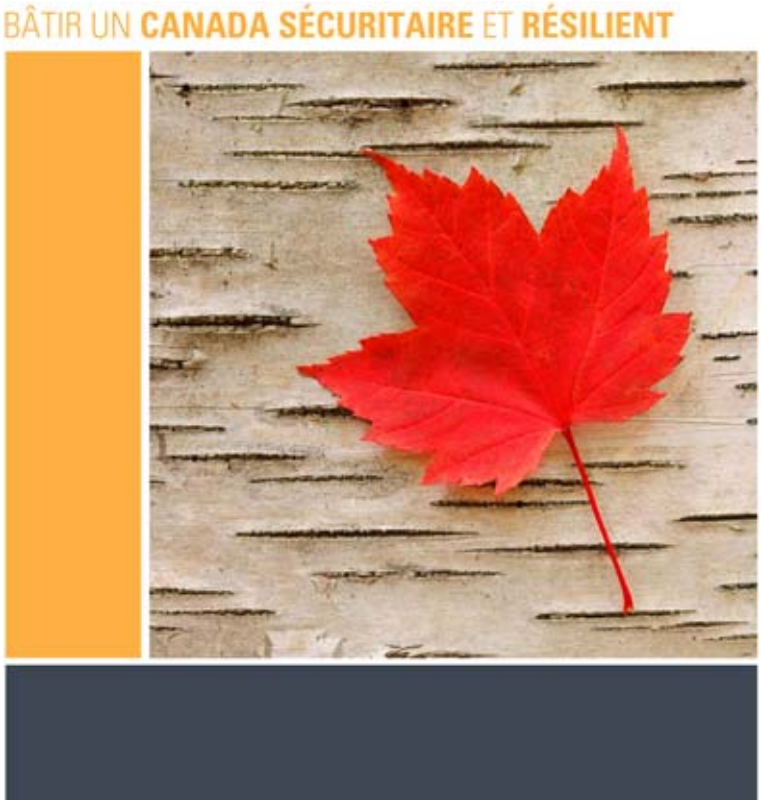
Sécurité publique Canada | Public Safety Canada



Sécurité publique Canada
Évaluation de l'ampleur de la cyberfraude
Document de travail sur les méthodes potentielles et les sources de données

AOUT 2011
SGDDI #465993

Canada

Évaluation de l'ampleur de la cyberfraude: Document de travail sur les méthodes potentielles et les sources de données

Par

Sara M. Smyth
Université Simon Fraser

et

Rebecca Carleton

préparée pour la

Division de la recherche et de la coordination nationale sur le crime organisé
Secteur de la police et de l'application de la loi
Sécurité publique Canada

Les opinions exprimées n'engagent que les auteurs et ne sont pas nécessairement celles du ministère de la Sécurité publique.

Rapport nº 020, 2011

Cat. No.: #PS14-4/2011F-PDF
ISBN No.: #978-1-100-97864-2

Table des matières

Sommaire

Si l'on souhaite suivre et accélérer les progrès dans les stratégies visant à lutter contre la cybercriminalité, il est fondamental que l'on dispose d'informations fiables sur l'ampleur de cette criminalité, le nombre d'incidents et de délinquants, le nombre d'outils du cyberespace employés pour commettre de tels crimes ainsi que le nombre de victimes. Le présent document de travail vise à examiner la possibilité de recourir à des méthodes novatrices pour évaluer l'ampleur de la cyberfraude, à repérer les sources de données existantes et les lacunes et, enfin, à suggérer de nouvelles sources de données susceptibles de fournir un portrait plus juste de l'ampleur de la cyberfraude au Canada. De plus, il explore des moyens éventuels de déterminer la proportion de cyberfraudes attribuables à des réseaux criminels plutôt qu'à des individus. Dans cette recherche, on a consulté de la documentation et effectué des entrevues avec du personnel chargé de l'application de la loi et de la technologie de l'information (TI).

D'après la documentation et les entrevues, le plus grand obstacle à une bonne gestion du problème de la cyberfraude est le manque de données fiables. Dans ce domaine, le gouvernement du Canada s'appuie principalement sur des données fournies par la police. Pourtant, nombre de raisons font que certains cas de fraude ne sont pas signalés à la police. Ainsi, certaines sociétés peuvent préférer traiter ces cas à l'interne; des gens peuvent signaler ces cas à leur seule institution financière.

D'après la recherche, les informations actuelles sur la cyberfraude sont communiquées à une diversité d'organisations, à savoir banques, organismes de réglementation ou corps de police, ou alors elles ne sont tout simplement pas consignées. Visiblement, les données sont insuffisantes pour évaluer l'ampleur et le coût de la cyberfraude au Canada, et l'information disponible est incomplète ou fragmentée. Le défaut pour des victimes de signaler des cyberfraudes, qu'il s'agisse d'individus, de sociétés ou de gouvernements, fait en sorte que nombre de cas ne sont pas consignés ou comptabilisés dans les statistiques officielles de la criminalité. Le résultat de cette recherche illustre clairement la nécessité de créer un centre national qui consignerait et évaluerait les données sur la cyberfraude dans tout le Canada. Une banque de données centrale et nationale sur les auteurs et les cas connus de cyberfraude faciliterait l'identification et le dépistage de suspects de cyberfraude et permettrait de mieux faire comprendre à l'échelle du pays une telle fraude commise par un individu ou un groupe. Ultimement, une banque sur de tels incidents pourrait aider les responsables de l'application de la loi à comprendre les types de cyberfraudes commis dans notre pays.

Par ailleurs, la complexité des technologies et la distribution mondiale des réseaux informatiques rendent plus difficiles la détection et la lutte contre la cyberfraude, tout comme le dépistage et la poursuite en justice des criminels dont les opérations s'effectuent en ligne. De plus, des défis opérationnels se posent pour ce qui est de s'assurer que les responsables de l'application de la loi possèdent la formation et les ressources nécessaires pour traiter adéquatement le problème et pour identifier l'auteur d'une cyberfraude. Dans beaucoup de cas, chercher à repérer l'auteur pose un problème, car le cyberattaquant habile brouille sa piste grâce à des serveurs mandataires et à d'autres techniques d'obscurcissement.

D’après la présente recherche, la meilleure source d’informations supplémentaires sur la cyberfraude est la communauté des fraudeurs. Les entrevues avec ces derniers peuvent aider à découvrir la structure d’un réseau caché et amener les responsables de l’application de la loi à identifier les intervenants clés au sein d’un groupe. Parmi les options disponibles pour mettre au jour cette communauté clandestine, un modèle tronqué de Poisson semble le plus efficace. Idéalement, la présente recherche pourrait ouvrir la voie à une collecte et à une analyse de données qui éclaireraient les responsables de l’application de la loi ou de l’élaboration des politiques ainsi que les enquêteurs sur l’ampleur de la cyberfraude et de la communauté des cybercriminels au Canada. Cette recherche peut faire progresser les stratégies de prévention et de suppression de la cyberfraude, mais aussi le développement de moyens empiriques pour évaluer l’efficacité de certaines initiatives, notamment d’éléments de la Stratégie de cybersécurité du Canada.

1.0 Introduction

Comment recueillir, évaluer et communiquer plus efficacement des renseignements sur des cyberfraudes? À l'évidence, la première étape consiste à identifier et à définir plus exactement l'objet de l'évaluation. Normalement, la loi conserve une neutralité « technique » à l'égard des infractions (autrement dit, une fraude demeure une fraude, quelle qu'en soit la méthode). Il importe de définir les phénomènes de criminalité, parce que cela permet à tous les intervenants, y compris la police, les procureurs et les juges, d'en avoir la même compréhension. De plus, une définition universelle facilite la constitution de statistiques, celles-ci servant ensuite à dresser un portrait juste des menaces et de l'évolution actuelles liées à la cyberfraude. Donnons d'abord un aperçu et une définition générale de la cybercriminalité, puis examinons les nombreuses formes que peut prendre la cyberfraude.

1.1 Définition et classification de la cybercriminalité

L'utilisation d'Internet a explosé au cours des dix dernières années; en effet, le nombre de ses utilisateurs a quintuplé, puisqu'il est passé de 361 millions en 2000 à près de deux milliards sur la planète en 2010 (McAfee, 2010 a), 4). La façon dont les Canadiens font des affaires a également changé. L'utilisation de chèques par des consommateurs a chuté tandis qu'a augmenté de façon marquée celle des cartes de crédit ou de débit ainsi que les transactions par Internet pour l'achat, la vente ou la gestion financière (Canada 2005, 7). Aujourd'hui, quelque 60 % des Canadiens effectuent des opérations bancaires en ligne; aux États-Unis, huit foyers sur dix le font (Symantec 2010, 12). À l'instar d'autres aspects de la mondialisation, la croissance d'Internet a été beaucoup plus rapide que l'adaptation des mécanismes de contrôle réglementaire, ce qui a ouvert de nouvelles possibilités criminelles et posé des défis de taille aux services de police du monde entier.

La cybercriminalité prend une multitude de formes qui ne se plient à aucune classification normalisée. L'absence de définition claire est problématique et a une incidence sur de nombreux aspects de la prévention et des mesures correctionnelles (Gordon et Ford 2006, 13). Le cybercrime est plus difficile à définir que le crime classique hors ligne, car un ordinateur ou un appareil peut être l'agent, la cible ou l'instrument d'un crime, et le crime peut être perpétré sur l'ordinateur seul ou à d'autres endroits hors ligne (Gordon et Ford 2006, 13). Généralement parlant, le cybercrime consiste à utiliser un ordinateur pour faciliter ou commettre une infraction criminelle (O'Neill 2000, 241).

On peut définir la cyberfraude, elle, comme un acte malhonnête ou trompeur commis grâce à Internet (ou à une technologie informatique) qui prive le public ou une personne d'un bien, d'argent, d'un titre de valeur ou d'un service (Smith et Urbas 2001, 1). On peut commettre une fraude par Internet en communiquant une information fallacieuse ou trompeuse, en ne respectant pas une entente contractuelle conclue en ligne ou en s'appropriant des fonds transmis électroniquement. Lors de transactions par Internet, on ne dispose pas de précieux indices sociaux qui nous aident à éviter la fraude dans le monde hors ligne, tels l'apparence, l'expression du visage, le langage corporel, la voix, la tenue et les manières car il y a entente instantanée et paiement entre anonymes opérant n'importe où dans le monde. Cela augmente beaucoup la

possibilité pour des individus de cacher leurs véritables identité et intentions et explique en bonne mesure qu'il est plus facile de commettre une fraude par Internet (que hors ligne).

À ses articles 2 à 10, la Convention sur la cybercriminalité de 2001 du Conseil de l'Europe répartit cette dernière selon quatre catégories principales :

1) Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques;
2) Infractions informatiques;
3) Infractions se rapportant au contenu;
4) Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

La cybercriminalité peut aussi prendre la forme d'attaques massives et coordonnées contre l'infrastructure de l'information essentielle d'un pays, par exemple celles lancées contre l'Estonie en 2007 (Schjolberg 2008, 9). De telles attaques sont non seulement en hausse, mais d'une complexité exponentielle au fil du temps (Walther 2004, 7).

L'une des distinctions fondamentales entre les criminalités informatique et classique est que cette dernière survient dans un espace donné et touche un certain nombre de victimes, alors que la cybercriminalité a un impact mondial (Royaume-Uni 2010, 5). L'auteur de cybercrimes peut opérer n'importe où dans le monde et viser un grand nombre de personnes ou d'entreprises sans tenir compte des frontières entre les pays. Ceci pose évidemment un défi pour l'application de la loi, et les auteurs de cybercrime cherchent souvent à tirer parti de ce fait en réalisant leurs activités dans un pays donné, mais à l'encontre de nombreux autres pays. De façon délibérée, leurs activités ciblent des pays ou transitent par des pays dont ils savent la réglementation faible ou dont la coopération lors d'enquêtes est connue pour être lacunaire (Royaume-Uni 2010, 5). Ils minimisent ainsi le risque que leurs activités soient détectées, retracées ou leur valent une condamnation.

Vu l'ampleur de la cybercriminalité et l'immense bassin de victimes potentielles, il est difficile d'évaluer précisément le nombre de tels incidents chaque année. Chose certaine, les États-Unis ont enregistré dans l'ensemble le plus grand nombre d'activités malveillantes dans le monde en 2009 et ont été le pays d'origine du plus grand nombre d'attaques en 2009, puisqu'ils ont connu 23 % de l'activité mondiale dans ce domaine (Symantec 2010, 16)[1]. D'après Symantec, cependant, on cherche de plus en plus à faire émaner cette activité malveillante de pays en développement et, en 2009, cette tendance s'est accentuée (Symantec 2010, 7). Pour la première fois depuis que Symantec analyse cette activité par pays, soit en 2006, un autre pays que les États-Unis, la Chine ou l'Allemagne figure aux trois premiers rangs[2]. La principale explication en est

[1] Il s'agit d'une légère diminution par rapport à 25 % en 2008.
[2] En 2008 et en 2009, les États-Unis figuraient au premier rang comme pays d'origine d'attaques, pour le code malveillant, pour les hôtes d'hameçonnage et les robots de recherche, tandis que la Chine venait au deuxième rang comme pays d'origine d'attaques. En 2009, le Brésil venait au troisième rang pour les activités malveillantes, l'Allemagne au quatrième (après s'être classée troisième en 2008). D'après Symantec, voici la classification des principaux pays en 2009 concernant les activités malveillantes : États-Unis (19 %), Chine (8 %), Brésil (6 %), Allemagne (5 %), Inde (4 %), Royaume-Uni (3 %), Russie (3 %), Pologne (3 %) Italie (3 %) et Espagne (3 %).

que la sécurité de l'information ainsi que la législation et les politiques afférentes sont moins élaborées dans les économies émergentes, celles-ci offrant alors un environnement dans lequel des activités criminelles peuvent être effectuées avec moins de risque d'être détectées et avec moins de crainte (Smith et Urbas 2001, 2). Notons que le Canada n'a figuré ni en 2008 ni en 2009 parmi les dix premiers pays pour l'ensemble des activités malveillantes relevées par Symantec, ce qui donne à penser que notre pays n'est pas devenu un havre pour les auteurs de cybercrimes, même s'il a été relativement lent à adopter des lois pour résoudre le problème[3].

1.3 Définition des victimes de la cyberfraude

Bien que les particuliers (c.-à-d. le grand public) soient les premières victimes de la plupart des fraudes dans la mesure où ils en assument habituellement le coût financier, entre autres par une majoration des primes d'assurance, des frais des cartes de crédit et des taux d'intérêt, il existe d'autres victimes. On peut distinguer entre les *premières victimes*, notamment des particuliers, des entreprises ou des organismes publics qui subissent les préjudices initiaux d'une fraude, et les *victimes secondaires*, c.-à-d. celles qui en dernier ressort paient les pertes économiques provoquées par le crime (Levi et Burrows 2008, 304). Il s'agit d'institutions financières, de compagnies d'assurance et d'autres qui, aux termes d'un contrat ou d'une mesure réglementaire, consentent à rembourser une partie ou la totalité de leurs coûts aux premières victimes. Il faut souligner que certaines cyberfraudes ne touchent qu'une seule classe de victimes, mais que d'autres touchent plus d'une classe en fonction des circonstances du cas (Levi et Burrows 2008, 304). Par exemple, dans le cas d'une fraude concernant une carte de paiement, les victimes peuvent être le détenteur et l'émetteur de celle-ci ainsi que le marchand.

Le présent document de travail vise d'abord à évaluer la possibilité de recourir à des méthodes novatrices pour estimer l'ampleur de la cyberfraude, tout comme les sources de données existantes et les lacunes, puis à suggérer de nouvelles sources de données susceptibles de fournir un portrait plus juste de son ampleur au Canada. Il importe donc de se pencher sur les divers coûts d'une fraude pour les différentes victimes :

- les coûts directs assumés par les victimes à la suite d'une fraude (c.-à-d. le montant exact de la perte);
- les coûts assumés par les victimes pour prévenir une fraude avant l'événement (c.-à-d. les mesures défensives prises par des institutions des secteurs tant public que privé pour se prémunir contre la fraude, telles que le déchiquetage des documents ou le recours à des mesures de sécurité TI);
- les coûts d'intervention après la fraude (c.-à-d. frais de justice criminelle, notamment services des policiers, des procureurs et des tribunaux ainsi que, dans le cas d'organisations, enquêtes privées internes, renforcement des mesures de sécurité et notification de consommateurs) (Levi et Burrows 2008, 305).

D'autres pertes indirectes, plus difficiles à quantifier, peuvent découler d'une réduction de l'utilisation des services bancaires en ligne (en supposant que ces derniers soient plus

[3] À titre d'exemple, le Canada a été le dernier pays du G-8 à adopter des mesures législatives anti-pourriel.

économiques pour la banque victime) ou d'un préjudice à la réputation de l'organisation flouée sur le marché (en supposant que la fraude porte des consommateurs et d'autres sociétés à éviter de faire affaire avec elle). En dernière analyse, la question de savoir quel groupe ou quelle entité assume les coûts de la cyberfraude est complexe et il sera difficile d'en établir le total pour l'économie canadienne (ce problème est examiné en détail plus loin).

1.4 Les types les plus fréquents de cyberfraude

La cyberfraude consiste à s'emparer intentionnellement du bien d'autrui par tromperie, et ce crime de situation gagne en popularité. Cela s'explique en bonne partie par un changement fondamental dans les méthodes par lesquelles différents biens sont possédés et stockés grâce au développement rapide de la technologie, des communications et de la mondialisation (Albanese 2005, 7). Ainsi dans la société canadienne, les transactions par carte de crédit ou de débit surpassent en valeur celles au comptant; de plus, l'arrivée et l'expansion d'Internet, qui facilite les transactions sans fil, a rendu relativement facile le vol, tout comme la conversion d'un bien volé en comptant (Albanese 2005, 7).

Aujourd'hui, les infractions liées à l'identité sont la façon la plus courante de frauder des consommateurs. Voici d'autres exemples de fraude par Internet : paiement à l'avance (par exemple demandé depuis le Nigéria), loterie et héritage, vente aux enchères en ligne, sans compter d'autres infractions liées à l'identité et aux cartes de paiement. La fraude par Internet a été facilitée par l'obtention de numéros de cartes de crédit à partir de divers services en ligne, qui peuvent ensuite servir à payer frauduleusement des biens ou des services commandés en ligne. Voici des exemples de certaines des fraudes par Internet les plus fréquentes et qui se répandent le plus.

Fraude suscitant la crainte chez la victime

Une fenêtre flash trompeuse laisse entendre à l'utilisateur que son ordinateur est infecté par un virus et l'invite à acheter un faux logiciel antivirus pour résoudre son problème. Si la victime consent à l'achat, elle fournit les données de sa carte de crédit à l'auteur de la fraude. Une telle fraude constitue l'une des menaces les plus fréquentes par Internet, car elle se fonde sur une manipulation psychologique de la victime (McAfee 2010 a), 7). En suscitant chez des utilisateurs d'Internet la crainte que leur ordinateur et leurs données soient menacés, des gens ont obtenu l'accès à leurs appareils et sont ainsi parvenus à les frauder directement de millions de dollars. Symantec a noté une augmentation marquée des fraudes de cette nature au cours des six premiers mois de 2009 comparativement aux six derniers mois de 2008; cette société a aussi relevé 250 variantes de ce type de fraude en circulation dans Internet (Symantec 2009).

Hameçonnage

Voilà l'une des menaces les plus marquantes dans Internet aujourd'hui. Des attaques récentes font preuve d'une sophistication technique plus poussée; en effet, elles mettent à profit des failles bien connues des navigateurs Web populaires, notamment Internet Explorer, pour installer des logiciels malveillants qui recueillent des données sensibles sur la victime. L'hameçonnage prend

différentes formes : pourriel, message instantané ou demande fictive sur un site de réseautage social, souvent avec hyperlien renvoyant à un site Web réaliste, mais faux, qui vise à capter le mot de passe ou encore le numéro de carte de crédit ou de compte bancaire de la victime en imitant la présentation et le comportement d'un site Web bancaire en ligne authentique. Nous l'avons déjà dit, ce type de fraude a grandement bénéficié des nombreuses trousses logicielles conçues à cette fin, dotées d'une interface pointer-cliquer peu coûteuse, facile à employer et vendue dans l'économie en ligne clandestine. L'hameçonnage tire en partie son grand succès de la capacité des sites Web bien conçus à tromper le consommateur ordinaire (Dhamija et al. 2006)[4].

En 2009, Symantec a détecté 59 526 hôtes d'hameçonnage, ce qui représentait une augmentation de 7 % par rapport aux 55 389 de 2008 (Symantec 2010, 18). Toujours en 2009, 36 % des adresses URL d'hameçonnage repérées par Symantec se trouvaient aux États-Unis (Symantec 2010, 18). En 2005, 60 % des répondants à un sondage réalisé par la société VISA auprès de Canadiens ont affirmé qu'ils fourniraient probablement des renseignements personnels en réponse à un courriel qui leur semblerait provenir de source autorisée, tandis que 4 % d'entre eux ont affirmé avoir été victimes d'hameçonnage (Stroik et Huang 2009, 193).

Vente aux enchères en ligne

Lors d'une vente aux enchères en ligne, le vendeur peut cacher son identité; belle occasion pour lui de tromper l'acheteur (Lee et al. 2010, 2991). Comme nous l'avons mentionné, l'anonymat d'Internet accroît la probabilité que le vendeur profite de l'occasion; de son côté, l'acheteur éprouve beaucoup de difficulté à faire confiance à ce dernier et à en anticiper le comportement (Lee et al. 2010, 2991). Une fraude lors d'une vente aux enchères en ligne, possible tant durant qu'après celle-ci, peut suivre l'un ou plusieurs des scénarios suivants : fausse représentation de l'article; fausse enchère visant à maintenir le prix peu élevé; fausse enchère du vendeur visant à relever le prix; ajout de frais cachés pour un article, par exemple d'expédition ou de manutention; non-livraison de l'article; offre d'un bien provenant du marché noir; transaction en ligne frauduleuse moyennant carte de crédit (Lee et al. 2010, 2992). Une autre plainte fréquente porte sur un faux paiement au vendeur, notamment par chèque volé ou falsifié ou à même un compte insuffisamment approvisionné pour couvrir le paiement.

