
5 ☐ None of the above – ***SKIP*** *to Check Item D*

45d. **How many computers do you have access to for personal use or for operating a home business?**

101
0 ☐ None
1 ☐ 1
2 ☐ 2
3 ☐ 3
4 ☐ 4 or more

45e. **Do YOU use the Internet for personal use or for operating a home business?**

102
1 ☐ Personal use
2 ☐ Operating a home business
3 ☐ Both
4 ☐ None of the above

45f. **Have you experienced any of the following COMPUTER-RELATED incidents in the last 6 months** *(Read answer categories 1–6) –*

Mark (X) all that apply.

103 *
1 ☐ **Fraud in purchasing something over the Internet?**
2 ☐ **Computer virus attack?**
3 ☐ **Threats of harm or physical attack made while online or through E-mail?**
4 ☐ **Unrequested lewd or obscene messages, communications, or images while online or through E-mail?**
5 ☐ *(Only ask if box 4 is marked in Item 45c)* **Software copyright violation in connection with a home business?**
6 ☐ **Something else that you consider a computer-related crime?–***Specify* ✍
_____
_____
7 ☐ No computer-related incidents –***SKIP*** *to Check Item D*

45g. **Did you suffer any monetary loss as a result of the incident(s) you just mentioned?**

104
1 ☐ Yes
2 ☐ No – ***SKIP*** *to 45i*

45h. **How much money did you lose as a result of the incident(s)?**

105 $_____ .00 Amount of loss
x ☐ Don't know

45i. **Did you report the incident(s) you just mentioned to** *(Read answer categories 1 –5) –*

Mark (X) all that apply.

106 *
1 ☐ **A law enforcement agency?**
2 ☐ **An Internet Service provider?**
3 ☐ **A Website administrator?**
4 ☐ **A Systems Administrator?**
5 ☐ **Someone else? –** *Specify* ✍
_____
_____
6 ☐ None of the above

[1] *Indisponible en français*

ANNEXE C : Mesure de la cybercriminalité par l'ESG

L'ESG 2000 (cycle 14) est le premier cycle où l'on recueille des données détaillées sur l'accès et l'usage de la technologie au Canada (l'ESG 1994 a livré des renseignements restreints à ce sujet). Voici les questions ayant servi à l'évaluation de l'activité criminelle dans Internet :

1. Au meilleur de votre connaissance, en naviguant sur Internet, vos enfants ont-ils trouvé de la matière favorisant la haine ou la violence contre un groupe particulier?

2. Avez-vous déjà reçu du courrier électronique qui vous a semblé menaçant ou harcelant?

3. En naviguant sur Internet, avez-vous trouvé de la matière favorisant la haine ou la violence contre un groupe particulier?

4. En naviguant sur Internet, avez-vous trouvé des sites Web comportant de la pornographie?
   Est-ce que vous cherchiez cette matière ou y êtes-vous arrivé de façon inattendue?
   Est-ce que vous avez trouvé cette matière offensante?

5. Avez-vous eu des difficultés liées à la sécurité sur Internet?

Veuillez préciser le (ou les) problème(s) lié(s) à la sécurité sur Internet :

1) Virus
2) Messages menaçants par courrier électronique
3) Personnes s'infiltrant dans les comptes de courrier électronique ou les fichiers informatiques
4) Renseignements personnels rendus publics
5) Autres

Source : *Enquête sociale générale, cycle 14, 2000.*