Site Web fictif

Le processus consistant à acheter un bien ou un service directement en ligne sans enchère est également sujet à la fraude. Au cours des dernières années, les gens se sont perfectionnés dans la création de sites Web frauduleux et de produits de consommation réalistes. Depuis de faux produits pharmaceutiques jusqu'à des logiciels, les gens recherchent constamment de nouvelles

[4] Une étude de Dhamija et al. a établi qu'un bon site Web d'hameçonnage trompe 90 % des utilisateurs et que les indices actuels de navigation anti-hameçonnage sont inefficaces. L'étude a aussi établi que 23 % des utilisateurs ne regardent ni la barre d'adresse ou d'état ni les indicateurs de sécurité et que l'utilisateur moyen se trompe 40 % du temps, lorsqu'il s'agit de détecter un site Web d'hameçonnage.

façons d'en tromper d'autres et de les amener à fournir des renseignements personnels ou relatifs à leur carte de crédit.

Rencontre en ligne

Pour commettre une infraction liée à un site de rencontre en ligne, le fraudeur commence habituellement par afficher une photographie attrayante sur le site (souvent celle d'un mannequin ou d'une célébrité quelconque). Le fraudeur envoie des messages à d'autres membres du site pour faire part de son intérêt. L'étape suivante consiste à échanger avec la victime potentielle, le plus souvent par courriel ou messagerie instantanée. Le fraudeur établit un lien personnel en vue de demander du comptant, un bien ou un avantage quelconque. Certains fraudeurs correspondent avec leur victime durant des semaines ou des mois, planifiant et échafaudant un plan et gagnant la confiance d'une personne crédule qu'ils n'ont jamais rencontrée. La victime se laisse séduire par une histoire habituellement chargée d'émotion, prometteuse sur le plan financier ou à saveur religieuse. Évidemment, le fraudeur continue à leurrer sa victime et à jouer le jeu aussi longtemps qu'il ne lui a pas soutiré des renseignements relatifs à sa carte de crédit, à son compte bancaire ou même de l'argent (Longe et al. 2009, 128).

Fraude nigériane 419

Cette fraude doit son nom à l'article 419 du *Code criminel* du Nigéria (Chawki 2009). Également connue comme celle du « paiement à l'avance », elle consistait à l'origine, souvent à partir de ce pays, à cibler des victimes n'importe où dans le monde grâce à une lettre envoyée habituellement par la poste. Peu après, des fraudeurs d'autres pays, notamment d'Afrique, des États-Unis, du Canada et de la Grande-Bretagne, ont eu recours à Internet pour perpétrer cette fraude. On en parle couramment comme du « paiement à l'avance », parce que la victime est incitée à verser une avance au fraudeur contre la promesse d'obtenir plus tard une forte somme (King et Thomas 2009, 207).

La fraude prend habituellement la forme d'un pourriel de la part d'un étranger devant transférer des millions de dollars hors de son pays, puis de l'offre au récipiendaire d'un pourcentage des fonds pour son aide à effectuer le transfert. Le fraudeur demande aussi à sa victime d'assumer d'emblée divers frais pour boucler l'affaire. Le plus souvent, la fraude s'inscrit dans une longue relation au cours de laquelle la victime s'engage graduellement dans le scénario, séduite par l'aptitude du fraudeur à instaurer une sympathie, de bons rapports et une confiance avec elle, sans jamais la rencontrer en personne (King et Thomas 2009, 210). Cette fraude a pris une ampleur considérable au cours des dernières années et créé un problème mondial pour les organismes d'application de la loi. Comme pour tous les types de cyberfraude, les plaintes déposées auprès des autorités n'émanent que d'une petite fraction des victimes. Le Centre antifraude du Canada affirme avoir reçu 167 plaintes à ce sujet de janvier à septembre 2004, les victimes ayant perdu environ 4,2 millions de dollars (Chawki 2009, 6).

Investissements et valeurs mobilières

De nos jours, Internet sert couramment à échanger des titres et, dans beaucoup de cas, il a été l'instrument de fraudes dans le marché mondial. Dans les exemples les plus patents, on s'est servi de la bourse des valeurs mobilières pour attirer des investisseurs ou pour manipuler le marché, grâce à un stratagème consistant à gonfler artificiellement le cours d'une action pour la vendre ensuite à profit. On y recourt couramment pour manipuler une action dont le prix est bas (cotée en cents), habituellement émise par une société ayant peu de valeur ou peu attrayante (Paget 2009, 12). Après avoir acheté un grand nombre de parts à bas prix, un promoteur sans scrupule de cette action utilise un programme de messagerie électronique en masse pour envoyer des messages enthousiastes à des milliers d'utilisateurs Internet. Un ou deux jours plus tard, après une hausse artificielle du cours de l'action, le fraudeur vend ses parts et réalise un profit rapide, alors que les investisseurs naïfs et avides perdent leur argent. La prolifération de spéculateurs sur séance en ligne contribue à la volatilité du cours des actions, particulièrement de celles qui sont peu négociées. Cela ouvre de nouvelles possibilités à des fraudeurs souhaitant manipuler le cours des actions, seuls ou avec d'autres. Au Canada, les fraudes les plus fréquentes que l'on observe en matière de valeurs mobilières sont la manipulation illicite du marché, les stratagèmes d'investissement à rendement élevé, les investissements illicites à l'étranger et les stratagèmes pyramidaux (à la Ponzi) (SCRC 2010).

D'après le Service canadien de renseignements criminels, les fraudes relatives à des valeurs mobilières sont de plus en plus élaborées et, au cours des dernières années, les organismes chargés de l'application de la loi ont relevé des cyberfraudes combinant des éléments de nombreux stratagèmes et mettant en cause de nombreux cybermoniteurs tant du pays d'origine qu'étrangers (SCRC 2010). L'ampleur et la complexité de ces stratagèmes aident à camoufler une activité criminelle et génèrent des profits substantiels, en plus de faciliter l'évasion fiscale et le blanchiment d'argent. Certains sites de réseautage social, comme *MySpace* et *Facebook,* de même que des tableaux d'affichage en ligne, comme *Craigslist,* ont également servi à publier des communiqués à l'allure professionnelle, mais faux, ainsi que de la documentation promotionnelle anonyme et aussi à recruter des complices. Par ailleurs, des fraudeurs recourent de plus en plus à des marchés virtuels, à des systèmes de négociation électronique ou à des services de virement télégraphique pour transférer anonymement des fonds ailleurs. D'autres sites Web du marché noir servent à acheter et à vendre des renseignements volés relatifs à des comptes, notamment à des cartes de crédit, ou offrent des services commerciaux illicites.

Selon l'Indice des investisseurs 2009 des Autorités canadiennes en valeurs mobilières (ACVM), un peu moins de quatre Canadiens sur dix (38 %) se sont peut-être fait offrir un investissement frauduleux, soit une proportion conforme aux constatations de 2006 et de 2007 (Ipsos Reid 2009, 63). Parmi eux, une personne sur dix (11 %) a reconnu avoir investi de l'argent dans ce qui s'est révélé un investissement frauduleux. Sur l'ensemble de la population canadienne, cela signifie que 4 % des Canadiens ont été victimes de fraude, soit la proportion relevée en 2006 et en 2007 (Ipsos Reid 2009, 6). Les Canadiens sont sollicités en vue d'un investissement frauduleux le plus souvent par courriel (33 %), par un inconnu au téléphone (28 %), par un ami, un membre de leur famille ou un collègue de travail (18 %) (Ipsos Reid 2009, 5). Par ailleurs, le montant investi à ces occasions semble avoir augmenté. En 2009, 38 % de ces personnes ont investi 5 000 $ ou plus

comparativement à 32 % d'entre elles en 2006. Le montant moyen investi dans l'ensemble du Canada a été de 7 634 $. La plupart des victimes ne récupèrent jamais leur argent.

Un Canadien sur quatre (26 %) affirme avoir signalé la tentative de fraude aux autorités comparativement à 17 % d'entre eux en 2007 et à 14 % en 2006 (Ipsos Reid 2009, 5). Pourtant, depuis 2006, moins de Canadiens pensent qu'il importe de faire part de leurs soupçons à ce sujet[5]. Quant à ceux qui n'ont pas signalé la tentative parce qu'il s'agissait probablement d'un pourriel (16 %), ils ont sans doute estimé que cela ne changerait rien de le faire (12 %), ils étaient incertains qu'il s'agissait d'une fraude (12 %), ils avaient estimé n'avoir rien de concret à signaler (11 %) ou ils avaient préféré tout simplement ignorer le fait (11 %) (Ipsos Reid 2009, 5).

Identité

L'une des stratégies les plus courantes pour frauder consiste à créer de faux documents d'identité. Une fois qu'une fausse identité a été établie de façon convaincante, il est possible de voler de l'argent ou de poser un autre acte illicite, puis d'échapper à une enquête ou à une poursuite. Internet favorise ce type d'activité frauduleuse en facilitant la manipulation du courriel et d'une adresse Internet et en camouflant la source d'un message grâce à des instruments techniques tels qu'un dispositif de préservation de l'anonymat, un réexpéditeur anonyme ou tout autre instrument semblable.

La fraude relative à une carte de crédit est la plus fréquente se rapportant à l'identité (Berg 2009, 227). À titre d'exemple, le gouvernement du Royaume-Uni a signalé 328 millions de livres sterling de pertes en 2008 liées à la fraude relative à une carte de crédit, au cours de laquelle cette carte a été utilisée en l'absence du consommateur (une augmentation de 13 % par rapport à l'année précédente) (Royaume-Uni 2010, 5). Dans ce scénario, le fraudeur usurpe l'identité de la victime pour demander et se procurer une nouvelle carte de crédit ou utiliser frauduleusement une carte appartenant à la victime. Voici d'autres fraudes ayant trait à l'identité : usurper l'identité de la victime pour se procurer des services publics, notamment téléphoniques; ouvrir un compte bancaire grâce aux données personnelles de la victime ou tirer un chèque sur le compte de celle-ci; obtenir un emploi au nom de la victime; obtenir un permis de conduire ou une autre pièce d'identité produite par un organisme gouvernemental au nom de la victime; faire une fausse déclaration d'impôt; emprunter au nom de la victime.

Carte de crédit

Dès le début du commerce électronique, des fraudeurs en ligne ont ciblé les cartes de crédit (Wall 2010 a), 70). Les utilisateurs d'Internet se sont dits préoccupés par la collecte et l'utilisation des renseignements personnels qu'ils fournissaient lors de leurs achats en ligne (Sheehan et Hoy 200, 62); toutefois, souvent cela ne les empêchent pas de passer outre à leurs préoccupations en matière

[5] Huit Canadiens sur dix (78 %) estiment important de faire part de leurs soupçons que quelqu'un leur a offert un investissement frauduleux (40 % d'entre eux y étant fortement favorables comparativement à 53 % en 2006, et 38 % y étant plus ou moins favorables comparativement à 33 % en 2006).

de données confidentielles en échange d'avantages tels que la commodité (Chellappa et Sin 2005, 181). Cette tendance pose un problème puisque des biens ou des services peuvent être acquis facilement grâce à une carte valide obtenue frauduleusement. On peut également se les procurer grâce à une carte contrefaite à partir de données volées, par exemple dans l'économie clandestine en ligne abordée ci-dessous. On peut aussi cloner une carte de crédit grâce aux données recueillies par un lecteur clandestin (opération dite d'« écrémage ») durant une transaction licite ou sur le relevé d'une carte de crédit jeté au rebut (Wall 2010 a), 70).

Au cours des dernières années, le marché de ce type de fraude (dite « aux cartes bancaires ») a beaucoup évolué. Comme nous le verrons plus loin, des groupes de discussion volumineux et hautement modérés se consacrent à l'achat et à la vente de renseignements et de produits volés, à l'échange d'astuces et de techniques et à l'affichage de nouvelles sur la cybercriminalité (Howard 2009, 28). Plusieurs opérations d'application de la loi largement diffusées (notamment Firewall, la plus célèbre, en 2004) ont obligé à rendre clandestines de nombreuses opérations de cartes bancaires auparavant apparentes; une bonne part des discussions actuelles en ligne sur le sujet se tiennent plutôt par canaux sécurisés, notamment un clavardoir Internet (IRC), par messagerie ou par courriel (Howard 2009, 26). Les pertes globales canadiennes dues à la fraude aux cartes de paiement ont chuté légèrement, passant de 512,2 millions de dollars en 2008 à 500,7 millions de dollars en 2009 (SCRC 2010, 29). Dans le même temps, les pertes dues à la fraude aux cartes de débit ont augmenté de 36 %, passant de 104,5 millions de dollars en 2008 à 142,3 millions de dollars en 2009 (SCRC 2010, 29).

Délit d'initié

Une personne employée à l'interne peut recourir à Internet pour obtenir anonymement des données qui ne concernent pas son travail et en faire un usage frauduleux à son avantage personnel (Campbell 2009). Des employés du secteur tant public que privé ont profité d'occasions pour commettre diverses fraudes en ligne : manipuler un système de traitement électronique de demandes d'indemnisation, compromettre une clé de signature numérique électronique, modifier ou détourner de leur véritable destinataire des transferts de fonds électroniques (Smith et Urbas 2001, 54). Un initié véreux peut également accéder par électronique au relevé d'un client ou d'un autre employé et en tirer profit à une fin frauduleuse. Un tel geste malveillant est couramment perpétré par un employé ou un entrepreneur en titre aussi bien que par un ex-employé mécontent d'avoir été renvoyé ou mis à pied ou qui a démissionné.

Soulignons également qu'un initié « bien intentionné » ou négligent pose une menace supplémentaire s'il divulgue des données susceptibles d'être exploitées par un non-initié malveillant à l'encontre d'une organisation (Wall 2010 b), 3). D'après des estimations, en 2009, les atteintes à la protection des données perpétrées résultaient de la négligence d'un initié à hauteur de 40 % aux États-Unis et de 46 % au Royaume-Uni (Wall 2010 b), 3). Dans certains cas, l'initié utilise un mot de passe très simple, voire le même mot de passe pour tous les sites sécurisés auxquels il a accès. Ou encore, il écrit ses mots de passe sur des papillons qu'il colle à l'écran de son ordinateur ou les communique à ses collègues, afin que ceux-ci prennent connaissance de ses courriels (p. ex. durant ses vacances) (Wall 2010 b), 9). D'autres initiés courent sciemment le risque de contourner les mesures de sécurité pour être plus efficace dans leur travail (Wall 2010 b), 9). Dans d'autres cas, un employé peut être amené par un non-initié

malveillant à dévoiler un renseignement sensible ou à lui donner accès à un système dans un stratagème d'« ingénierie sociale », intimement convaincu de rendre service et agissant de bonne foi (Wall 2010 b), 10).

2.0 Ampleur et coût de la cyberfraude

Sous ses diverses formes, la cyberfraude représente-t-elle un problème sérieux au Canada? Comment se comparent sa fréquence et son coût à ceux d'autres crimes? Bien que nombre de cyberfraudes soient documentées dans les médias électroniques et la presse, leur fréquence et les pertes qu'elles provoquent sont extrêmement difficiles à établir avec précision. Le Canada ne dispose pas d'un moyen uniforme pour recueillir des données à leur sujet.

À l'instar d'autres types de fraude, celle qui est commise par Internet est rarement signalée aux autorités chargées de l'application de la loi. Il est donc extrêmement difficile de mesurer l'ampleur et la portée du problème. Le manque de statistiques valables et fiables nous a sérieusement nui pour comprendre la nature, l'ampleur et l'impact de la cyberfraude, tout autant que la capacité des responsables de l'application de la loi à la contrer. La principale source de renseignements à son sujet, ce sont les enquêtes sur les victimes d'entreprises et les centres de signalement pour consommateurs ainsi que les comptes rendus anecdotiques de poursuites criminelles fructueuses dans les médias. Les incidents de cyberfraude rendus publics ne représentent qu'une faible partie de tous ceux qui surviennent; on a donc besoin de recueillir plus systématiquement des données sur la nature et l'ampleur de cette fraude dans notre pays.

Diverses raisons déterminantes font que les entreprises décident de ne pas signaler une fraude à la police. Celles-ci peuvent hésiter, craignant que l'incident n'ait trop peu d'importance ou qu'il ne soit impossible de récupérer leur perte par la voie juridique; ou encore que le résultat escompté ne justifie pas le temps et les ressources nécessaires pour signaler l'incident aux autorités et prendre part à une poursuite (Smith et Urbas 2001, 41). Elles s'en remettent parfois à d'autres moyens, par exemple faire appel à un enquêteur interne ou privé ou encore signaler l'incident à une entité non responsable de l'application de la loi (telle PhoneBusters, le CANAFE ou le Conseil canadien des bureaux d'éthique commerciale) (Taylor-Butts et Perreault 2008, 12). L'autre raison importante dissuadant une entreprise de signaler un tel incident est la tendance à dissimuler au public le fait d'avoir été victime de fraude, par crainte de perdre des affaires ou de nuire à leur réputation commerciale sur le marché (Smith et Urbas 2001, 42). Les gouvernements, eux, hésitent à faire part des infractions à leur service de sécurité de la TI, par crainte de s'aliéner l'électorat ou que celui-ci perde confiance en la fonction publique.

À l'évidence, on a besoin de recueillir plus systématiquement des données sur la nature et l'ampleur de la cyberfraude au Canada et d'analyser le problème plus en profondeur. Il importe aussi de constater que, dans les quelques cas où une recherche s'effectue, il existe nombre de problèmes liés aux données ou à la méthodologie (White et Fisher 2008, 13). Ainsi, on ne définit pas et n'utilise pas uniformément les expressions « vol d'identité », « fraude » et « cyberfraude » entre organismes et organisations. Ainsi, les données dont on peut disposer ne sont pas nécessairement comparables; en effet, elles dépendent de diverses variables propres à chaque organisme, notamment : budget, dotation, ressources, sensibilisation au problème et mesure prise à l'échelle nationale. On doit aussi évoquer la difficulté de constituer un échantillon aléatoire de

victimes d'une cyberfraude ou d'un vol d'identité, car celles qui communiquent avec des responsables de l'application de la loi ou un organisme ne représentent pas nécessairement l'ensemble des victimes. Par conséquent, les études identifiant les victimes en fonction de leur communication initiale avec un organisme, des responsables de l'application de la loi ou même d'un sondeur ne témoignent probablement pas de toutes les victimes et de toutes les infractions en matière de fraude ou de vol d'identité.

En fait, on ne dispose que de peu de statistiques fiables sur l'ampleur de cette fraude ni de moyen précis pour estimer le nombre de telles fraudes, et cela, largement parce qu'une part importante de ces incidents ne sont pas signalés, identifiés, voire détectés par les victimes. On a une certaine idée de l'ampleur de la cyberfraude grâce aux sondages auprès de certains groupes du milieu ou de ménages. En règle générale, cependant, le secteur privé compte peu de sources de données centralisées et les données disponibles ne sont ni complètes ni comparables d'une entreprise à l'autre (Canada 2005, 12). Outre que les victimes sont difficiles à repérer et à joindre, les données disponibles ont diverses sources et nombre d'entre elles souffrent de lacunes méthodologiques (Levi et al. 2007, 8).

Les statistiques officielles n'indiquent pas toujours le moyen par lequel une cyberfraude a été perpétrée, de sorte qu'il est difficile d'établir la portée et l'ampleur du problème. Faute de renseignements plus fiables et précis, on ne peut documenter la nature et l'étendue exactes de ce problème. Statistiques Canada a mis au point une Déclaration uniforme de la criminalité en collaboration avec l'Association canadienne des chefs de police (Canada 2005, 35). Entrée en vigueur en 1962, elle sert à établir des statistiques sur la criminalité et le trafic à partir des crimes ayant fait l'objet d'une enquête de la part de tous les services de police canadiens (Canada 2005, 35). Autrement dit, les statistiques officielles sur la fraude au Canada, établies grâce à la Déclaration uniforme de la criminalité, ne prennent en compte que les incidents de fraude signalés à la police (Taylor-Butts et Perreault 2008, 5). Sous la rubrique « type de fraude » figure toute fraude comportant l'utilisation non autorisée d'un ordinateur ou l'utilisation d'un ordinateur à des fins illégales, notamment le piratage informatique, l'emploi illégal de l'identité ou du mot de passe personnel d'un usager (Kowalski 2002, 17). L'ajout de la rubrique « cybercrime » à la déclaration UCR2 en 2005 a permis à la police d'indiquer si un ordinateur ou Internet a servi à commettre une fraude. Cependant, cette déclaration ne ventile pas les données jusqu'à permettre de préciser le type de fraude commise par ordinateur ou par Internet.

Pour sa part, l'Association des banquiers canadiens (ABC) publie presque chaque année un rapport sur la fraude par carte de crédit (ABC, 2011). D'après son rapport récent, on a signalé 45 103 vols de carte de crédit au cours de l'année terminée en décembre 2009, qui ont entraîné une perte de 27 208 823 $CAN[6]. La perte moyenne par carte a été de 693,26 $. Selon l'ABC, 2 442 demandes frauduleuses de carte de crédit ont été faites en 2009 au Canada, ce qui a entraîné une perte de 4 707 088 $CAN, soit de 1 927,55 $CAN en moyenne par compte. Il y aurait eu 294 549 achats frauduleux avec carte de crédit par commerce électronique, téléphone ou courriel

[6] Cela ne comprend que les cartes Amex, MasterCard et Visa. À distinguer des cartes perdues (22 304 Canadiens ayant signalé avoir perdu une carte).

pour un total de 140 443 893 $CAN en 2009, entraînant une perte moyenne de 140 443 893 $CAN en 2009, la perte moyenne par compte s'établissant à 476,81 $CAN.

Bien que nombre d'enquêtes nord-américaines incluent vraisemblablement des répondants canadiens, seule une petite portion des études portent explicitement sur le Canada. En 2007, l'Alliance CATA a fait enquête auprès de 322 experts canadiens en sécurité de la TI pour relever les défis importants dans ce domaine (Wennekes 2008). Selon les réponses obtenues, la plupart de ces experts se fient aux avis de leur réseau personnel d'experts de la TI. De plus, ces réponses mettent en lumière l'absence actuelle de pratiques idéales comme défi pour leurs organisations. Normalement, des pratiques idéales découlent de la sagesse collective, puis sont mises en commun (Wennekes 2008). Cette mise en commun est cruciale pour partager un ensemble de connaissances sur les pratiques idéales nécessaires à la sécurité de l'information.

D'après l'enquête, ces experts canadiens en sécurité de la TI considèrent leurs collègues et leur réseau personnel comme leurs principales sources de renseignements dans ce domaine (Wennekes 2008). Fait important, ils se disent tout à fait à l'aise de s'appuyer sur leur réseau personnel. Au sein d'un tel réseau, ils risquent moins de paraître mal informés ou mis au défi sur le plan technique; par ailleurs, les membres de ce réseau sont visiblement considérés comme sources crédibles d'information. Ces constatations corroborent les résultats de la recherche effectuée par des experts canadiens en sécurité de la TI, évoquée ci-dessous à la rubrique 9.2. D'après elles, de nouvelles initiatives, notamment créer une base de données en ligne des pratiques exemplaires que pourraient enrichir et consulter ces experts, mettre en place une communauté en ligne (p. ex. pour faire part de conseils et d'astuces) ou tenir des séances ou conférences d'information sur ces pratiques exemplaires pour chaque secteur d'activité, permettraient de contrer de façon proactive les menaces de cyberfraude et aussi de recueillir des renseignements fiables sur les menaces et les vulnérabilités existantes.

Une autre source de renseignements sur la cyberfraude est l'Enquête sur la fraude contre les entreprises, menée en 2008 par Statistique Canada auprès de 4 330 entreprises canadiennes du commerce au détail, de la banque et de l'assurance (Taylor-Butts et Perreault, 2008). Au total, 57 % des entreprises de vente au détail, 45 % des agences d'assurance et 84 % des institutions bancaires au pays qui ont fourni des informations avaient fait l'objet de fraude au cours des douze mois précédents. Dans le secteur de la vente au détail, les fraudes les plus fréquentes ont été un retour frauduleux de marchandises (81,2 %); l'utilisation frauduleuse d'une carte de crédit (32,1 %), l'utilisation d'argent contrefait (15,2 %) ou l'utilisation frauduleuse d'un chèque (15 %). Dans le secteur bancaire, les fraudes les plus fréquentes sont l'utilisation frauduleuse d'une carte de débit (49,8 %), l'utilisation frauduleuse d'un chèque (29,1 %), le dépôt avec insuffisance de fonds (9,9 %) et l'utilisation d'argent contrefait (6,2 %). Dans le secteur de l'assurance sur la santé et les biens, les fraudes les plus fréquentes sont une demande d'indemnisation frauduleuse (77 %), un paiement à l'avance (pourcentage estimé à 21,7 %) et une fausse facturation (pourcentage estimé à 17,3 %) (Taylor-Butts et Perreault, 2008). Fait intéressant, sept établissements de vente au détail sur dix et environ la moitié (52 %) des établissements bancaires ayant fait l'objet d'une fraude ou d'une tentative de fraude au cours des douze mois précédents ont signalé que ces actes avaient été commis en personne par le fraudeur (Taylor-Butts et Perreault, 2008). La poste ordinaire a été le moyen le plus souvent employé pour frauder une compagnie d'assurance (32 %); les banques,

elles, ont signalé qu'Internet (23 %) et le courriel (17 %) ont été les principaux instruments des fraudes dont elles avaient été l'objet (Taylor-Butts et Perreault, 2008).

D'après les auteurs, près de la moitié des magasins de détail (47 %) et des compagnies d'assurance (47 %) ont affirmé que, en général, ils n'avaient jamais signalé, ou alors rarement, les fraudes aux responsables de l'application de la loi (Taylor-Butts et Perreault 2008, 12). Moins d'un magasin de détail sur cinq ayant subi une fraude a affirmé l'avoir signalée soit à PhoneBusters (c.-à-d. au Centre d'appel antifraude du Canada), soit au Centre de signalement en direct des crimes économiques de la GRC (Taylor-Butts et Perreault 2008, 12). Les statistiques officielles sous-estiment probablement le nombre de fraudes commises à l'encontre de tels établissements au Canada.

De plus, la Gendarmerie royale du Canada ainsi que la Police provinciale de l'Ontario mènent présentement deux initiatives distinctes visant à centraliser le signalement des fraudes. La GRC tient le Centre de signalement en direct des crimes économiques (RECOL), mais elle tient aussi, conjointement avec la Police provinciale de l'Ontario, le centre PhoneBusters (qui a été renommé le Centre antifraude du Canada) pour recueillir les plaintes de fraude, mettre en commun des éléments de preuve avec d'autres organismes chargés de l'application de la loi sur la valeur en argent des pertes, les caractéristiques des victimes et l'emplacement géographique des incidents ainsi que pour éduquer la population au sujet des stratagèmes de fraude. En 2005, on a standardisé les renseignements recueillis dans ces deux initiatives (soit les données sur les crimes économiques commis par téléphone, Internet, télécopieur et courriel); ces deux bases de données sont néanmoins demeurées distinctes (Canada 2005, 13).

Selon le *Rapport statistique annuel 2010* du Groupe de l'analyse des renseignements criminels du Centre antifraude du Canada, le nombre de plaintes pour fraude de marketing de masse[7] au Canada est passé de 36 470 en 2008 à 48 837 en 2010 (Centre antifraude du Canada 2010). Fait intéressant, le nombre total de victimes a diminué tandis que les pertes totales en argent ont chuté de 59 273 771,99 $CAN en 2008 à 53 843 364,58 $CAN en 2010. L'âge moyen des Canadiens les plus souvent ciblés par une fraude de marketing de masse est de 50 à 59 ans. En 2010, les Canadiens ont déposé 11 783 plaintes relativement à des opérations frauduleuses de marketing de masse effectuées dans notre pays et ayant fait 2 752 victimes canadiennes (Centre antifraude du Canada 2010). La perte totale de ces dernières s'est élevée à 12 748 068,93 $CAN (comparativement à 7 674 plaintes et à des pertes de 10 370 441,40 $CAN en 2009). L'Ontario a été la principale province ciblée par ce type de fraude en 2010. D'après les plaintes formulées au Canada, les victimes ont été sollicitées en premier lieu par téléphone ou télécopieur et en deuxième lieu par courriel, Internet ou message texte (il s'agit des victimes ayant déclaré les plus grosses pertes en argent). Selon le nombre total de plaintes, c'est une escroquerie de service

[7] La fraude de marketing de masse a trait au hameçonnage, au stratagème de dons de bienfaisance, à la vente de marchandise, à une agence de recouvrement, à une offre d'emploi, au gain d'un prix ou encore à une escroquerie de marchandise ou de service (indéterminés).

qu'ont signalée surtout des consommateurs canadiens[8]. En 2010, les victimes étrangères des fraudes de marketing de masse réalisées à partir du Canada ont perdu un total de 8 960 571,96 $CAN. Au cours de la même année, le nombre total de plaintes et de victimes canadiennes d'un vol d'identité a augmenté, même si leurs pertes en argent ont diminué. La Western Union a été la principale entreprise retenue par les victimes canadiennes pour recevoir un paiement[9].

En 2008, la société TELUS et l'École de gestion Rotman de l'Université de Toronto ont procédé conjointement à une étude sur l'état de la sécurité de la TI au Canada (Hejazi et al. 2010, 228). Les réponses fournies par 300 experts en TI et en sécurité canadiens leur ont permis de comprendre en quoi les cybermenaces et les vulnérabilités différaient au Canada par rapport aux États-Unis. Une étude de suivi a été réalisée en 2009 auprès de 600 organisations et organismes gouvernementaux du Canada. Elle a permis de constater que les répondants signalaient un nombre beaucoup plus élevé d'infractions qu'en 2008 (11,3 par année en 2009, soit 3 de plus qu'en 2008). Par ailleurs, l'étude révèle que les pertes annuelles dues aux infractions ont atteint 834 149 $CAN par organisation comparativement à 423 469 $CAN en 2008. En outre, le Canada a rejoint les États-Unis en 2009 quant au nombre d'infractions : 14 % des entreprises canadiennes ont signalé une fraude en 2009 comparativement à 12 % des entreprises américaines en 2008[10]. En 2009, le nombre d'infractions signalées au Canada a augmenté : les accès non autorisés à des renseignements de la part d'employés ont augmenté de 112 % comparativement à 2008 et les fraudes financières se sont accrues de 75 %. D'après la recherche de 2009, la crise financière a eu une incidence négative sur les programmes de sécurité de la TI, les répondants y signalant une réduction moyenne de 10 % des budgets.

Une étude de suivi a été menée en 2010 auprès de 523 organisations canadiennes et organismes gouvernementaux (Begin 2010 b)). Selon ses auteurs et en 2010, les budgets de sécurité de la TI sont demeurés sous leur niveau de 2008. Le nombre d'infractions signalées s'est accru de 29 % par rapport à 2009, et la plus grande partie de cette hausse a touché des entités gouvernementales. En 2010, les entités gouvernementales visées dans la recherche ont signalé une moyenne de 22,4 infractions, soit une hausse de 74 % par rapport aux 13,4 infractions enregistrées en 2009. Autre tendance relevée durant cette recherche : alors que les utilisations frauduleuses d'un réseau sans fil, les attaques par saturation de service et la dégradation de site Web diminuaient, les attaques d'ingénierie sociale augmentaient qui abusaient de la confiance que l'utilisateur entretient dans ses relations avec d'autres, par exemple grâce à un stratagème d'hameçonnage. Les réseaux de

---

[8] Notons que la principale fraude de marketing de masse signalée sur le plan international concerne la « vente d'une marchandise par le plaignant » et que la principale fraude réalisée dans ce domaine à partir du Canada et signalée par des consommateurs américains concerne le « gain d'un prix ».

[9] Rappelons-nous, cependant, que ces renseignements n'étaient pas représentatifs de la fraude au Canada, car les personnes et les entreprises qui font un signalement à la police peuvent le faire auprès de leur service policier local plutôt qu'aux centres mis sur pied dans les initiatives susmentionnées (Canada 2005, 14).

[10] Notons aussi que l'une des faiblesses de l'étude a été qu'elle comparait les statistiques canadiennes sur les infractions à la sécurité de 2009 à celles de l'étude annuelle sur la cybercriminalité réalisée en 2008 par le Computer Security Institute (américain). Si les chercheurs avaient comparé des statistiques des deux pays pour l'année 2009, ils auraient pu conclure que le dossier des infractions au Canada n'était pas plus sombre que celui des États-Unis.

zombies, qui servent souvent à diffuser ce genre d'attaques, seraient également en hausse, rapporte-t-on. Enfin, le vol d'identité et celui des renseignements confidentiels des clients seraient aussi en hausse.

Certaines études menées ailleurs mettent également en lumière le coût de la cyberfraude sur une période donnée. Cependant, la collecte de données hors du Canada présente aussi certains problèmes de fiabilité et d'exactitude au moment d'évaluer le coût de la cyberfraude. La perte totale subie pour l'ensemble des fraudes et des stratagèmes d'Internet signalés aux organismes américains d'application de la loi en 2008 s'est élevée à 264,6 M$US, ce qui représente une augmentation de 10 % par rapport à l'année précédente et de 32 % par rapport aux 68 M$US en 2004 (Wagner 2009). L'organisme américain Consumer Sentinel affirme avoir reçu 370 012 plaintes de fraude en 2008, dont 193 817 (52 %) avaient trait au courriel et 40 596 (11 %) à Internet (site Web, notamment) (Paget 2009, 4). Cette année, les consommateurs ont déclaré des pertes par fraude de plus de 1,2 milliard de dollars américains, pour une perte moyenne de 349 $US. De ces plaintes, 64 % évoquaient Internet comme moyen de sollicitation, dont 49 % le courriel et 15 % le Web.

Si l'on en croit l'Internet Crime Complaint Centre des États-Unis, la perte totale pour fraude par Internet qui a été déclarée s'est établie à 560 M$US en 2009, la part la plus importante ayant trait à la non-livraison de marchandise (Royaume-Uni 2010, 13). Selon ce centre, les Américains ont, en 2008, déposé 33,1 % de plus de plaintes qu'en 2007, et le montant total des vols en ligne a atteint un record historique (Paget 2009, 4). En 2008, le centre a enregistré près de 275 000 plaintes ayant trait à une perte de 265 M$US, soit 10,6 % de plus qu'en 2007 (Paget 2009, 4). La moitié de ces fraudes s'est soldée par une perte de moins de 1 000 $US tandis que le tiers des plaignants (33,7 %) ont déclaré une perte de 1 000 à 5 000 $US (Paget 2009, 4). Seuls 15 % des plaignants ont déclaré une perte supérieure à 5 000 $US. Une vente aux enchères frauduleuse et la non-livraison d'une marchandise ont fait l'objet des principales plaintes déposées à ce centre.

Une enquête nationale sur les fraudes personnelles , menée en 2008 à l'échelle de l'Australie de juillet à décembre 2007 par le Bureau de la statistique de l'Australie, a permis d'estimer que près d'un milliard de dollars australiens ont été perdus lors de fraudes personnelles et que près d'un demi-million d'Australiens ont subi une forme de vol de leur identité durant cette période (Smith 2008, 379). D'après le gouvernement du Royaume-Uni, les pertes pour fraude par utilisation de la carte de crédit d'un consommateur en son absence se sont élevées à 328 millions de livres sterling en 2008, soit une augmentation de 13 % par rapport à l'année précédente (Royaume-Uni 2010, 5). En 2010, le Comité directeur du vol d'identité du Home Office a établi que l'économie du Royaume-Uni avait perdu au moins 1,2 milliard de livres sterling par vol d'identité et que cette fraude procurait aux criminels quelque 10 millions de livres sterling par jour (Royaume-Uni 2010, 13). Toujours au Royaume-Uni, les pertes en fraudes bancaires en ligne ont augmenté de 185 % de 2007 à 2008 et, au cours de la même période, les incidents d'hameçonnage se sont accrus de 186 %.

À l'évidence, on ne s'est pas donné beaucoup de peine, au Canada, aux États-Unis, en Australie ni au Royaume-Uni, pour apprécier la nature et l'ampleur de la cyberfraude. Non plus a-t-on essayé un tant soit peu d'en comprendre tous les coûts sociaux et économiques, notamment prévisibles.

On n'a pas non plus entrepris une démarche commune pour clarifier la signification de cette expression simple, mais trompeuse, qui couvre une grande diversité de comportements, de caractéristiques chez les victimes, de retards concernant la sensibilisation, la notification et le signalement et, enfin, de coûts liés aux enquêtes. Par ailleurs, les objectifs propres aux différentes collectes de données se sont traduits par une grande diversité dans les stratégies méthodologiques. On comprend sans peine que cela a nui à la connaissance du phénomène.

Les études mentionnées sont les sources publiques et dont la méthodologie est valable concernant l'ampleur de la cyberfraude. Elles comportent leurs limites, même si elles procurent certaines données récentes sur la fraude et nous permettent de dégager certaines conclusions sur la nature de la cyberfraude. Les données de chaque étude ne sont pas recueillies systématiquement tous les ans; à titre d'exemple, tandis que l'Étude conjointe sur les pratiques canadiennes en sécurité TI Rotman-Telus a été menée trois ans d'affilée, soit de 2008 à 2010, l'Enquête sur la fraude contre les entreprises n'a été commandée qu'en 2008. Les enquêtes s'appuient sur des méthodes différentes pour évaluer la fréquence et les coûts de cette fraude, en plus de couvrir divers secteurs d'activité ainsi que des types ou sous-catégories de fraude. Par ailleurs, elles portaient sur diverses organisations, dont le nombre d'employés différait, et non sur l'ensemble de l'économie. Enfin, on a fait peu d'efforts pour documenter l'origine des fraudes, donnée particulièrement importante dans le cas de la cyberfraude souvent commise sans égard aux frontières nationales.

Enfin, nombre de ces sources ont été établies à partir d'enquêtes fondées sur des opinions au sujet de fraudes, qui ne sont pas aussi fiables que des statistiques administratives lorsqu'on souhaite estimer les coûts de ces fraudes. Ainsi, des enquêtes sur les victimes comportent souvent la question : avez-vous été victime de telle ou telle fraude? Or cette question ne tient pas compte du fait que ces divers types de fraude prêtent à confusion et sont complexes, même pour des experts aguerris de la lutte à la fraude, eux-mêmes estimant obscure la signification précise de certains types de conduites étiquetées comme frauduleuses (Levi et Burrows 2008, 304). Pour certains types de fraude, on ne dispose d'aucune donnée, en bonne partie parce qu'elles n'ont pas été étudiées ou parce que les données à leur sujet sont soit inconnues, soit confidentielles; par conséquent, il n'est pas clair si ces fraudes (p. ex. rencontre en ligne ou vol d'identité) sont peu préoccupantes ou totalement sous-estimées. En outre, on a tendance à recueillir des données uniquement sur les pertes par fraude, alors qu'on sait peu de choses sur les pertes prévisibles ou la prévention des pertes.

3.0 Cyberfraude, crime organisé et économie clandestine en ligne

Du point de vue des politiques et de l'application de la loi, il est essentiel de comprendre si les personnes qui commettent des fraudes au Canada le font à l'intérieur ou à l'extérieur des frontières canadiennes (Canada, 2005, 21). L'implication des groupes du crime organisé dans la fraude est un enjeu important, peu importe s'ils essaient simplement d'amasser de l'argent rapidement et facilement ou s'ils utilisent les revenus de la fraude pour financer d'autres activités criminelles. Les discours actuels concernant le lien existant entre les technologies informatiques et le crime organisé comportent encore des rumeurs et des exagérations; toutefois, dans le contexte d'un Internet mondialement envahissant, différents types d'organisations, qu'elles soient légales ou illégales, dépendent de plus en plus d'Internet pour fonctionner et réussir (Grabosky, 2006,

187). Il est évident que le cyberespace constitue, pour différents types de criminels, la zone protégée dont ils ont besoin pour renforcer leurs capacités organisationnelles et opérationnelles.

Aux fins de la présente section, une organisation criminelle est une association ou un groupe d'au moins trois personnes qui consacre la majeure partie de ses efforts à commettre des activités criminelles dans le but premier d'en retirer un avantage matériel (Brenner, 2002, 7). Cette définition est tirée de l'article 467.1 du *Code criminel* du Canada, qui définit une organisation criminelle comme suit :

> Groupe, quel qu'en soit le mode d'organisation *a*) composé d'au moins trois personnes se trouvant au Canada ou à l'étranger et *b*) dont un des objets principaux ou une des activités principales est de commettre ou de faciliter une ou plusieurs infractions graves qui, si elles étaient commises, pourraient lui procurer — ou procurer à une personne qui en fait partie — , directement ou indirectement, un avantage matériel, notamment financier.

Les organisations criminelles ont des structures variées et doivent être définies au sein d'un continuum (Morselli, 2010). À une extrémité, on retrouve les groupes du crime organisé traditionnels, comme la mafia italo-américaine, qui est formée de structures organisationnelles complexes et qui mise sur une division du travail hiérarchique ainsi que sur des liens familiaux ou ethniques étroits. Ces groupes ont tendance à se concentrer sur les activités locales, comme le trafic de stupéfiants, le blanchiment d'argent, le prêt usuraire, les jeux de hasard illicites et la prostitution (Brenner, 2002, 7). À l'autre extrémité, il existe bon nombre d'exemples de réseaux criminels structurés de façon plus souple et comprenant de nombreux petits réseaux composés de multiples intervenants (Morselli, 2010). Il n'y a aucune incongruité entre les réseaux criminels à court terme, dont les liens et les affiliations sont changeants, et les organisations criminelles plus formelles. En effet, les deux types de structures organisationnelles existent depuis longtemps et sont parfois interconnectés (Morselli, 2010, 16).

De nouveaux réseaux criminels à l'échelle mondiale ont pris forme dans le cyberespace : ils sont relativement petits, divers sur le plan ethnique et culturel, structurés de façon souple, transitoires et axés sur un objectif précis (Brenner, 2002, 45). Ils exercent habituellement leurs activités en partenariat avec des criminels indépendants (p. ex. développeurs, négociants ou courtiers) (Morselli, et coll., 2002, 22), principalement en raison de la structure unique d'Internet, soit un réseau formé de réseaux, qui est diversifié, fluide et hautement génératif (Brenner, 2002, 39). Les réseaux criminels en ligne ont tendance à se caractériser par la collaboration et sont peu organisés. Par exemple, les petits groupes informels de pirates informatiques, comme cnxhacker et milw0rm, sont structurés comme une cybergang et exécutent habituellement leurs activités de façon latérale (Brenner, 2002, 26).

Bon nombre de ces groupes se sont adaptés aux changements technologiques et ont utilisé les technologies informatiques pour faciliter leurs activités criminelles hors ligne, comme le trafic de stupéfiants et le blanchiment d'argent. Les enchères en ligne fournissent un moyen de faire circuler de l'argent dans le cadre d'achats qui semblent légitimes. Comme la monnaie virtuelle et les banques électroniques deviennent choses courantes, le nombre d'occasions de cacher le trafic de produits de la criminalité dans des types de transactions illégales de plus en plus vastes risque d'augmenter. Dans d'autres cas, les criminels organisés utilisent Internet pour élaborer de

nouveaux crimes et pour accroître la perpétration de crimes traditionnels[11]. Parmi les exemples de groupes traditionnels du crime organisé exécutant des activités adaptées aux technologies, mentionnons les triades asiatiques et les yakuzas japonais, dont les activités criminelles vont du piratage informatique à la fraude par carte de crédit (Choo, 2008, 273).

Les groupes criminels ont été capables de se concentrer sur la publication des vulnérabilités des logiciels ainsi que l'élaboration de programmes malveillants et de nouvelles techniques de piratage sophistiquées (Choo, 2008, 277). Ils ont également réussi à accroître leurs attaques de façon exponentielle en utilisant davantage l'automatisation et en fournissant un accès étendu à leurs programmes malveillants (UNDOC, 2010, 204). Des millions de pourriels peuvent être envoyés dans une courte période et des outils logiciels personnalisés permettent désormais aux attaquants néophytes de cibler des milliers de victimes possibles en quelques heures à peine (UNDOC, 2010, 204).

En outre, la capacité à avoir accès à une foule de produits, de services et de renseignements provenant d'autres personnes dans le monde permet aux délinquants de combiner leurs efforts en vue de perpétrer des attaques hautement sophistiquées beaucoup plus complexes que la victimisation d'une seule personne ou entité (UNDOC, 2010, 28). Les réseaux criminels virtuels sont souvent rattachés à un lieu de réunion en ligne, que ce soit un forum sur le Web ou un canal IRC (Royaume-Uni, 2010, 11). Le canal IRC est un protocole de communications constitué d'un certain nombre de fonctions intéressantes : il permet des communications de groupe en temps réel, est constamment ouvert, requiert peu de largeur de bande et est disponible gratuitement dans tous les systèmes d'exploitation (Symantec, 2008, 5). Comparativement aux forums sur le Web, qui ont une présence indiscrète, les canaux IRC passent habituellement inaperçus et sont de nature beaucoup plus transitoire (Symantec, 2008, 9).

Il existe également un certain nombre de vastes forums modérés sur le Web qui permettent aux délinquants d'acheter et de vendre des renseignements et des produits, d'échanger des conseils, des techniques et des nouvelles après la perpétration de cybercrimes ou simplement de discuter (Howard, 2009, 28). Ces forums ont habituellement une durée de vie plutôt courte compte tenu du risque d'être découverts par les organismes d'application de la loi (Howard, 2009, 28). Même s'il est juste de les considérer comme des affiliations de participants structurées de façon souple, ces groupes présentent un certain niveau de collaboration et d'organisation (Symantec, 2008, 8). Les forums ont des niveaux d'adhésion différents : certains permettent à leurs membres de publier des annonces et d'interagir avec les autres dès le début, alors que d'autres procèdent à un examen par les pairs pour déterminer les vendeurs possibles et restreignent les privilèges des membres jusqu'à ce que certains critères soient respectés (Symantec, 2008, 4).

---

[11] Par exemple, Morselli et ses collaborateurs renvoient à une étude menée par Icduygu et Tokas (2002) qui porte sur la traite de personnes au Moyen-Orient et en Turquie. Les auteurs ont découvert que les trafiquants avaient habituellement accès aux plus récentes technologies de communications, y compris les téléphones cellulaires. C'est pour cette raison qu'ils ont réussi à exécuter leurs activités de traite de façon plus efficace en courant moins de risques d'être découverts ou appréhendés.

Ce processus est compréhensible compte tenu de l'importance de la confidentialité de toute activité criminelle organisée, et l'Internet fournit une grande possibilité de dissimulation aux personnes qui l'utilisent. Aux prises avec une perpétuelle menace d'être découverts ou appréhendés, beaucoup de participants des organisations criminelles essaient de réduire les risques d'être découverts par les services de police ou d'être trahis par leurs complices en tentant d'établir la confiance et la solidarité entre les participants du groupe (Morselli, 2011, 26). Dans le cas de nombreux réseaux criminels en ligne, les membres ne se rencontrent que très rarement en personne et les individus ne sont souvent connus que par leur pseudonyme ou leur surnom informatique (Morselli, 2011, 26). Les membres peuvent au besoin communiquer avec d'autres personnes qui ont les compétences techniques requises en masquant leur identité afin de réduire de façon significative le risque d'être découverts. Bon nombre de forums sur le Web assurent leur propre surveillance et disposent de mesures de protection, comme des mesures permettant de se débarrasser des utilisateurs déloyaux (p. ex. les escrocs qui exploitent d'autres criminels) (Morselli, 2011, 26).

Beaucoup de groupes criminels en ligne ont également un port d'attache dans un pays où il y a peu de lois contre la cybercriminalité, voire aucune. Cette méthode fournit une protection supplémentaire contre les organismes d'application de la loi et permet aux groupes criminels d'exécuter leurs activités en courant moins de risques. En Russie, par exemple, le manque de possibilités économiques et d'occasions d'emploi a forcé de nombreuses personnes hautement éduquées ayant de fortes compétences en programmation informatique et des aptitudes techniques à travailler dans le monde cybernétique illicite (Choo, 2008, 275). Le groupe Shadowcrew, qui disposait d'un certain nombre d'administrateurs et de personnes-ressources en Russie, était un réseau international de vol d'identité qui offrait un forum en ligne afin d'échanger de l'information sur le vol, le commerce et la vente de renseignements personnels pouvant être utilisés pour commettre de la fraude. Il s'agit de l'un des premiers groupes à avoir acquis une notoriété en tant que forum actif sur le Web dans le domaine de la fraude en ligne (Symantec, 2008, 9). Le groupe a apparemment été impliqué dans le trafic de plus de 1,7 million de cartes de crédit en ligne (Choo, 2008, 277).

Le groupe Shadowcrew pratiquait une forme de crime organisé spécial : les membres de ce groupe travaillaient à distance sans jamais avoir à se rencontrer et ils se réunissaient pour des raisons particulières (Menn, 2010, 173). Certains membres du groupe étaient responsables du fonctionnement de forums sur le site Web qui portaient sur les stratégies liées au vol d'identité, au pollupostage et à la falsification de documents, entre autres (Symantec, 2008, 9). Ces forums ont attiré bon nombre de nouveaux participants ayant des niveaux de compétences variés et ont permis aux néophytes d'entrer dans le commerce grâce à l'économie clandestine (Symantec, 2008, 9). D'autres membres misaient sur le piratage de systèmes de caisses enregistreuses de diverses entreprises pour évaluer si les numéros des cartes de crédit volées seraient acceptés et pour classer les documents d'identification personnelle, qui seraient par la suite vendus au moyen des forums ou d'un site d'enchères en ligne. D'autres devaient vendre les renseignements volés ainsi que l'argent blanchi et, finalement, certains membres étaient chargés de recueillir les numéros de carte de crédit et de fournir des instructions sur la façon d'obtenir et de falsifier des documents (Zambo, 2007, 557). Cette réalité décrit bien le fait qu'une grande quantité de réseaux modernes de la cybercriminalité s'organisent (Wall, 2009, 55). Les stratagèmes frauduleux comme celui du groupe Shadowcrew soulignent la nature transnationale des crimes cybernétiques et la capacité

des individus à se réunir en ligne pour fournir des services spécialisés et du matériel visant à exécuter des activités illicites (Symantec, 2008, 12).

Il n'y avait pas moins de 4 000 membres inscrits au groupe Shadowcrew provenant du monde entier et dont les activités s'organisaient autour d'un seul site Web (www.shadowcrew.com) dans le but de vendre des cartes de crédit entre août 2002 et octobre 2004 (Hilley, 2006, 10). Le groupe a fait très peu d'efforts pour cacher son objectif illégal. Le site était ouvert au public aux fins d'inscription et pouvait être consulté par quiconque le voulait. Il était donc facile pour les organismes d'application de la loi de surveiller les activités du groupe (Symantec, 2008, 9). Les membres utilisaient des techniques de piratage et d'hameçonnage pour recueillir des numéros de carte de crédit devant être utilisés pour acheter des biens qui étaient ensuite envoyés à une adresse précise prévue à cette fin (Hilley, 2006, 10). Les membres ont aussi volé des passeports, des numéros de comptes bancaires et des numéros de sécurité sociale aux États-Unis. On estime que les pertes causées par leurs crimes s'élèvent à plus de 4 millions de dollars américains (Hilley, 2006, 10). En 2005, le groupe a été démantelé dans le cadre de l'opération FIREWALL, une opération d'infiltration de 18 mois menée par des organismes d'application de la loi américains et internationaux (Hilley, 2006, 10)[12].

Le Russian Business Network (RBN), une organisation criminelle d'origine russe, a aussi été considéré par VeriSign comme un fournisseur de services de sites d'hameçonnage et de dépôts de programmes malveillants au cours des dernières années (Choo, 2008, 280). Il est reconnu comme responsable d'environ la moitié des incidents d'hameçonnage survenus en 2006 à l'échelle mondiale et d'avoir hébergé des sites Web responsables d'une quantité importante de crimes informatiques perpétrés à l'échelle planétaire (Symantec, 2008, 9). Le RBN était un fournisseur d'accès Internet (FAI) situé à St. Petersburg qui n'hébergeait que des éléments illégaux et malveillants, notamment des sites Web frauduleux et des programmes malveillants (Menn, 2010, 171). Par exemple, Rock Group, une organisation spécialisée dans l'hameçonnage, a utilisé son service d'hébergement et a eu un revenu d'environ 150 millions de dollars américains en 2006. En outre, un certain nombre de documents prolifiques remplis de programmes malveillants (p. ex. trousses d'attaques et boîtes à outils) ont été élaborés et distribués au moyen du RBN (Symantec, 2008, 13).

La majeure partie des cibles du RBN étaient des institutions financières, et leurs clients étaient principalement situés à l'extérieur de la Russie. L'absence de cibles russes ainsi que les liens étroits de l'organisation avec le gouvernement de la Russie n'ont pas incité les organismes d'application de la loi locaux à intenter des poursuites contre le RBN, rendant ainsi difficiles les opérations menées par les autorités d'autres gouvernements (Menn, 2010, 171). Le RBN était connecté à d'autres FAI locaux, avec lesquels il partageait des adresses IP, des fournisseurs de services ainsi que des inscriptions et des coordonnées interreliées. De cette manière, le RBN exécutait ses activités impudemment au sein d'un réseau de FAI illicites situés en Russie, ce qui facilitait les interactions entre les délinquants (Menn, 2010, 172). Le RBN n'avait pas de site Web

[12] Veuillez prendre note que deux autres forums consacrés à la fraude en ligne, Carderplanet et Darkprofits, ont également été démantelés dans le cadre de l'opération FIREWALL.

à lui seul et ne pouvait être consulté que par les personnes ayant des liens avec les individus exploitant le réseau (Symantec, 2008, 14).

En 2007, le RBN a déplacé ses activités de la Russie à des FAI disposant d'un protocole IP s'étendant jusqu'en Chine et à Taïwan (Menn, 2010). Au même moment, par contre, l'augmentation de la surveillance minutieuse des médias, des organismes d'application de la loi et de l'industrie de la sécurité concernant la quantité d'activités criminelles facilitées par le RBN a entraîné la suppression de certains domaines contrôlés par ce dernier, et on a du même coup mis un terme à ses activités chinoises et taïwanaises. Ces interruptions n'ont pas mené à des arrestations massives; toutefois, le modèle de réseau à grande échelle consolidé de FAI illicites au sein d'un seul pays a été affaibli (Menn, 2010). Désormais, les fournisseurs de services illicites ont tendance à offrir un ensemble diffus de services loués auprès de FAI légaux de plusieurs pays, diminuant ainsi la possibilité que l'ensemble de leurs activités illicites soient découvertes et suspendues (Menn, 2010).

L'économie clandestine a également évolué et est devenue un marché mondial de plus en plus affiné où des compétences et des données techniques peuvent être achetées pour lancer des attaques précises. Symantec rapporte que les trousses de programmes facilement disponibles (ou trousses de logiciels criminels), qui sont largement accessibles pour la vente dans l'économie clandestine, facilitent le travail des novices qui désirent compromettre des systèmes informatiques et voler des renseignements (Symantec, 2010, 11).

Une trousse de logiciels criminels est une boîte à outils permettant à une personne d'acheter un programme malveillant conçu pour voler des données et d'autres renseignements personnels (Symantec, 2010, 11). L'efficacité de ces trousses en tant que moyen de lancer des cyberattaques a été démontrée en 2009 lorsque les cinq principales trousses d'hameçonnage surveillées par Symantec ont été responsables d'une moyenne combinée de 23 % de toutes les tentatives d'hameçonnage observées au cours de l'année (Symantec, 2010, 18). La diminution des obstacles auxquels font face les néophytes qui désirent entrer dans le domaine de la cybercriminalité se traduit par l'augmentation des menaces posées par des programmes malveillants qui utilisent un accès à distance pour voler des renseignements confidentiels (Symantec, 2010, 18). Par exemple, le très connu botnet Mariposa (« botnet », ou « réseau de zombies », est un terme habituellement associé à un logiciel malveillant), qui a infecté plus de 15 millions d'ordinateurs à l'échelle mondiale, a été lancé par des attaquants aux compétences informatiques limitées qui ont téléchargé le programme sur pour moins de mille dollars [Deloitte, 2010(b)]. Cela signifie que l'économie clandestine en ligne a prospéré, alors que l'économie dominante a à peine commencé à se rétablir de la crise financière mondiale (Symantec, 2010, 15).

Les renseignements portant sur les cartes de crédit, qui sont habituellement vendus en vrac, étaient l'élément le plus souvent annoncé pour être vendu sur les serveurs de l'économie clandestine connus de Symantec en 2009; les numéros de carte de crédit étaient vendus entre 0,85 et 30 dollars américains chacun (Symantec, 2010, 18). Les États-Unis étaient le pays comptant le plus d'annonces concernant des cartes de crédit sur les serveurs de l'économie clandestine,

totalisant 67 % de toutes les annonces (Symantec, 2010, 18)[13]. De façon générale, les cartes provenant de l'Europe ou de l'Asie sont plus dispendieuses que celles des États-Unis ou du Canada (Panda, 2010, 18). Les détails provenant de cartes émises aux États-Unis peuvent coûter aussi peu que 2 dollars américains pour des renseignements de base et jusqu'à 40 dollars américains pour des renseignements complets portant sur des cartes Or, Platine et Entreprise (Panda, 2010, 18).

Les renseignements portant sur des cartes de crédit volées doivent toutefois être transformés en argent comptant, et les criminels cherchent constamment des moyens novateurs d'y parvenir (Panda, 2010, 7). Le processus selon lequel les justificatifs d'identité volés sont convertis en devises valides ou en marchandises est connu sous le nom de « décaissement » (Menn, 2010, 25). Les cybercriminels utilisent habituellement des complices involontaires ou des mules pour les aider dans le cadre du processus de décaissement. Le terme « mule » provient du mode de transport que les passeurs utilisaient pour la contrebande de biens illégaux; aujourd'hui, il décrit les personnes recrutées au moyen d'Internet pour servir d'intermédiaires dans le cadre du transfert de fonds illégalement obtenus grâce à l'hameçonnage, aux enregistreurs de frappe et aux autres escroqueries en ligne (Paget, 2009, 10). La mule donne son numéro de compte bancaire aux criminels, qui l'utilisent ensuite pour recevoir les fonds dérobés ou les biens achetés qui seront revendus (Menn, 2010, 35). Généralement, les mules reçoivent les dépôts directs dans leur compte personnel au sein du même pays où la victime a été volée et elles retirent l'argent et effectuent un virement télégraphique outre-mer dans un compte spécifié par le criminel (la mule reçoit un certain pourcentage du virement ou un salaire de base).

Pour recruter des mules, les délinquants affichent de fausses offres d'emploi dont la rémunération est élevée, souvent en les envoyant sous forme de pourriels ou en les publiant sur des sites de recherche d'emploi légaux comme Monster.com (Menn, 2010, 35). Pour chacune des transactions effectuées, la mule obtient un pourcentage du montant concerné en transférant le solde au moyen d'un service de virement de fonds anonyme (un service de virement télégraphique comme Western Union, par exemple). Les mules sont souvent des personnes qui cherchent à amasser de l'argent rapidement; ce type d'emploi est devenu populaire dans la vague de la récession financière mondiale. Les mules peuvent elles aussi devenir des victimes; elles ne savent souvent pas ce qu'elles font et perçoivent la transaction comme une manière de récolter rapidement de l'argent (Panda, 2010, 13).

Le réseautage social et les communications en ligne constantes, ainsi que l'abondance des appareils de communication, des réseaux et des utilisateurs, ont également apporté de nouveaux risques et possibilités d'activités illégales. L'arrivée des sites de réseautage social comme Facebook et Twitter donne un accès accru à une foule de renseignements utiles et de cibles possibles. Comme les utilisateurs affichent toutes sortes de renseignements, comme où ils vivent et ce qu'ils font à un moment précis, il est plus facile pour les étrangers d'avoir accès à des renseignements personnels grâce à l'ingénierie sociale : l'art de tromper ou de manipuler les personnes afin qu'elles divulguent des renseignements personnels qu'elles ne donneraient habituellement pas aux inconnus. Par exemple, une personne peut afficher un message à propos

[13] La situation n'a pas changé depuis 2008.

d'un sujet intéressant semblant provenir d'un « ami » de confiance, mais lié à un site Web dangereux visant à voler les données de sa carte de crédit et d'autres renseignements précieux (Panda, 2010, 6).

Les délinquants peuvent passer inaperçus en soutirant de petites sommes d'argent à un grand nombre de victimes. Le professeur David Wall a utilisé le terme « micro-fraude » pour décrire le phénomène de victimisation électronique à l'échelle mondiale par lequel les criminels, organisés en réseau, cherchent à recueillir de l'information. Ce phénomène tend à avoir une faible incidence de façon individuelle, mais une incidence globale importante (Wall, 2010(a), 69). Les fraudes de ce genre sont habituellement trop petites pour être prises en considération, et les victimes (notamment les banques) ne mettent souvent qu'une croix sur cet argent, ou la fraude ne porte pas sur un montant assez élevé pour que les services de police procèdent à une enquête. Wall signale que les services de police sont hésitants à l'idée de mobiliser des ressources d'enquête dans des cas où les pertes sont inférieures à 5 000 ou 7 000 dollars américains et que les banques acceptent habituellement d'annuler les pertes de moins de 1 500 dollars américains. Cette réalité est d'une grande importance, car la plupart des micro-fraudes engendrent des pertes moyennes de moins de 2 000 dollars américains par victime (Wall, 2010(a), 80)[14]. Dans le même ordre d'idées, l'Enquête de 2008 sur la fraude contre les entreprises au Canada a rapporté que la grande majorité des points de vente au détail (89 %) et des banques (91 %) qui ont été victimes de fraude au cours des douze derniers mois ont signalé qu'ils faisaient face à des pertes cumulatives de 20 000 dollars canadiens ou moins en raison de fraudes commises directement contre eux (Taylor-Butts et Perreault 2008, 16).

Comme le mentionne Wall, ces fraudes ont tendance à être commises en grand nombre, mais presque de façon invisible (Wall, 2010(a), 80). Même si les médias surestiment souvent le problème de la cyberfraude, la non-déclaration des cas par les victimes représente également une difficulté (Wall, 2010(a), 80). Il arrive fréquemment que les victimes ne constatent tout simplement pas les incidents survenus ou qu'elles ne les signalent pas par pur embarras, ou bien que les incidents soient signalés directement à la banque, ne faisant donc pas partie des statistiques officielles de la criminalité (Wall, 2010(a), 80). Cela signifie que les profils du délinquant et de la victime sont faibles, parce que très peu de micro-fraudes sont signalées. En outre, il y a un problème lié au fait que bon nombre de micro-fraudes sont commises dans plusieurs pays à la fois, ce qui complexifie la tâche des services de police de cerner le problème et d'y remédier. Dans la plupart des cas, les micro-fraudes ont une incidence trop minime pour justifier les dépenses liées aux ressources policières, même à l'échelle locale (Wall, 2010(a), 80). La façon la plus efficace pour contrer les micro-fraudes repose sans doute dans une solution à la fois technologique et éducative; il faudrait notamment veiller à ce que les utilisateurs d'ordinateurs personnels sécurisent davantage leur système et se tiennent à l'affût des manœuvres frauduleuses. Toutefois, comme le signale Wall :

[14] Les pertes moyennes sont signalées comme suit : marchandise ou paiement non livré (800 $), fraude dans le cadre d'enchères sur (610 $), fraude par carte de crédit ou de débit (223 $), lettre frauduleuse typique du Nigéria (1 650 $) et vol d'identité (1 000 $). Ces chiffres, cités par Wall, sont fondés sur 275 285 plaintes reçues et 72 490 cas signalés par l' Crime Complaint Centre (centre de plaintes contre la cybercriminalité) en 2008 (Source : IC3, 2009).

> [TRADUCTION] Jusqu'à maintenant, l'un des problèmes majeurs liés au contrôle des micro-fraudes causées par des épouvantiels, par exemple, est l'absence d'un système de signalement efficace, uniforme et facile à utiliser. Cette réalité s'est longtemps traduite par la perte du renseignement stratégique essentiel qui permet d'obtenir une meilleure vue d'ensemble des répercussions à l'échelle nationale, tout comme le renseignement criminel tactique important lié aux délinquants, ce qui nuit à la capacité des policiers de procéder à des enquêtes (Wall, 2009, 64).

Il est important que les groupes de la cybercriminalité organisée soient décentralisés et ne fournissent pas une seule cible ou un seul point de défaillance pour les organismes d'application de la loi, principalement parce qu'ils dépendent de criminels multiples provenant de divers pays, plus particulièrement de milieux non règlementés (Etges et Sutcliffe, 2008, 91). La nature globale de ces organisations et le fait qu'elles changent constamment de lieu géographique complexifient la tâche des autorités de trouver les auteurs et de mettre un terme à leurs activités (Symantec, 2009, 56). L'Internet fournit également davantage de confidentialité que n'importe quel autre milieu physique réel. La structure non hiérarchisée fondée sur l'organisation en réseau convient parfaitement aux criminels de l'ère numérique en ce qui a trait à la coordination et à la collaboration. La preuve en est le nombre d'ordinateurs utilisés pour perpétrer des crimes à distance (p. ex. les bots)[15]. L'économie clandestine en ligne fournit également des occasions à l'échelle mondiale d'effectuer de l'exportation sous forme immatérielle (p. ex. programmes malveillants et renseignements volés relatifs à l'identité) et de se spécialiser dans les produits et services individuels (p. ex. vecteur d'attaque [applications et réseaux], dissimulation de données, fraude financière, vol d'identité et fraude par carte de crédit) (Etges et Sutcliffe, 2008, 92). Pour lutter contre ces structures sophistiquées qui sont organisées en réseau et qui exécutent leurs activités sur Internet, les gouvernements doivent former des coalitions entre les organismes d'application de la loi, les organismes gouvernementaux, les organisations du secteur privé, les organisations non gouvernementales (ONG) et les organisations professionnelles de tous les pays concernés (Etges et Sutcliffe 2008, 93). La lutte contre la cyberfraude constitue l'exemple parfait où le renseignement financier et l'interaction entre les secteurs privé et public sont essentiels (Gottschalk, 2010, 268).

4.0 Lois canadiennes et étrangères en matière de cyberfraude

4.1 Cadre législatif du Canada

Les autorités juridiques doivent composer avec plusieurs défis, notamment la difficulté d'appliquer les lois en vigueur contre les activités criminelles perpétrées au moyen des nouvelles technologies. Pour promulguer des lois à cet égard, il faut tenir compte du fait qu'il est complexe de protéger les consommateurs tout en favorisant la croissance du commerce électronique sans imposer des restrictions indues sur le transfert transfrontalier des données. (Davis, 2003, 208).

[15] Les bots sont des ordinateurs qui ont volontairement été infectés par un virus et qui permettent aux criminels de contrôler certaines fonctions à distance à l'insu de leur propriétaire. Ces ordinateurs peuvent être utilisés pour lancer des attaques coordonnées ou pour diffuser des pourriels dans le but de perpétrer des manœuvres frauduleuses.

Une disposition contre la fraude (article 380) a longtemps été intégrée au *Code criminel*, mais le *Code* ne précisait aucune infraction relative au vol d'identité avant l'entrée en vigueur de la nouvelle législation relative au vol d'identité (dont il sera question ci-après). À l'exception des infractions portant sur les ordinateurs (article 342.1) et les dispositifs permettant d'obtenir des services d'ordinateur (342.2), les infractions précisées dans le *Code* relatives à la propriété et au vol ont été établies avant l'arrivée de l'informatique et d'Internet[16]. Une autre infraction du *Code* traite par ailleurs de méfaits concernant des données (article 430). Toutefois, cette disposition n'a jamais été utilisée au Canada afin de poursuivre un individu qui a commis une fraude ou procédé à un vol d'identité.

Le projet de loi S-4, *Loi modifiant le Code criminel (vol d'identité et inconduites connexes)* a reçu la sanction royale le 22 octobre 2009, ce qui a permis l'ajout de plusieurs infractions au *Code criminel* ciblant les aspects du vol d'identité qui n'étaient pas déjà inscrits dans la loi. Il faut noter qu'il n'existait aucune infraction relative au vol d'identité auparavant. Plus précisément, le projet de loi était axé sur les étapes réalisées en prévision du vol d'identité en rendant illégal l'obtention, la possession, le transfert ou la vente de pièces d'identité qui concernent une autre personne. Voici les principales dispositions de ce projet de loi :

- **Article 1 :** ajout des paragraphes 56.1(1) à (4) au *Code* – fabriquer, posséder, transmettre ou vendre une pièce d'identité qui concerne une autre personne.
- **Articles 4 et 5** : ajout des paragraphes 342(3) et 342.01(1) au *Code* – posséder ou utiliser, de façon frauduleuse, des données relatives à une carte de crédit ou en faire le trafic, et posséder, importer ou exporter sciemment un appareil permettant de copier des données relatives à une carte de crédit.
- **Article 8 :** Ajout des alinéas 368(1)*c*) et *d*) au *Code* – employer un document contrefait comme s'il était authentique, faire le trafic de documents contrefaits et posséder un document contrefait dans l'intention de l'utiliser.
- **Article 9** – Ajout de l'article 368.1 au *Code* – faire le trafic d'appareils permettant de fabriquer un faux document.
- **Article 10** – Ajout à l'infraction existante du fait de se faire passer pour une autre personne pour éviter une arrestation ou une poursuite ou entraver le cours de la justice. Définition de l'expression « supposition de personne », soit le fait de prétendre être celle-ci ou utiliser tout renseignement identificateur ayant trait à une autre personne. Pour qu'une personne soit reconnue coupable de vol d'identité, le poursuivant doit commencer par prouver qu'elle a, en toute connaissance de cause, obtenu ou possédé des « renseignements identificateurs » sur une autre personne. Le projet de loi définit un « renseignement identificateur » comme « tout renseignement – y compris un renseignement biologique ou physiologique – d'un type qui est ordinaire utilisé, seul ou avec d'autres renseignements, pour identifier une personne physique ». Le nouvel article 402.1 du *Code* fournit des exemples de « renseignement identificateur ». L'article 10 ajoute également le paragraphe 402.2(2) au *Code* – transmission, mise à la

[16] Cependant, en vertu de l'article 342.1 du *Code*, l'utilisation non autorisée d'un ordinateur et l'interception de communications informatiques constituent des actes criminels pouvant entraîner une peine d'emprisonnement de 10 ans.

disposition, distribution, vente, offre de vente et possession de « renseignements identificateurs » concernant une autre personne – et modifie l'article 403 en remplaçant « supposition intentionnelle de personne » par « fraude à l'identité ».

Plusieurs dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) peuvent contribuer à réduire de façon importante le risque de vol d'identité et de fraude à l'identité en limitant la collecte, l'utilisation et la divulgation de renseignements personnels. En vertu de la LPRPDE, les organisations qui participent à des activités commerciales doivent adopter des mesures pour protéger les renseignements personnels qu'elles recueillent[17]. Les organisations des secteurs public et privé commencent également à établir des politiques de lutte contre la fraude qui limitent les risques associés à la pénétration généralisée d'Internet au Canada. Toutefois, il faut davantage uniformiser ces initiatives pour régler le problème de la fraude Internet transfrontalière.

4.2 Cadre législatif des États-Unis

Aux États-Unis, la réglementation du commerce électronique, y compris les activités frauduleuses dont il est question dans le présent document, relève généralement de la Federal Trade Commission (FTC) et, à un degré moindre, du département de la Justice (DOJ), qui peut mener des poursuites criminelles et tenter d'obtenir des mesures injonctives civiles en vertu de l'article 1345 du titre 18 du United States Code. (Cukier et Levin, 2009, 262). La Constitution américaine permet au Congrès de superviser le commerce entre les États, notamment le commerce électronique (pourriels, hameçonnage et autres activités frauduleuses perpétrées sur Internet). Plusieurs dispositions du *Uniform Commercial Code* traitent de la fraude sur Internet, y compris : l'*Access Device Fraud* (article 1029 du chapitre 18 du U.S.C.) (fraudes et activités connexes relatives aux appareils permettant un accès), la *Computer Fraud and Abuse Act* (article 1030 du chapitre 18 du U.S.C.) (fraudes et activités relatives aux ordinateurs), la *CAN-SPAM Act* (article 1037 du chapitre 18 du U.S.C.) (fraudes et activités connexes relatives aux courriels), la fraude par carte de crédit (article 1644 du chapitre 15 du U.S.C.) et l'*Identity Theft Assumption Deterrence Act* (article 1028 du chapitre 18 du U.S.C.) (fraudes et activités connexes relatives aux pièces d'identité, aux renseignements identificateurs et à l'information).

[17] La LPRPDE exige des organisations qu'elles respectent dix principes énoncés dans le Code type (annexe 1), notamment la limite de la collecte (les parties doivent restreindre la façon dont elles recueillent l'information. De plus, le client doit être au courant qu'on recueille ses renseignements personnels et l'accepter), la qualité des données (qui doivent être précises et pertinentes), la justification des motifs (le parti doit préciser les fins de la collecte des renseignements), la limitation de l'utilisation (l'information recueillie dans un objectif particulier ne peut être utilisée à d'autres fins, sauf si la personne y consent ou que la loi le permet), des mesures de sécurité (les renseignements doivent être protégés, notamment contre les attaques de pirates), la transparence (la personne doit savoir ce qu'il advient de ses renseignements), l'accès au renseignement (la personne doit pouvoir avoir accès à son information, la réviser et y corriger les erreurs) et la responsabilité (un mécanisme de surveillance doit être en place). Il faut également noter que la LPRPDE impose des limites relatives à la durée pendant laquelle une organisation peut conserver des renseignements personnels. C'est-à-dire que même si des renseignements personnels sont recueillis avec l'accord d'un individu, ils ne peuvent être conservés à perpétuité, ce qui contribue à réduire le risque de vol d'identité en précisant clairement que les organisations doivent détruire l'information dont elles n'ont plus besoin.

En outre, la *Fair Credit Reporting Act* (article 1681 du chapitre 15 du U.S.C.) a été modifiée en 2003 par la *Fair and Accurate Credit Transactions Act*, dont certains articles s'attaquent expressément à la lutte contre le vol d'identité. Par exemple, cette loi exige des entreprises de cartes de crédit qu'elles corrigent les sommes erronées dans les quatre jours suivant la réception d'un rapport de police. En outre, elles doivent prendre des mesures supplémentaires pour vérifier l'identité d'un demandeur lorsque le dossier d'un consommateur est marqué d'une alerte à la fraude (White et Fisher, 2008, 5). La *Gramm-Leach-Bliley Act* (1999) contient un article qui traite de l'accès frauduleux à des renseignements financiers et exige des institutions financières (comme les banques et les sociétés d'investissement) qu'elles se dotent de politiques, de procédures et de contrôles visant à prévenir la divulgation non autorisée d'information financière sur les consommateurs (White et Fisher, 2008, 5). Finalement, le Congrès a créé la FTC au moyen de la *Federal Trade Commission Act*. La FTC tire ses pouvoirs de cette loi et des lois subséquentes, qui lui permettent de réglementer divers aspects du commerce électronique, de donner des ordres, d'infliger des amendes et de commencer des procédures contre des individus et des sociétés (Cukier et Levin, 2009, 262). La FTC peut également, en interdisant de façon générale les activités abusives et trompeuses, forcer les entreprises à appliquer les politiques sociales si elles ne respectent pas leurs propres politiques, malgré l'absence de lois pertinentes à cet égard.

4.3 Cadres législatifs de la Grande-Bretagne et de l'Australie

En Grande-Bretagne, la *Fraud Act* (2006) est entrée en vigueur le 15 janvier 2007 et intègre la fraude par déclaration mensongère, l'interdiction de divulguer de l'information au détriment d'une autre personne et l'abus de pouvoir en vue de réaliser des gains malhonnêtes. En Australie, le comité d'établissement d'un Code criminel modèle du Comité permanent des procureurs généraux, composé d'agents haut placés de toutes les administrations, a mis sur pied un projet en 1990. Le Commonwealth a inscrit les principes de responsabilité établis du Code criminel modèle dans le chapitre 2 de la *Criminal Code Act 1995*. Des modifications ultérieures ont par ailleurs permis l'ajout de dispositions notables portant notamment sur le vol, la fraude et d'autres infractions liées à la propriété, au faux-monnayage, à la corruption et aux infractions contre les représentants du Commonwealth. La *Cybercrime Act 2001* est entrée en vigueur en octobre 2001 et a permis l'ajout de dispositions à la *Criminal Code Act 1995*, à la *Crimes Act 1914* et à la *Customs Act 1901*. La *Cybercrime Act* a contribué à moderniser les infractions informatiques au sein du Commonwealth et a servi d'exemple pour d'autres États et les territoires (Urbas et Choo, 2008, 20)[18]. La *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004* a ajouté la partie 10.8, sur les infractions relatives à l'information financière, à la *Criminal Code Act 1995*. Elle contient des infractions concernant l'utilisation malhonnête d'information financière ou l'emploi d'appareils (comme des copieurs de carte) pour obtenir de l'information sans consentement (Urbas et Choo, 2008, 20). En vertu de la *Spam Act* (2003), il est interdit d'envoyer en masse des courriels non sollicités en Australie et à des destinataires australiens, sous peine de sanctions civiles, comme des amendes importantes (Urbas et Choo, 2008, 20).

[18] En effet, par la suite, plusieurs États et territoires se sont inspirés de ce modèle (de législation en matière de cybercriminalité).

5.0 Questions de compétence concernant les enquêtes sur la cyberfraude et la poursuite en justice de ses auteurs

Un certain nombre des questions importantes en matière de compétence découlent de la nature transfrontalière de la cybercriminalité. Une capacité limitée d'application de la loi pour intervenir dans un contexte de mondialisation croissante, d'évolution rapide des technologies et de tensions issues de conflits entre souverainetés nationales ainsi que l'importance de la coopération internationale (Gabrosky, 2006, 275) ne sont qu'un aperçu de ces questions. La liste ci-dessous présente un résumé des principales questions de compétence attribuables à la complexité de la cyberfraude :

- compétence (existence d'une compétence et problème de compétences concurrentes);
- difficultés législatives associées aux différents systèmes de justice pénale (nécessité d'une double incrimination);
- gestion des alliances et des partenariats stratégiques, respect de la confidentialité et de la souplesse des interventions (particulièrement avec le secteur privé);
- gestion de différents régimes liés à la protection des renseignements personnels;
- mise au point d'une entraide et d'une communication du renseignement stratégique en temps opportun;
- nécessité d'obtenir la collaboration et l'aide des fournisseurs d'accès Internet (FAI);
- nécessité d'interroger des banques de données informatiques et d'intercepter des communications à l'échelle internationale;
- difficultés liées à la gestion et à la coordination des extraditions (Urbas et Choo, 2008, 8).

La nature transnationale de la cybercriminalité remet en question les conceptions traditionnelles de la compétence en matière pénale. En effet, il n'est plus nécessaire que le méfait soit commis entièrement sur le territoire d'une seule souveraineté (Brenner, 2006, 190). Par exemple, en 2000, le virus Love Bug, qui a été lancé à partir des Philippines, a infecté des ordinateurs d'au moins une vingtaine de pays (Brenner, 2006, 190). La personne qui aurait lancé le virus ILOVEYOU n'a jamais été traduite en justice pour le méfait qu'elle a commis, car il n'était pas défini dans les lois des Philippines à ce moment-là, même s'il est punissable dans un certain nombre de pays touchés par le virus (Gabrosky, 2006, 186).

La cybercriminalité peut traverser les frontières, et les activités d'un délinquant donnent souvent lieu à la perpétration d'un crime dans plusieurs pays simultanément. C'est pourquoi il est important d'atteindre les objectifs suivants à l'échelle internationale :

- harmonisation des infractions substantielles commises à l'aide d'un ordinateur dans les lois nationales;
- harmonisation des dispositions de procédure liées aux enquêtes sur les crimes informatiques et la poursuite en juste de leurs auteurs;
- mise en place de mesures de collaboration qui faciliteront la communication d'éléments de preuve et d'information ainsi que l'extradition de suspects (Schjolberg, 2008, 1).

Il est encourageant de constater que des organismes internationaux et des agents de l'application de la loi de partout dans le monde ont pris des mesures pour lutter contre la cybercriminalité. Des intervenants provenant d'organismes d'application de la loi, d'organismes gouvernementaux, d'organisations non gouvernementales et du secteur privé ont formé de nouvelles coalitions pour s'attaquer à la nature transnationale de la cybercriminalité. Le Canada est un membre actif de plusieurs organisations internationales, notamment le Groupe d'experts à haut niveau sur la criminalité transnationale organisée, le Comité d'experts sur la cybercriminalité du Conseil de l'Europe et le groupe d'experts du gouvernement sur la cybercriminalité de l'Organisation des États américains. Le gouvernement du Canada est l'hôte de sommets mondiaux, dirige des études internationales et a contribué à rédiger l'ébauche de la Convention sur la cybercriminalité du Conseil de l'Europe. L'Association canadienne des fournisseurs Internet (ACFI) communique actuellement des éléments d'information à des fournisseurs d'accès Internet européens et travaille de concert avec d'autres pays pour mettre au point des solutions à l'échelle internationale.

Depuis de nombreuses années, Interpol, une organisation internationale d'application de la loi comptant 188 pays membres, occupe un rôle de premier plan dans une intervention internationale organisée visant à lutter contre la fraude en ligne. Le Secrétariat général continue d'offrir une aide spécialisée aux autorités nationales d'application de la loi de ses pays membres grâce à divers services de soutien opérationnels, de bases de données et de formation destinés aux policiers. Interpol est déterminé à nouer des partenariats stratégiques avec d'autres organisations internationales d'application de la loi et du secteur public. À titre d'exemple, la base de données d'Interpol sur les cartes de paiement contrefaites a été créée précisément pour faire la promotion de la coopération internationale. Interpol est régulièrement l'hôte des réunions de son groupe consultatif sur la fraude des cartes de paiement, qui est constitué d'enquêteurs principaux et d'experts en médecine légale d'un grand nombre de ses pays membres, ainsi que de représentants des principales entreprises de cartes de crédit comme Visa, American Express et MasterCard.

Au cours des dernières années, bien des étapes ont été franchies dans la lutte contre la cybercriminalité transnationale. L'une des plus importantes est l'établissement de la Convention sur la cybercriminalité du Conseil de l'Europe. Cette convention, qui vise à harmoniser le droit substantiel et procédural, sert de modèle à de nombreuses nations partout dans le monde. Il s'agit du premier traité multilatéral visant à faciliter la coopération internationale en ce qui concerne la poursuite en justice des auteurs de crimes informatiques. Le traité a été signé à Budapest, le 23 novembre 2001, par les États membres du Conseil de l'Europe ainsi que par plusieurs États non-membres, notamment le Canada, le Japon, l'Afrique du Sud et les États-Unis, qui ont participé à son élaboration (Huey et Rosenberg, 2004, 597). La Convention est entrée en vigueur le 1er juillet 2004. En date du 16 mars 2011, 47 pays avaient signé la Convention.[19]

Parmi ces 47 pays qui ont signé la Convention, 30 pays l'ont ratifiée et l'ont mise en application, dont les États-Unis. Le Canada, quant à lui, n'a pas ratifié la Convention. En vertu de la Convention, chaque pays signataire est tenu d'ériger en infraction le fait de commettre certains

[19] Site officiel des traités du Conseil de l'Europe : http://conventions.coe.int/Treaty/FR/v3DefaultFRE.asp.

crimes au moyen de systèmes informatiques, notamment la fraude et la falsification informatique, les infractions liées à la pornographie juvénile et la violation du droit d'auteur. Les pays signataires sont également tenus de conférer de nouveaux pouvoirs en matière de fouille et de saisie à ses responsables de l'application de la loi, notamment en ce qui concerne la conservation rapide de données informatiques stockées, la fouille et la saisie de données informatiques stockées ainsi que la collecte de données informatiques en temps réel. Conformément à l'article 25 de la Convention, les responsables de l'application de la loi de chaque pays signataire « s'accordent l'entraide la plus large possible ».

Ailleurs dans le monde, des organisations régionales ont commencé à se préoccuper des questions importantes non résolues concernant la cybercriminalité transnationale. À la fin des années 1990, le Sous-groupe sur le crime en haute technologie a mis sur pied un réseau d'experts pour aider en tout temps les intervenants dans leurs enquêtes sur la criminalité technologique pour s'assurer qu'aucun criminel ne trouve refuge dans un pays (Schjolberg 2008, 13). Le G8 a également négocié l'adoption de principes et d'un plan d'action visant à lutter contre la criminalité technologique, ainsi que de pratiques exemplaires, notamment des lignes directrices liées à la sécurité des réseaux informatiques, aux demandes d'assistance internationale, à la rédaction législative et au dépistage des communications électroniques transfrontalières (Urbas et Choo, 2008, 12). De plus, le G8 a collaboré à la préparation de conférences de formation destinées à des organismes de lutte contre la cybercriminalité de chaque continent (à l'exception de l'Antarctique) ainsi que de conférences destinées à des intervenants de l'application de la loi et de l'industrie et traitant de méthodes visant à accroître la coopération et à dépister les communications en ligne de criminels.

L'Organisation de coopération et de développement économiques (OCDE) a, elle aussi, pris des mesures semblables. En 2002, l'OCDE a publié le document *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité*. Ces lignes directrices ont pour objet : de promouvoir parmi l'ensemble des parties prenantes une culture de la sécurité en tant que moyen de protection des systèmes et réseaux d'information; de renforcer la sensibilisation aux risques pour les systèmes et réseaux d'information, aux politiques, pratiques et mesures ainsi qu'à la nécessité de les adopter et de les mettre en œuvre; promouvoir parmi l'ensemble des parties prenantes une plus grande confiance dans les systèmes et réseaux d'information et dans la manière dont ceux-ci sont mis à disposition et utilisés; et créer un cadre général de référence qui aide les parties prenantes à comprendre la nature des problèmes liés à la sécurité et les procédures pour la sécurité des systèmes et réseaux d'information (Urbas et Choo, 2008, 10).

L'Union européenne (UE) a adopté une décision-cadre, qui est entrée en vigueur en 2005. En vertu de cette décision-cadre, les États membres pourront criminaliser l'atteinte à l'intégrité d'un système, l'atteinte à l'intégrité des données et l'accès illicite à des systèmes d'information (Urbas et Choo, 2008, 15). Parallèlement, la Coopération économique Asie-Pacifique (APEC) est déterminée à inciter ses États membres à adopter des lois exhaustives liées à la cybercriminalité ainsi qu'un cadre stratégique qui prévoit des mesures importantes, des procédures et des arrangements en matière d'entraide juridique qui sont conformes aux instruments juridiques internationaux (Urbas and Choo 2008, 16). L'APEC a dirigé un projet sur la cybercriminalité visant à renforcer les capacités législatives et d'enquête de ses États membres. Dans le cadre de ce

projet, les principales forces économiques viennent en aide aux pays moins avancés en finançant la formation des responsables de l'application de la loi (Li, 2007). Des mesures semblables ont également été mises en place par l'Association des Nations de l'Asie du Sud-Est (ANASE) en 2006, et la Ligue des États arabes, ainsi que certains États membres de l'Union Africaine. De plus, en 2008, l'OTAN a ouvert un centre d'excellence sur la cyberdéfense en Estonie afin de mener des recherches sur la guerre électronique. L'Organisation des États américains a aussi pris des mesures pour s'attaquer aux menaces contre la cybersécurité et a exhorté ses États membres à adopter des lois pour lutter contre la cybercriminalité et faciliter la coopération internationale.

Le 11e Congrès des Nations Unies contre le crime, qui s'est tenu en 2005, a porté principalement sur le lien entre le crime organisé et la cybercriminalité. L'Assemblée générale des Nations Unies a adopté un certain nombre de résolutions pour mettre fin à l'utilisation abusive des technologies de l'information. Les Nations Unies ont constitué un Groupe de travail sur la gouvernance de l'Internet, qui a participé au Sommet mondial sur la société de l'information, lequel s'est déroulé en Tunisie en novembre 2005 (Schjolberg, 2008, 10). Le Secrétaire général a lancé en mai 2007 le Programme mondial de cybersécurité, un cadre de dialogue et de coopération international ayant pour objet d'élaborer des stratégies et des solutions qui permettront d'accroître la sécurité de l'information. De plus, l'Union internationale des télécommunications (UIT), à Genève, est devenue l'organisation des Nations Unies qui s'emploie le plus activement à harmoniser les lois internationales sur la cybercriminalité et à trouver des moyens de promouvoir la coopération internationale et de s'appuyer sur les accords internationaux en vigueur sur le sujet, particulièrement la Convention sur la cybercriminalité du Conseil de l'Europe (Schjolberg, 2008, 20).

Le secteur privé a lui aussi pris des mesures pour tenter de renforcer la capacité des responsables de l'application de la loi partout dans le monde de s'attaquer au problème de la cybercriminalité. À titre d'exemple, Microsoft a investi des millions de dollars pour concevoir un programme de formation et des ressources technologiques destinés aux organismes de l'application de la loi à l'échelle internationale afin d'améliorer leur capacité d'enquêter sur les délits assistés par ordinateur perpétrés contre des enfants (Microsoft, 2005). À l'origine, ce projet a été élaboré avec l'aide de plusieurs corps de police étrangers, la GRC et le service de police de Toronto (GRC, 2005). Même s'il a servi principalement à lutter contre la pornographie juvénile en ligne, il peut également faciliter la tenue d'enquête sur d'autres types de délinquants et leur poursuite en justice, comme les auteurs de fraude et de vol d'identité. Ces réussites démontrent que l'on peut remporter la lutte contre la cybercriminalité transnationale.

6.0 Autres questions pour les organismes d'application de la loi et les procureurs

La Gendarmerie royale du Canada (GRC) doit faire enquête sur tout crime informatique commis au Canada. Elle est également chargée d'enquêter sur les crimes informatiques perpétrés contre le gouvernement du Canada, sans égard à l'endroit d'où vient le délinquant, ainsi que sur toute infraction commise par des groupes organisés ou qui touche des intérêts nationaux du Canada. La GRC compte une section des infractions commerciales dans chaque grande ville au Canada. Au moins un enquêteur spécialisé dans le crime informatique travaille dans chacune de ces sections.

Le Groupe judiciaire de la criminalité technologique - GRC, basé à Ottawa, appuie aussi ces opérations, en plus d'offrir son aide et ses compétences à tous les services de police canadiens et à tous les organismes fédéraux en ce qui a trait aux crimes commis contre un système informatique ou à l'aide de celui-ci ainsi qu'aux crimes en matière de télécommunications.
Cependant, comme il est mentionné plus haut, la nature anonyme d'Internet pose un problème important aussi bien aux organismes d'application de la loi qu'aux victimes, car près de la moitié de celles-ci ignorent comment quelqu'un a obtenu leurs renseignements personnels. Souvent, les délinquants masquent leur identité et sont capables de créer des boucles ou de se servir de serveurs situés dans de nombreux territoires pour mener leurs attaques. La personnification électronique, ou mystification, peut aussi aider à cacher l'identité de l'auteur de l'attaque, comme le font les services de courriel anonymes et le chiffrement de l'information électronique. Cela a d'énormes conséquences sur les interventions de la police dans les cas de vol d'identité et de fraude, qui sont interreliés. Comme les statistiques officielles sur la cyberfraude ne montrent que la pointe de l'iceberg, il est extrêmement difficile pour les agents d'application de la loi de mettre au point un plan d'intervention complet et axé sur une démarche préventive (Blanco Hache et Ryder, 2011, 40).

De plus, le manque de coordination dans le traitement des plaintes, même entre les organismes d'une même administration, pose des problèmes importants, car chaque incident peut être pertinent pour de nombreux organismes et peut mener à la consignation d'informations auprès d'organismes fédéraux, provinciaux ou locaux d'application de la loi, ainsi qu'auprès d'agences d'évaluation du crédit, d'institutions financières et d'organismes de réglementation (Smith, 2008, 381). Ce manque de coordination mène aussi à un arriéré de données pertinentes et, puisque de nombreux organismes ne coordonnent pas leurs efforts et ne communiquent pas le renseignement qu'ils recueillent, il est difficile de savoir si une plainte est liée à un seul incident ou non. Habituellement, les victimes ne se rendent pas compte qu'elles ont été la cible d'un voleur d'identité jusqu'à ce qu'elles postulent un emploi ou demandent un prêt ou un prêt hypothécaire. Elles peuvent aussi découvrir que leur compte bancaire a été utilisé à des fins criminelles, ou des agences d'évaluation du crédit peuvent communiquer avec elles. Des commerces qui ont adopté une démarche préventive peuvent aussi informer les victimes du vol de leur identité (Smith, 2008, 381). Selon de récentes recherches, plus de 80 % des victimes de vol d'identité se rendent compte qu'elles ont été ciblées à la suite d'une expérience négative (p. ex. lorsqu'une institution financière refuse de leur accorder un prêt), et non grâce à des pratiques commerciales axées sur la prévention. La victime a déjà subi des pertes lorsqu'elle constate le vol (White et Fisher, 2008, 8). Certaines victimes découvrent le vol en moins de trente jours, mais nombre d'entre elles ignorent pendant des mois ou même des années que leur identité a été volée (White et Fisher, 2008, 8). Manifestement, plus il s'écoule de temps entre le vol et la découverte de celui-ci, plus il est difficile d'en retracer l'auteur et d'établir son identité. Des délais plus longs entraînent de plus grandes pertes financières chez la victime et l'obligent à faire davantage d'efforts pour se disculper (White et Fisher, 2008, 8). Ils font aussi en sorte que la victime sera moins susceptible de signaler l'incident. En effet, selon les estimations actuelles, près de 40 % des victimes d'un vol d'identité ne signalent pas le crime (White et Fisher, 2008, 8). Elles croient peut-être que la preuve est insuffisante ou que l'affaire n'est pas assez grave pour que la police fasse enquête, ou encore qu'il n'y a rien à faire. Les entreprises victimes de ce genre de crime ne le signalent pas toujours, souvent parce qu'elles craignent de subir des représailles ou que le fait que leurs vulnérabilités en matière de sécurité soient connues entraîne des pertes ou entache leur réputation

(Smith, 2008, 387). De plus, lorsque le vol n'est signalé qu'à une banque ou qu'à une société émettrice de carte de crédit, l'information ne parvient peut-être pas à la police, ce qui signifie que la fraude ne sera pas reconnue officiellement et ne fera pas partie des statistiques sur les crimes liés au vol d'identité (White et Fisher, 2008, 10).

7.0 Estimation des populations cachées d'auteurs de cyberfraude

Le problème que posent les populations inconnues ou cachées de délinquants est évident en termes d'application de la loi, d'allocation des ressources, d'élaboration des politiques en matière de justice pénale et de théorie criminologique (Rossmo et Routledege, 1990). Pour qu'un incident lié à la cyberfraude fasse partie des statistiques officielles sur la criminalité, la victime doit signaler le crime, la police doit donner suite au signalement et l'affaire doit être consignée officiellement. Dans le domaine de la cyberfraude particulièrement, il est difficile d'avoir un bon aperçu de la nature et de la fréquence des vols, puisque, souvent, les victimes ignorent qu'elles ont été la cible de voleurs ou ne signalent pas le crime pour d'autres raisons, par exemple parce qu'elles croient que l'incident n'est pas assez important pour que la police fasse enquête. En raison de ces problèmes, certaines approches ont été mises au point pour déceler les populations cachées de délinquants grâce à l'exploration de données. L'utilisation d'une forme de la méthode « capture-recapture », utilisée avec succès auprès d'autres populations criminelles, est la meilleure façon de commencer à examiner cette catégorie inconnue de délinquants.

Les méthodes « capture-recapture » sont utiles en tant qu'outil d'exploration des données auprès de diverses populations. En bref, ces méthodes permettent d'estimer la taille d'une population et peuvent être considérées comme une variante d'un modèle linéaire général (Weaver et Collins, 2007). Habituellement, elles nécessitent deux échantillons et elles permettent d'établir une proportion en se basant sur les individus qui font partie des deux échantillons afin de créer une distribution hypothétique d'échantillonnage. Grâce à ces méthodes, on se sert des caractéristiques récurrentes décelées dans les données à l'étude pour tirer des conclusions sur la proportion d'une population qui est active, mais qui n'est pas incluse dans les statistiques (Bouchard, 2007). Les méthodes de « capture-recapture » ont été mises au point pour la première fois en biologie, pour estimer la taille de populations animales (Seber, 1973), mais elles sont parfois été utilisées pour étudier les populations humaines, dans le domaine de la recherche épidémiologique.

Les modèles de « capture-recapture » ont été utilisés énormément dans le domaine de l'abus d'alcool ou d'autres drogues pour estimer le nombre d'usagers de drogues pouvant faire l'objet de traitements dans diverses collectivités (Bohning, 2004)[20]. Ces méthodes ont aussi été utilisées

[20] Voir aussi Calkins RF, Atkan GB (2000) Estimation of heroin prevalence in Michigan using capture-recapture and heroin problem index methods. *J Drug Issues* 30:187–204; Hser Y (1993) Population estimation of illicit drug users in Los Angeles county. *J Drug Issues* 23:323–334; Choi Y, Comiskey C (2003) Methods for providing the first prevalence estimates of opiate use in Western Australia. Int J Drug Policy 14:297–305; Hickman M, Cox S, Harvey J, Howes S, Farrell M, Frischer M, Stimson G, Taylor C, Tilling K (1999) Estimating the prevalence of problem drug use in inner London: a discussion of three capture–recapture studies. *Addiction* 94:1653–1662; Smit F, Toet J, van der Heijden P (1997) Estimating the number of opiate users in Rotterdam using statistical models for incomplete count data in *European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), 1997 Methodological Pilot Study of*

dans le domaine de la recherche criminologique. Des analyses faites par Willmer, Greene et Stollmack sur des populations générales de délinquants ont marqué la première utilisation des méthodes de « capture-recapture » en criminologie. À la suite de ces premières tentatives, les chercheurs ont aussi utilisé ces méthodes pour estimer les populations de cambrioleurs (Riccio et Flinkestein, 1985), de voleurs de voitures (Collins et Wilson, 1990), de prostituées (Rossmo et Routledge, 1990) et de leurs clients (Roberts et Brewer, 2006), de propriétaires d'armes illégales (van der Heijden et coll., 2003) et de narcotrafiquants (Bouchard et Tremblay, 2005). En raison de la nature inhérente des actes criminels, les méthodes de « capture-recapture » doivent être étendues afin de vérifier deux hypothèses clés : l'homogénéité et l'indépendance des populations.

Le problème est qu'aucun facteur extérieur ne peut influencer l'inclusion de l'acteur (ou son absence) dans le deuxième échantillon recueilli à l'aide de deux méthodes : les cas doivent être indépendants l'un de l'autre dans tous les échantillons (Weaver et Collins, 2007). Cela peut causer un problème dans le cadre des efforts actuels dans le cas où, par exemple, un délinquant qui s'est fait prendre tenterait de ne pas être détecté de nouveau. De la même façon, les deux échantillons doivent être homogènes au point où il n'existe aucune raison structurelle pour qu'un individu soit davantage susceptible d'être pris qu'un autre. En raison des variantes entre chaque cas de cyberfraude, on ignore comment l'ensemble de ces cas pourrait être homogène. Un travail d'avant-garde au sujet de l'utilisation des méthodes de « capture-recapture » pour détecter des cultures de drogue jusque-là inconnues des autorités a permis de bien comprendre comment minimiser les répercussions de ces potentielles violations d'hypothèses (Bouchard, 2007).
En termes généraux, une distribution d'échantillonnage représente tous les résultats possibles d'une hypothèse. Une distribution normale, parfois appelée courbe de Laplace-Gauss, est appropriée pour certains types de données, mais ce n'est pas toujours le cas. Par exemple, imaginez une situation dans laquelle vous devez estimer une distribution du nombre d'infractions aux règlements de la circulation. Il est possible de trouver le dossier des individus qui ont commis une, deux ou trois infractions, mais aucun dossier n'existe pour les individus qui n'en ont pas commise (Rider, 1953). Pour mesurer la cyberfraude, une distribution tronquée discrète serait une représentation plus appropriée en raison de la difficulté que pose l'estimation de la fréquence à laquelle les individus qui n'ont jamais été appréhendés ou qui n'ont été appréhendés qu'une seule fois commettent des infractions. Particulièrement, les méthodes de Poisson tronquées permettent de prédire un nombre précis de fois où un événement se produira pendant une période donnée, au cours de laquelle aucune information ne sera donnée au sujet du « groupe de contrôle, qui est non observé » (David et Johnson, 1952).

Cependant, la distribution de Poisson peut causer des problèmes lorsqu'elle est appliquée à des populations criminelles, car une distribution générale de Poisson exige un certain nombre d'hypothèses : la population à l'étude doit être isolée et homogène, et la probabilité qu'un individu soit observé, puis observé de nouveau, doit demeurer constante pendant la période d'observation (Bouchard, 2007). La première et la deuxième hypothèses provoquent des difficultés évidentes. Comme l'indique Bouchard, « les délinquants ont tendance à commettre des infractions pendant certaines périodes de leur vie, puis à arrêter; certains sont plus actifs que d'autres, et les

---

Local Prevalence Estimates. EMCDDA, Lisbon; Brecht M-L, Wickens TD (1993) Application of multiple-capture methods for estimating drug use prevalence. *J Drug Issues* 23:229–250.

possibilités qu'ils soient appréhendés de nouveau peuvent être différentes d'un individu à l'autre » (Bouchard, 2007). Fait peut-être encore plus important, la troisième hypothèse pose un problème avec les populations criminelles, puisque les délinquants sont capables de tirer des leçons de leurs erreurs et de modifier leur comportement à la suite d'une arrestation. Ils peuvent aussi faire l'objet d'une surveillance accrue à la suite d'une arrestation (Bouchard, 2007).

Bouchard a montré que l'utilisation des méthodes de Poisson tronquées, comme l'estimateur de Zelterman, conçu précisément pour contrer l'effet des départs sur ces hypothèses (Collins et Wilson, 1990), fournit une méthode appropriée pour capturer les populations criminelles cachées. La formule suivante permet d'obtenir l'estimation :

$$Z = N / (1 - e^{(-2*n2/n1)})$$

Z représente la population totale, N représente le nombre total d'individus arrêtés en raison d'une accusation au pénal, n1, le nombre d'individus appréhendés une seule fois, et n2, le nombre d'individus appréhendés deux fois pendant une période donnée (Bouchard, 2007). Par conséquent, si les données sur les individus connus qui ont été appréhendés au moins une fois « respectent la distribution de Poisson précisée par l'équation Z, la cellule manquante dans la distribution, c'est-à-dire le nombre de délinquants qui n'ont jamais été appréhendés, devrait être estimée correctement » (Bouchard, 2007). Cette approche permet d'évaluer les populations cachées.

Les avantages associés à l'utilisation de l'estimateur de Zelterman de Poisson pour estimer les populations criminelles sont évidents. Premièrement, il peut minimiser les répercussions de l'hétérogénéité de la population qui risque d'être appréhendée en éliminant la minorité de récidivistes qui ont été appréhendés à de nombreuses reprises. Particulièrement, la formule donnée par Zelterman inclut uniquement les délinquants appréhendés une (n1) ou deux fois (n2) afin d'établir le taux d'arrestation. Comme Bouchard l'indique :

> Zelterman (1988) et d'autres chercheurs qui ont conçu des modèles similaires (Chao, 1989) basent leur approche sur le raisonnement selon lequel les modèles d'estimation devraient être assez complexes pour être significatifs, mais assez simples pour contenir uniquement les paramètres nécessaires, en plus d'être près des nombres à estimer. Les observations qui sont près de l'objet d'intérêt devraient, intuitivement, y être associées de plus près (Bouchard, 2007).

Cette caractéristique causera des estimations plus conservatrices, mais il y a une certaine logique dans la notion selon laquelle les informations sur les délinquants qui n'ont jamais été appréhendés peuvent être estimées le plus précisément possible à partir d'informations sur les délinquants qui ne sont que rarement appréhendés. Fait intéressant, plus d'informations sont fournies à l'aide de modèles plus complexes qui tiennent compte de tous les individus appréhendés et de leur divers

taux d'arrestation (Bouchard, 2007)[21], ou de modèles qui tiennent compte d'une série de covariables avant de faire une estimation (Bouchard, 2007)[22].

Autre avantage du modèle de Poisson tronqué associé aux estimateurs de Zelterman : il peut être utilisé sur un seul échantillon (par exemple les données sur les arrestations), contrairement à d'autres approches de « capture-recapture » qui doivent pouvoir compter au moins sur trois échantillons pour faire des estimations. Cela peut être considéré comme un inconvénient, car dans certains cas, la triangulation serait avantageuse pour établir un échantillon, mais la méthode préférée pour estimer une population cachée de cyberfraudeurs exige de porter une attention particulière sur les individus qui ne font pas partie de la population générale. Autrement dit, le fait d'utiliser uniquement les données sur les arrestations limite l'interprétation à des estimations du nombre de délinquants « qui risquent d'être appréhendés », qui ne comprennent que les populations considérées comme cachées (Bouchard et Tremblay, 2005).

Une inquiétude qui peut naître de l'utilisation du modèle de Poisson tronqué associé à Zelterman est qu'on ne peut pas lancer l'hypothèse que la population de cyberfraudeurs inconnus est une population fermée, car il est possible que les délinquants mènent des activités criminelles, puis arrêtent de le faire. Malgré ce fait, le modèle suppose que « la population cachée qui nous intéresse est une population "fermée" » (Bouchard, 2007). Pour résoudre ce problème, d'autres chercheurs qui ont employé le modèle de Poisson tronqué associé à Zelterman ont compensé en utilisant des données à un niveau agrégé. Par exemple, lors du recensement des populations cachées de cultivateurs de marijuana, Bouchard démontre que la « possibilité que d'importants écarts existent par rapport à cette hypothèse est minimisée grâce à l'analyse de la distribution des nouvelles arrestations à un niveau agrégé (arrestations et nouvelles arrestations par les autorités provinciales) plutôt qu'au niveau d'une ville ou d'un quartier » (Bouchard, 2007). Cela n'élimine pas la possibilité que des individus cessent de mener des activités criminelles, mais les mesures prises au niveau agrégé réduisent les chances que des délinquants « soient exclus de l'échantillon simplement parce qu'ils se sont installés dans une autre ville ou un autre quartier » (Bouchard, 2007).

Il existe aussi certaines preuves (Kendall, 1999) que l'utilisation de modèles fermés pour des populations ouvertes n'est pas nécessairement aussi problématique que l'on pourrait penser au départ. Comme le suggère Bouchard, « si la période à l'étude est assez courte, les mouvements de la population criminelle ne seront probablement pas assez rapides et importants pour avoir des répercussions sur les estimations » (Bouchard, 2007) provenant de modèles de populations fermées, comme ceux associés à Zelterman. Puisque le modèle de Poisson tronqué associé à Zelterman n'a toujours pas été mis à l'essai avec une population de cyberfraudeurs, et que la composante inhérente « non spatiale et non géographique » de la cybercriminalité nécessite plus

---

[21] « Comparativement aux 30 298 délinquants estimés par Greene et Stollmack (1981) à l'aide d'un modèle hétérogène de Poisson pour D.C. en 1975, l'équation Z estime le nombre de délinquants à 29 842 (une sous-évaluation de 2 %). »

[22] « Comparativement aux 62 722 délinquants en possession d'une arme illégale, un nombre estimé par van der Heijden et coll. (2003), le modèle de régression basé sur Poisson, l'équation Z estime le nombre de délinquants à 50 866 (une sous-évaluation de 23 %). »

de recherches, il serait prudent, en plus d'utiliser le modèle, de faire appel à des modèles de Markov cachés ou à d'autres modèles conçus pour des populations ouvertes. Il faut choisir une méthode de capture de données en portant une attention particulière aux caractéristiques propres à une population afin de choisir la méthode la plus appropriée.

8.0 Établissement des caractéristiques des cyberfraudeurs, enquêtes et réseaux

Les chercheurs ont établi certaines théories pour expliquer pourquoi les gens commettent de la fraude. Parmi les principaux facteurs relevés, citons :

- la perception d'une *occasion*, comme l'absence de mesures de contrôle qui permettent de déceler la fraude ou de la prévenir, ou la possibilité de les contourner;
- un délinquant qui possèdes des *motifs* pour voler des biens, parce qu'il a des difficultés financières ou des dettes, ou encore parce qu'il vit au-dessus de ses moyens;
- une *rationalisation* des actes illégaux, comme la croyance que la victime peut essuyer la perte ou que l'argent volé sera remboursé;
- l'absence de *moyens de prévention*, c'est-à-dire des pratiques de sécurité et un cadre réglementaire inefficaces, ou des ressources et des tactiques insuffisantes en matière de prévention de la fraude.

Les motivations et les justifications des cyberfraudeurs sont semblables. Cependant, l'Internet a créé de nouvelles occasions de commettre de la fraude, et les délinquants peuvent s'installer dans des secteurs où les fournisseurs de services Internet ont de la difficulté à surveiller et à filtrer le trafic croissant sur leurs réseaux (Symantec, 2010, 8). L'Internet est un domaine très vulnérable, où il n'y a que peu de mesures de protection contre les fraudeurs (White et Fisher, 2008, 17). De plus, les sites de réseautage social offrent de nouvelles possibilités de commettre des crimes et certains analystes de l'industrie ont prédit que de nouvelles menaces pèseront sur ces sites à mesure que le nombre d'utilisateurs s'accroîtra (McAfee, 2010(b), 2). Les utilisateurs ont prouvé qu'ils se fient énormément à ces réseaux sociaux et qu'ils cliquent sans hésitation sur des hyperliens ou sur d'autres types d'invitations pour voir du contenu que leurs « amis » leur ont fait parvenir (McAfee, 2010(b), 4).

Certaines autres nouvelles tendances ont contribué à l'accroissement du nombre de cas de cyberfraude et de leur fréquence :

- une économie clandestine s'est établie autour du vol, de l'assemblage et de la revente de l'information (Deloitte, 2010(a), 5);
- les particuliers et les organisations dépendant de plus en plus des technologies informatiques pour conserver et traiter les informations et les communications;
- les transactions financières, les investissements et la vente en ligne, de même que la distribution à grande échelle de propriété intellectuelle, créent de nouvelles occasions de commettre une fraude et des vols;
- les difficultés économiques qu'ont connues certaines personnes à la suite de la crise économique mondiale de 2008 à 2010 ont créé de nouvelles occasions d'exploiter les peurs et les difficultés économiques des gens (Urbas et Choo, 2008, 6).

Par exemple, Symantec signale que le nombre d'envois de pourriel et de tentatives d'hameçonnage pour des raisons financières est demeuré sensiblement le même en 2008 et en 2009, mais qu'on a constaté une augmentation marquée du nombre de messages faisant de la publicité pour le refinancement de dettes et de prêts hypothécaires ainsi que du nombre d'offres de prêts et de possibilités de gagner de l'argent en travaillant à la maison (Symantec, 2010, 13). De nouveaux emplois ont aussi été créés dans l'économie clandestine toujours plus robuste. Quelqu'un peut ainsi devenir un « porteur d'argent » ou un « commis aux virements électroniques », dont il est question à la section 3.0 (Deloitte 2010(a), 6). Cela démontre que les cybercriminels ont déjà adapté leurs techniques pour profiter des événements actuels et des importantes tendances économiques.

Comme David Wall l'a mentionné (Wall, 2009), et comme on l'avait signalé auparavant, l'émergence de tendances et de liens connus entre les cyberfraudeurs a fait naître certaines questions au sujet des relations entre les utilisateurs d'un réseau. Plus particulièrement, le cyberespace fournit à de nombreux types de criminels un refuge qui leur permet également d'accroître leurs capacités organisationnelles et opérationnelles. On a tenu compte de la possibilité d'établir un réseau traditionnel de délinquants, mais certains faits prouvent que la structure hiérarchique ne s'applique pas aux réseaux en ligne de cyberfraudeurs. En d'autres mots, il serait inutile de posséder une compréhension aussi simpliste de la structure du réseau sans connaître la structure prédominante (Morselli, 2009).

Méthodologiquement, le meilleur endroit où commencer à recueillir des données est auprès de ceux qui combattent la cyberfraude : les enquêteurs des organismes d'application de la loi et les professionnels de la sécurité des technologies de l'information. Des données ont été recueillies lors d'entrevues téléphoniques au sujet de l'identification des organisations criminelles et de leurs membres, de la détermination de la façon dont les dirigeants sont nommés, des méthodes de recrutement, des activités criminelles, des niveaux de menace et des stratégies des groupes de travail mixtes. Puisque l'on connaît peu de choses sur cette population cachée de délinquants, il est pertinent d'examiner ce qui est connu à leur sujet afin de s'assurer de choisir le modèle de recherche le mieux adapté.

9. Méthodologie

La méthode de l'entrevue semi-structurée a été employée pour recueillir des renseignements sur les participants à la recherche. Les questions visaient la possibilité de recourir à des méthodes novatrices pour évaluer l'ampleur de la cyberfraude, identifier les sources actuelles de données et les lacunes et, enfin, suggérer de nouvelles sources de données susceptibles de procurer un portrait plus juste de l'ampleur de la cyberfraude au Canada. De plus, on a examiné les moyens possibles de déterminer la part de la cyberfraude attribuable à des réseaux criminels plutôt qu'à des individus. Les entrevues ont été réalisées par téléphone et ont pris de 45 à 60 minutes chacune.

Le codage des notes d'entrevue était ouvert, les notes étant relues en tenant pour acquis que les thèmes prévus dans le guide d'entrevue ressortiraient spontanément (Esterberg 2002). L'analyse a permis de dégager parmi les données des constantes susceptibles d'être elles-mêmes ajoutées aux codes thématiques. On a ensuite réexaminé la transcription des entrevues à la lumière d'un codage ciblé afin de valider les modèles initiaux. Alors que le codage thématique initial révélait certaines

caractéristiques relatives à la prévention de la cyberfraude et à l'application de la loi afférente, le codage ciblé a permis de dégager des constantes imprévues à partir des différentes sources de données, notamment sur le point de vue adopté respectivement par le personnel de la TI et par les responsables de l'application de la loi. Les résultats de la recherche ont été ventilés selon sept catégories thématiques qui correspondaient aux méthodes de codage ciblé.

9.1 Échantillon

Des responsables, dix de la sécurité de la TI et neuf de l'application de la loi, venus de divers endroits au Canada ont été interviewés. Ce groupe a été constitué à partir d'un échantillon intentionnellement stratifié de relations personnelles, puis on a étendu cet échantillon par « sondage en boule de neige ». Aucun des participants n'était connu des chercheurs avant l'entrevue. Puisqu'on garantissait l'anonymat et la confidentialité des répondants interviewés, un code a été attribué aux notes d'entrevues et aucun des répondants n'a été identifié par son nom. Aucune rémunération n'a été offerte aux répondants pour participer à l'étude.

Les responsables de sécurité de la TI venaient de différents secteurs d'activité partout au Canada : vente au détail, banque, finance, université, alimentation, restauration, énergie ou gouvernement. Tous occupaient des postes de niveau supérieur ou étaient cadres et possédaient de nombreuses années d'expérience dans leur domaine. Le personnel responsable de l'application de la loi, pour sa part, venait de différentes provinces et régions du Canada. Il s'agissait de membres de détachements de la GRC ou de services de police municipaux de grandes villes canadiennes. Tous possédaient une expérience des enquêtes sur la cyberfraude à titre d'agents d'application de la loi dans notre pays.

9.2 Résultats

9.2.1 Méthodes et moyens de perpétration de la fraude

Les résultats des entrevues montrent que de nombreuses infractions de cyberfraude sont commises au Canada et qu'il existe toute une gamme de stratagèmes, relativement simples jusqu'à très sophistiqués. On a demandé aux répondants quels types d'incidents frauduleux en matière de sécurité de la TI avaient été le plus fréquemment signalés au cours des douze derniers mois. Parmi ceux-ci figuraient l'écrémage au moyen d'un appareil portatif ou la modification d'un appareil de paiement par carte de débit ou de crédit au terminal d'un point de vente. Cette technique comportait parfois l'installation d'un enregistreur vidéo au-dessus du terminal pour capter le NIP. De l'avis de certains répondants, ce type de fraudes semblait être le fait d'« employés dans de nombreux cas, non pas qui remplaçaient le clavier d'identification personnelle, mais qui retiraient des tuiles du plafond et y installaient une caméra; possiblement du personnel d'entretien ou d'autres employés ».

L'hameçonnage était fréquent aussi, tout comme le vol avec carte de crédit et l'utilisation frauduleux d'une carte de crédit volée pour acheter une marchandise ou un service. D'après un répondant, responsable de l'application de la loi, la plupart des infractions portées à sa connaissance relevaient d'« un stratagème par lequel le fraudeur recourait à une caméra ou à un

faux clavier d'identification personnelle pour enregistrer des données ou filmer le client introduisant son NIP, puis reproduisait la carte et se mettait à l'utiliser ». Un autre type de cyberfraude signalé par des répondants ciblait un service public (d'électricité, en l'occurrence). Au sujet du dommage causé, un répondant a fait remarquer : « ça ne rapporte rien de s'en prendre à nous à des fins financières; nous redoutons des attaques contre notre infrastructure essentielle, car celles-ci provoquent des pannes. »

Les propos des répondants ont fait ressortir que les auteurs de cyberfraudes adaptent rapidement leurs techniques pour profiter des événements courants et des tendances économiques. Ainsi, après le récent tremblement de terre au Japon, des courriels frauduleux semblent avoir été diffusés sur-le-champ pour réclamer des dons en faveur des victimes. Au dire de l'un des responsables de l'application de la loi :

> En 2008, on a vu apparaître de nouveaux stratagèmes tirant profit du ralentissement économique (offre d'emploi frauduleux, site de clavardage, site Web) ciblant les personnes recherchant un travail ou de l'argent rapide, par exemple des prêts d'un montant peu élevé pour lesquels il faut verser une avance. Les sites de réseautage social ou d'offre d'emploi, Craigslist ou Kijiji jouent tous un rôle déterminant. Une nouvelle arnaque, celle du « client mystère », consiste à demander à une cible d'agir comme client de Western Union, souvent à un point de vente Wal-Mart, pour s'y présenter et envoyer de l'argent.

Un autre répondant du sous-échantillon d'application de la loi a formulé le commentaire suivant concernant l'évolution des moyens de commettre une cyberfraude :

> Je n'en reviens pas du nombre de gens qui viennent porter plainte après avoir envoyé de l'argent à l'étranger – le plus souvent par courriel et non par lettre −; ces personnes servent de mules pour le transfert d'une somme à l'étranger. Elles s'attendent à recevoir quelque chose en retour, mais ne reçoivent jamais quoique ce soit. D'autres personnes publient une annonce pour vendre leur voiture sur le Web et des gens d'autres pays leur demandent de leur expédier la voiture. Heureusement, la plupart des victimes sont assez intelligentes pour ne pas le faire; cependant, elles nous informent de l'incident sur notre site Web au lieu de déposer une plainte officielle.

Dans la même veine, chaque année au moment d'effectuer la déclaration d'impôt, de faux centres fiscaux voient le jour à des sites Web invitant les victimes à donner des renseignements personnels, notamment leur numéro d'assurance sociale, pour savoir s'ils vont bénéficier d'un remboursement d'impôt. De plus, des gens mettent souvent en vente dans le cyberespace des marchandises populaires et à la mode qu'ils ne possèdent pas. Un répondant a ainsi évoqué des pertes monétaires subies à l'occasion des Jeux olympiques d'hiver de 2010 à Vancouver :

> Il y a eu quelque 26 personnes qui ont été fraudées par l'intermédiaire de Craigslist ou de Kijiji, après qu'on leur eut offert des billets pour des événements olympiques. Le fraudeur avait pris leur argent, puis leur avait dit qu'il ne possédait aucun billet; il avait obtenu l'argent des gens sans avoir l'intention de leur fournir de billets. En général, la plupart des pertes des victimes avaient été inférieures à 1 000 $.

Certaines victimes subissent des pertes plus lourdes. Le même répondant l'a laissé entendre : « Dans un autre cas, la victime avait versé d'avance 30 000 $ pour louer une propriété; elle venait d'arriver au Canada ».

9.2.2 Dommage causé à la victime

Cela n'étonnera personne, les entrevues avec les répondants responsables de l'application de la loi semblaient porter avant tout sur les victimes individuelles de la cyberfraude, alors que les entrevues menées avec les représentants de la TI étaient davantage axées sur les entreprises de leur secteur d'activité. À titre d'exemple, lorsqu'on a demandé à un répondant du premier groupe combien de cyberfraudes visaient directement des personnes, sa réponse a été succincte : « Toutes ! »

Pour ce qui est du dommage causé, le même répondant a expliqué que la cyberfraude frappait plus durement les entreprises que les personnes :

> La plupart des cartes bancaires permettent de retirer jusqu'à 1 000 $ par jour, soit quelque 3 000 $ en trois jours. S'il s'agit d'une carte de crédit, le fraudeur peut faire de gros achats (p. ex. un téléviseur ou une chaîne stéréophonique) ou effectuer des appels interurbains.

Cela a été particulièrement le cas des fraudes individuelles réalisées uniquement en ligne, par exemple par l'intermédiaire de petites annonces virtuelles, ou de l'achat d'un produit par Internet, dont le montant est habituellement peu élevé, souvent aussi peu que 200 $. L'une des explications, c'est que les gens semblent davantage disposés à passer outre aux avertissements et à ne pas se montrer soupçonneux ni nerveux, si le montant en jeu est faible.

Un autre responsable de l'application de la loi a bien mis en lumière les personnes victimes de la cyberfraude en faisant remarquer : « nous tendons à penser que de tels actes criminels ne concernent que les grandes villes, mais il s'en commet partout au pays; les victimes vivent souvent en milieu rural; le phénomène touche tout le pays, pas seulement Ottawa et les grosses banques torontoises. »

Un répondant du sous-échantillon d'application de la loi s'est dit préoccupé par certaines constantes chez les victimes : « Beaucoup de victimes sont âgées. Si elles perdent de l'argent, c'est très dur pour elles; même la perte de 1 000 $ ou de 2 000 $ peut se répercuter sur leur santé, leurs médicaments, leur alimentation, et le reste. »

Un autre répondant a renchéri :

> Je n'ai traité aucune menace contre une entreprise; la plupart de ces menaces sont signalées à la Section des infractions commerciales de la GRC. Je traite des menaces contre des personnes; jeunes et aînés sont souvent ciblés par courriel, dans des stratagèmes du genre « Envoyez-nous de l'argent » ou « Transférez de l'argent dans tel compte ».

Selon un autre répondant, il y a peu de constantes parmi les victimes : « les victimes se répartissent entre hommes et femmes de différents âges ».

Par ailleurs, certains groupes du crime organisé semblent s'en tenir à de petits montants, pour que les victimes n'aient pas tendance à porter plainte et pour que la police n'ait pas envie d'enquêter. Même des fraudes importantes, par exemple celles qui se fondent sur la séduction, utilisent un site de rencontre en ligne, mettent souvent en jeu une relation personnelle et sortent parfois du cyberespace, la somme demandée par le fraudeur tourne autour de 3 000 $ à 5 000 $ (même si elle varie en fonction de la fortune de la victime). Règle générale, la présente recherche a permis d'établir que le montant volé est généralement inférieur à 5 000 $.

D'après un employé en TI, néanmoins, le cumul de telles pertes pour une victime secondaire comme une banque peut atteindre 100 000 $ par mois, soit 1,2 million de dollars par année. Les répondants ont évoqué certains dommages non monétaires causés par les incidents de cyberfraude portés à leur connaissance. Lorsque du personnel TI traitait des dommages, c'était principalement de dépenses administratives, tant pour les prévenir que pour intervenir après les fraudes. L'un des répondants a ainsi parlé des dépenses encourues après la perte initiale :

> Les conséquences sur les opérations exigent du temps, à savoir éliminer les logiciels malveillants et mettre à profit un logiciel antivirus. Et aussi tenir à jour l'antivirus, mettre en œuvre une pièce correctrice, rechercher les éléments vulnérables, surveiller le trafic sur le réseau, rechercher les éléments vulnérables à corriger.

Dans le cas des entreprises victimes, il faut inclure des dommages à leur réputation ou à leur marque de commerce ainsi que la perte de clients. Dans le cas des personnes, les dommages non monétaires comprennent la détresse émotionnelle, l'embarras et l'impuissance, le tort à leur réputation, l'intimidation, le stress et la dépression. En particulier, l'arnaque par la séduction peut se révéler dévastatrice; des victimes envoient des milliers de dollars à des personnes qu'elles croient être leur âme sœur. Dans la forme extrême d'une telle arnaque, une victime canadienne est amenée à se rendre dans un autre pays, où on la retient en otage à son arrivée pour réclamer une rançon par Internet.

9.2.3 Caractéristiques des fraudeurs

Dans le sous-échantillon TI, les répondants semblaient différer d'opinion sur les auteurs des infractions : des initiés ou des non-initiés malveillants? D'après l'un de ces répondants, des employés de l'entreprise étaient à l'origine des fraudes « dans quelque 20 % des cas ». D'après un autre répondant TI, cependant :

> Les vols sont le fait de personnes étrangères à l'entreprise, mais qui bénéficient de complicités principalement internes, notamment pour l'installation d'un clavier d'identification personnelle ou d'une caméra. Dans le secteur de la restauration, le roulement du personnel atteint 400 %; il est donc difficile d'en assurer le suivi… Mais lors de l'embauche, nous avons pour politique de vérifier les antécédents des candidats en matière de crédit et auprès de la police.

Le même répondant laissait entendre la difficulté de prévenir la fraude Internet : « Ces commerces sont franchisés, alors il n'est pas facile de leur imposer [des politiques d'embauche]…; nous n'avons jamais attrapé quelqu'un en vérifiant ses antécédents auprès de la police…; on n'y repérerait que les individus déjà épinglés par la police.

Fait intéressant qui a été rapporté, un initié est traité autrement qu'un fraudeur étranger à l'entreprise, car il pourrait être affilié au crime organisé, comme l'a expliqué l'un des répondants TI :

> Si un employé est en cause, nous parlons d'une fraude d'initié, nous classons l'affaire autrement. Nous possédons des systèmes qui recherchent alors des antécédents judiciaires; bien que de tels cas ne soient pas fréquents, il y en a eu au cours des douze derniers mois. Habituellement, un initié est approché par un groupe criminel extérieur (à titre d'exemple, l'initié travaille à la réception et a accès aux données des clients).

Après avoir constaté à partir de l'échantillon de la TI qu'on s'occupait habituellement à l'interne d'un initié et qu'on signalait à la police un cyberfraudeur de l'extérieur, nous n'avons pas été très étonnés que certains responsables de l'application de la loi affirment que l'auteur d'un crime était habituellement étranger à l'organisation, si la victime était une entreprise. Ainsi l'un d'entre eux, lorsqu'on l'a interrogé sur la situation des fraudeurs, a dit que, autant qu'il sache, ils étaient tous « de l'extérieur ». Un autre répondant, du groupe TI celui-là, a également affirmé que l'auteur d'une cyberfraude était généralement étranger à l'entreprise.

9.2.4 Structure et fonction d'un réseau

D'après nombre de répondants en application de la loi et en sécurité de la TI, les cyberfraudes au Canada sont perpétrées par des gens appartenant à des réseaux du crime organisé. Dans l'échantillon TI, on estimait que la cyberfraude relevait d'un réseau en se fondant soit sur les caractéristiques communes aux infractions ou la complexité apparente de celles-ci, soit sur des renseignements fournis par une autorité extérieure. Voici les propos d'un répondant :

> … il y avait là une constante; lorsque nous avons constaté que des machines étaient systématiquement volées, il nous a été facile d'en déduire que ce ne pouvait être le fait d'une seule personne. Les magasins ont été cambriolés en temps suffisamment court pour que ce ne puisse être l'ouvrage de la même personne.

Selon un autre répondant, ce qui était frappant, ce n'était pas les caractéristiques de la fraude, mais son ampleur. À la question de savoir si la cyberfraude s'appuyait sur un réseau criminel, telle a été sa réaction :

> Je crois que oui. C'est beaucoup l'instinct qui me le fait dire, car certains aspects ont trop d'envergure pour une seule personne. Même pour certaines fraudes non sophistiquées, je pense que leur auteur a recours à des instruments créés par d'autres. Cela semble donc improbable que ce soit le résultat d'un travail individuel. La fraude semblait sophistiquée pour l'identification des cibles, mais ressortissait de moyens moins raffinés pour les attaques contre les cibles elles-mêmes.

Un autre répondant de la TI a fait part ainsi de la même conviction au sujet de la complexité des stratagèmes de cyberfraude et de la présence d'un réseau pour la soutenir : « les appareils sont perfectionnés, par conséquent nous estimons que les fraudeurs s'organisent entre eux… [particulièrement lorsque] d'autres appareils similaires apparaissent ailleurs au pays ». Autrement dit, les fraudes ont trop d'envergure et sont trop sophistiquées pour qu'une seule personne puisse les exécuter, surtout lorsque surviennent d'autres fraudes semblables à divers endroits au Canada.

Dans l'ensemble, les répondants croyaient que les fraudeurs travaillaient par petits groupes de deux ou trois. De plus, ils affirmaient que les fraudeurs n'étaient pas Canadiens et que, souvent, ils n'opéraient pas à partir de notre pays. « Nous sommes au courant de certaines personnes ou organisations appartenant à la mafia russe », d'affirmer un répondant. Selon eux, le principal moyen de savoir si ces personnes menaient leurs opérations d'en dehors du Canada ou non, c'était le fait que leur adresse IP renvoyait à des endroits hors de notre pays. Si d'autres répondants étaient persuadés qu'un réseau criminel commettait les cyberfraudes portées à leur connaissance, c'est que cette information leur provenait de la police : « [voilà] ce que m'a affirmé la banque ou la GRC; celle-ci m'a tout simplement appris qu'ils faisaient partie d'un groupe organisé ».

De même, à la question de savoir si les cyberfraudes qui leur étaient signalées avaient été commises par un réseau criminel, la plupart des responsables de l'application de la loi que nous avons interrogés nous ont répondu par l'affirmative. Certains d'entre eux étaient convaincus d'avoir affaire à un réseau hiérarchique. L'un d'eux :

> Oui. Dans des opérations d'écrémage, nous voyons souvent un groupe d'individus voler un clavier d'identification personnelle, puis quelqu'un d'autre le modifier par technologie Bluetooth, enfin un troisième utiliser la carte et se procurer l'argent comme tel. Or il m'apparaît assez clair que d'autres personnes dirigent ces paliers inférieurs; ils ne travaillent pas pour leur propre compte.

Cette structure hiérarchique a été corroborée par un autre répondant : « Si un fraudeur opère au palier inférieur, commettant un crime ou se procurant de l'argent d'un endroit à un autre, il ignore qui se trouve au palier supérieur. »

La présente recherche le confirme, la cyberfraude serait l'œuvre de petits groupes de personnes passablement bien organisées, très qualifiées au point de vue technique et sachant ce qu'elles font. D'après le sous-échantillon d'application de la loi : « Elles n'agissent jamais seules. Elles appartiennent à de petits groupes, sont fort bien organisées et connaissent leur travail. Souvent, elles sont très bien organisées… et toujours nombreuses. »

Un autre répondant renchérit sur ce point, opinant qu'un réseau donné était disséminé et que les réseaux :

> Étaient adaptables, et non pas structurés comme les réseaux criminels classiques. J'ignore si ces personnes utilisent leur véritable nom ou un indicateur en ligne. [Elles] communiquent par clavardoir dont l'accès est contrôlé et dont il faut connaître un membre.

> La plupart parlent anglais ou français; elles communiquent dans ces langues ou leur langue maternelle.

En règle générale, on a relevé une tendance à différer d'opinion au sujet de la forme d'une structure particulière. Dans certains cas, des répondants étaient d'avis que les réseaux étaient aussi liés à d'autres organisations criminelles plus classiques comme les Hell's Angels; pourtant on a peu appris sur la façon dont ils arrivaient à identifier ces groupes et à établir de tels liens. Selon un autre répondant, la structure des réseaux de cyberfraude ressemble à une structure hiérarchique classique : « Si une personne relève d'un palier inférieur, effectuant des fraudes ou se procurant de l'argent d'un endroit à un autre, il ignore qui se trouve au palier supérieur. Les personnes qui contribuent à mettre sur pied une fraude sont mieux informées de ce qui se passe dans le groupe. » Les principaux joueurs ont tendance à s'isoler du reste du groupe grâce à la technologie, à rendre plus difficile pour les responsables de l'application de la loi d'identifier le véritable chef, c.-à-d. la personne qui coordonne dans l'ombre les activités du groupe. On croit que les membres de ces groupes baignent également dans la contrefaçon de devises ainsi que dans la falsification de passeports et de pièces d'identité, en plus de la cyberfraude.

Parmi le sous-échantillon des répondants du secteur de l'application de la loi, on croit détenir la preuve que la structure de réseau hiérarchique classique n'allait pas nécessairement de soi, comme l'a souligné un répondant : « On semble plutôt être en présence d'une petite entreprise, parfois l'entreprise d'une seule personne; leurs membres peuvent entretenir des relations d'affaires, mais [pas] à la manière du crime organisé connu. » Invité à le faire, le même répondant s'est expliqué :

> Si quelqu'un possède une liste de cartes de crédit et de renseignements personnels, c'est de sa propre initiative; il recherche ensuite des comparses dans un clavardoir, puis dans un site de clavardage une autre personne susceptible de lui acheter sa liste; ce n'est pas du crime organisé, c'est une relation du genre fournisseur-client; pas comme celle des Hell's Angels qui procèdent de la même façon pour vendre de la drogue; ces gens-là ne sont pas fidèles à un fournisseur et à leurs clients; ils font des affaires entre eux, mais pas au sein d'une organisation au sens strict; ils se retrouvent pour transiger et disposent de lieux d'échange – à savoir un clavardoir, un site Web −, des lieux virtuels.

On a reconnu qu'il y avait beaucoup d'exagération et de spéculation dans ce domaine, même chez les responsables de l'application de la loi, et qu'il fallait d'autres études pour mieux connaître le genre de personnes s'adonnant à la cyberfraude. Cette divergence d'opinion sur la structure en réseau a été mise en lumière par un autre répondant : « [Ils] entendent des choses, connaissent certains détails, mais ce sont en bonne partie des rumeurs concernant les dirigeants de ces groupes. Nous avons besoin d'études plus poussées sur le genre de criminels à qui nous avons affaire. »

Aux dires des répondants, les réseaux ont habituellement leurs assises à l'étranger (Europe de l'Est [Roumanie, Bulgarie, Pologne ou Russie], Moyen-Orient, Extrême-Orient ou Afrique occidentale, ou encore Algérie, Chine, Sri Lanka, Ghana et Nigeria ainsi que Royaume-Uni, Allemagne, Espagne et France); leurs membres possèdent une bonne instruction tout comme beaucoup de connaissances et d'expertise en technologie informatique. Outre les personnes, des entreprises sont ciblées par des réseaux de cybercriminels : « Les sites Web de piratage et

d'hameçonnage à large diffusion sont d'un niveau supérieur; ces gens-là excellent au piratage et connaissent bien le système bancaire. »

S'il est difficile d'identifier la structure d'un réseau de cyberfraude, c'est peut-être en raison de la diversité des mesures d'application de la loi. Comme l'a fait remarquer un répondant :

> Une bonne part de nos enquêtes nous amène à appréhender le groupe intermédiaire. Certains corps policiers ont tendance à concentrer leurs efforts au niveau de la rue pour effectuer rapidement des arrestations, qui ne paralysent pas les organisations criminelles. Même en remontant la hiérarchie, nous ne parvenons qu'au palier intermédiaire. Le véritable leader ou bénéficiaire reste à l'abri à l'étranger, d'où il coordonne les activités.

Par ailleurs, les connaissances sur la structure d'un réseau variaient en fonction du type de criminalité, a-t-on dit. Invité à le faire, le même répondant s'explique ainsi :

> [La structure] dépend du type de fraude. Dans le cas du marketing de masse, elle s'appuie sur de petits groupes, bien intégrés, qui passent d'un stratagème à un autre, par exemple d'annonces frauduleuses sur un site de vente de voitures une semaine à un stratagème sur EBay la semaine suivante. Mais ils conservent le même *modus operandi* général − faux site Web ou encore achat ou vente de faux biens ou services −, mais l'adaptent d'un site à l'autre. Les groupes œuvrant dans la fraude à carte de crédit ne s'en tiennent pas à ce domaine; ils suivent la demande, par exemple, la contrefaçon de cartes de crédit. Mais aussi la contrefaçon de devises, de passeports ou de pièces d'identité, selon la marchandise en demande. Leurs membres changent-ils? Pour certains groupes, oui, compte tenu du type de fraude. Ils peuvent être liés à d'autres organisations criminelles, mais j'ignore comment ils trouvent ces autres groupes et établissent des liens avec eux.

Lorsqu'il s'agit de sites Web de piratage ou d'hameçonnage à large diffusion, les fraudeurs travaillent souvent dans une équipe d'experts, croit-on, chacun jouant un rôle particulier au sein du réseau. On suppose que le réseau est structuré en fonction de l'objectif à atteindre. Au dire de l'un des répondants, la structure se compose de « spécialistes, celui du hameçonnage cherchant à voler des renseignements, puis un autre s'en servant pour obtenir de l'argent; c'est un monde d'experts. Certains sont habiles à créer des cartes de crédit et d'autres à retirer de l'argent d'un guichet automatique bancaire (GAB). » Selon le même répondant, on insiste sur les connaissances plutôt que d'autres ressources; « ils peuvent collaborer pour maintenir un réseau de zombies, mais cela ne veut pas dire qu'ils font affaire ensemble : ils partagent leurs connaissances, pas nécessairement leur argent ou leurs activités criminelles. »

Par exemple, une personne peut se charger du hameçonnage, tandis qu'une autre, experte, utilise les renseignements volés pour créer une carte de crédit frauduleuse, grâce à laquelle une troisième personne, experte aussi, vole de l'argent dans le compte d'une victime à partir d'un GAB. Au cours de la présente recherche, on a établi que, parfois, ces personnes prennent contact entre elles dans un clavardoir ou un groupe de discussion sur le Web; elles s'unissent ensuite pour réaliser

des transactions criminelles chacun de leur côté. Et, renchérit un répondant de l'application de la loi :

> Ces gens se connaissent. Pas seulement en ligne. Mais lorsqu'ils sont en ligne, ils échangent de l'information sur la façon de se perfectionner. Ils se connaissent dans la vraie vie. Nous ne parvenons jamais à repérer le joueur clé. La plupart sont des hommes de 20 à 35 ans. Beaucoup sont bilingues, voire trilingues.

9.2.4 Activités d'application de la loi

Pour ce qui est de contrer la cyberfraude, le sous-échantillon du domaine de la TI a fait part d'une tendance à favoriser la prévention plutôt qu'à réparer après coup les dommages causés lors d'un incident. En particulier, la prévention semble être axée sur la sensibilisation aux réalités du monde des affaires plutôt que sur la compréhension de la nature et des caractéristiques de la cyberfraude. On semble s'entendre sur le fait que la cyberfraude relève d'un domaine propre et qu'on recourt à la technologie pour résoudre ce problème de façon proactive. Comme l'a dit l'un des répondants :

> Nous consacrons beaucoup de temps à établir un profil général de comportement, de sorte que nous pouvons nous pencher sur une situation et nous attendre à ce qu'un client se comporte d'une certaine manière; s'il déroge à la norme, nous devons nous y intéresser. Nous tenons à nous assurer que les gens évoluent en respectant des systèmes et des règles; grâce à ceux-ci, nous pouvons établir que quelqu'un pose un geste inusité ou imprévu.

Selon un autre répondant, la prise de conscience d'une cyberfraude en train de se dérouler dépend d'observations par des employés en mesure d'observer les activités au sein d'une entreprise. À son dire, dans le cas d'un copieur de carte, « quelqu'un finit par le remarquer ou donne l'alerte ». Dans d'autres cas, d'après un répondant :

> On a remarqué l'enlèvement de tuiles du plafond [pour y installer une caméra] et le comportement inusité de certaines personnes. Remplacer le clavier d'identification personnelle a déclenché une alarme et a mis le clavier hors fonction – c'est là un mécanisme de sécurité −; ce problème est bien connu dans notre secteur; il s'agit d'un mécanisme de protection standard. Tout cela nous ramène à l'ingénierie sociale et à être attentif à ce qui se passe au magasin.

Fait intéressant, même si les répondants de la TI connaissaient peu les réseaux de cybercriminalité, l'un d'eux a fait la remarque suivante : « Si de multiples fraudes se produisent, nous considérons être menacés. »

D'une façon générale, certains répondants de la TI ont affirmé que leur organisation avait renforcé ses mesures de sécurité en matière de TI et mis en place une détection en temps réel des transactions frauduleuses, notamment recouru à des logiciels spécialisés et à des analystes de sécurité. Certains acteurs de ce secteur se sont mis aussi à mieux vérifier les antécédents en matière de sécurité de leurs éventuels employés; et cela, malgré la difficulté de le faire, dit-on,

dans l'industrie de la vente au détail à cause des franchises. Certains répondants de la TI ont mis en avant une autre mesure susceptible d'être utile : un clavier d'identification personnelle biométrique. Bien que la carte à puce présente un grand avantage, paraît-il, elle ne constitue pas une solution parfaite au problème du vol d'identité et de la fraude.

Concernant les techniques dont les organismes d'application de la loi disposent actuellement pour combattre la cyberfraude, un répondant a observé que les progrès techniques constituent actuellement un problème. Plus précisément, il s'est dit « préoccupé par la capacité de suivre les progrès techniques, les utilisations de plus en plus diversifiées de la technologie. » La mobilité croissante de cette technologie préoccupe également : « au moyen d'un téléphone intelligent, on peut commettre un crime n'importe où, dans de multiples villes le même jour; nous peinons à suivre la trace d'un appareil. »

En dépit de la propension actuelle à ne pas signaler une fraude aux responsables de l'application de la loi, admet un répondant, « nous signalons tout; la police entre en jeu lorsqu'il s'agit d'un crime individuel. » Il n'est pas clair si la police possède les ressources nécessaires pour traiter tous les signalements. Comme l'a dit un responsable de l'application de la loi :

> La police ne dispose pas des ressources nécessaires pour traiter ces cas, car il y a beaucoup trop d'incidents de ce genre. Si le Canadien moyen perd quelques centaines de dollars, ce n'est pas une priorité pour nous. Des crimes plus importants sont commis, un meurtre par exemple. Il y a beaucoup trop d'incidents et il est impossible pour un corps policier de s'en occuper.

Or ni l'absence de signalement ni la pénurie de ressources pour y donner suite ne semblent le principal problème dans les activités d'application de la loi. Comme l'a révélé l'un des répondants de ce secteur :

> Le plus gros obstacle consiste à obtenir les renseignements dont nous avons besoin. Les fournisseurs de messagerie électronique ou d'accès Internet (FAI) se trouvent souvent hors des États-Unis ou du Canada, et il est souvent très difficile d'obtenir de l'information, sauf en cas de vie ou de mort. Une telle situation protège bien les renseignements personnels des gens, mais complique une enquête. Est-ce qu'il serait utile d'obtenir l'information par mesure judiciaire? Je ne sais pas si cela serait plus efficace.

9.2.5 Problèmes concernant les données et le signalement

Au sein du sous-ensemble des répondants de la TI, les principaux problèmes concernant un signalement semblaient être liés à la conviction que les autorités soit ne pourraient, soit ne voudraient rien faire au sujet de la cyberfraude. Au dire d'un répondant, « qu'est-ce qui nous pousserait à signaler un incident? D'après mon expérience, les responsables de l'application de la loi n'y donnent aucune suite et cela pourrait nous rendre cyniques, particulièrement parce que nous faisons l'effort de le signaler et que cela semble inutile. »

D’autres commentaires de répondants du sous-échantillon de la TI corroboraient cette préoccupation :

> Si je me fonde sur mes interventions auprès de la police, celle-ci se montre très peu préoccupée par la fraude par carte de crédit et ne souhaite pas faire enquête à la suite de nos demandes. Elle ne semble pas disposer de suffisamment de personnel qualifié. De plus, elle semble consacrer la plupart de son temps à lutter contre l’exploitation d’enfants par Internet, de sorte que son bassin de ressources est employé à autre chose. Elle doit embaucher et former davantage de gens.

Telle a été aussi la réponse d’un autre répondant de la TI :

> J’ai vécu un autre incident, personnel celui-là, lors de la vente en ligne de ma voiture. Je l’ai signalé à la GRC et elle m’a renvoyé à PhoneBusters; j’y ai obtenu un message automatique selon lequel personne ne pouvait me parler, parce que ce service recevait trop d’appels; je n’ai même pas pu laisser un message. Je me suis senti totalement dépourvu.

Dans certains cas, le sous-échantillon de la TI a révélé qu’une entreprise ne souhaitait pas collaborer avec la police par crainte de paraître vulnérable à la fraude aux yeux du public. Un répondant a renchéri à ce sujet lorsqu’on lui a demandé si son entreprise signalait les cyberfraudes : « Non. Mais cela n’a pas été rapporté par les médias. Elle n’a pas effrayé la clientèle. » Voici l’explication plus succincte qu’en offre un autre répondant du même groupe : une organisation, « souhaite que ce genre de choses ne se sache pas, car elle ne veut pas que son nom se retrouve dans le journal ».

On s’est également dit préoccupé par la logistique de la collecte de données et par un manque de communication entre les sources de données dans un environnement d’affaires concurrentiel par nature. Au dire d’un répondant :

> Lorsqu’une organisation a fait l’objet d’une intrusion, elle craint de le révéler à qui que ce soit. Elle garde le silence, c’est une question de fierté. Or toutes font l’objet d’intrusion, mais la mentalité veut qu’on n’en parle pas à d’autres organisations du secteur; personne n’apprend quoi que ce soit des erreurs des autres. Il faudrait un mécanisme discret permettant de mettre en commun [des renseignements].

Or, certains faits semblent montrer que les entreprises ne recueillent même pas nécessairement des données qui nous permettraient de mieux comprendre les cyberfraudes. Répondant : « Nous n’en faisons pas le décompte. Nous ne faisons pas de calculs. Nous évaluons le nombre d’attaques électroniques à la lumière des coupe-feu et des pourriels (99 % des courriels que nous recevons sont en fait des pourriels ou des courriels dangereux contenant un virus), mais nous ne relevons pas les incidents un à un. »

Dans d’autres cas, selon des répondants, même si des données étaient disponibles, on doutait qu’elles soient mises à profit de façon opportune ou pratique. De l’avis d’un répondant de la TI, « on ne voit pas beaucoup l’intérêt de poursuivre un criminel à col blanc ou un fraudeur. Nous ne

disposons pas de statistiques montrant à coup sûr que nous devons poursuivre en cas de cyberfraude; c'est un phénomène cyclique et non une priorité; l'industrie ne la signale pas, ne souhaite pas la révéler; et puis la plupart [des responsables de l'application de la loi] consacrent temps et énergie à la lutte contre l'exploitation en ligne des enfants. »

L'une des principales préoccupations parmi le sous-échantillon des répondants de la TI semblait être le manque de coopération entre l'industrie et le gouvernement : « dans nos relations avec le gouvernement fédéral, nous devons fournir des renseignements, mais nous ne recevons pas toujours de rétroaction. Nous supposons que rien n'est fait. Cette rupture dans la communication n'est pas fructueuse. » À notre demande, ce répondant a expliqué :

> D'après des discussions tenues par des banques lors de réunions, nous avons conclu que les responsables fédéraux de l'application de la loi au Canada nous sont de peu d'utilité pour nous tenir au courant des menaces de cyberfraude. Des alertes nous parviennent souvent par l'intermédiaire de l'Association des banquiers canadiens, mais elles n'ont aucune valeur parce qu'elles arrivent trop tard. Elles sont toujours lancées une semaine après que nous ayons été informés d'un stratagème.

Dans le sous-échantillon des répondants de la TI, les problèmes relatifs au signalement se doublaient aussi d'une comparaison avec les États-Unis. D'après un répondant :

> Les responsables de l'application de la loi ne sont d'aucun secours à ce chapitre. Nous devons leur fournir des renseignements, mais si un petit montant est en cause (moins de 100 000 $), ils ne sont pas disposés à donner suite. Comment savons-nous qu'ils ne souhaitent pas donner suite à ces affaires? Ils sont débordés et nous le font savoir. Aux États-Unis, les responsables de l'application de la loi sont davantage disposés à prêter main-forte pour de faibles montants. Question de capacité ou de connaissances? Ce n'est pas clair.

D'après des répondants, davantage de signalements sont faits à des organismes de réglementation comme la commission des valeurs mobilières, le Bureau de la concurrence et le Centre antifraude du Canada qu'à la police. Comme l'a expliqué un autre répondant, « aucune politique ne demande un signalement à la GRC, il y a seulement une pratique d'échange de renseignements avec d'autres entreprises. Toutes les principales sociétés d'appareils électriques canadiennes le font. » Le même répondant a comparé les pratiques américaines avec les canadiennes et fait remarquer que, au Canada, « on n'observe moins les lois et règlements qu'aux États-Unis. Ottawa ne réglemente pas autant l'industrie que les États-Unis. Là-bas, les banques et les sociétés cotées en bourse sont fortement réglementées. Notre gouvernement n'incite pas au signalement, celui-ci est plutôt facultatif. »

De plus, certaines banques et sociétés privées comptent une division de sécurité et s'occupent elles-mêmes de ces affaires. Dans d'autres cas, un signalement semblait occasionner un coût inutile à une entreprise. Au dire d'un répondant, « les technologies de sécurité sont coûteuses et la plupart des entreprises n'y consacrent pas l'argent qu'elles devraient au Canada. Résultat, il n'y a ni signalement ni recherche. » Parmi le sous-échantillon des répondants de la TI, la tendance au non-signalement n'était pas unanime; en fait, d'autres appuyaient totalement un système de

signalement obligatoire. Selon les propos d'un répondant, « le secteur privé adresse des reproches aux responsables de l'application de la loi, tandis que ceux-ci se plaignent de l'absence de signalement ».

À l'instar du sous-échantillon de la TI, lorsqu'on a demandé aux répondants de l'application de la loi quels étaient les principaux défis pour ce qui était d'évaluer la portée de la cyberfraude et le nombre de fraudeurs au Canada, ils ont affirmé que le manque d'éducation et d'échange de renseignements était au premier plan. Au sujet du signalement, ils semblaient conscients qu'une faible perte pouvait expliquer le sous-signalement de la cyberfraude. L'un des répondants a affirmé relativement aux données :

> Selon moi…, je ne sais pas…, je n'en ai pas la preuve, mais je crois que les gens ont tendance à déposer une plainte dans le cas d'une grosse perte. Leur nombre sera supérieur à ce qu'on pourrait prévoir, simplement parce que les gens qui perdent peu ne le signalent pas à la police, seulement à leur banque. La plupart du temps, les banques remboursent l'argent, de sorte qu'elles n'ont pas à signaler la perte à la police.

Par ailleurs, les motifs économiques de l'industrie pour ne pas signaler cette fraude ont été dévoilés par un répondant du sous-échantillon de l'application de la loi : « Si les banques ne [la signalent] pas, c'est peut-être parce qu'elles n'en souffrent pas, cela ne modifie pas leur résultat net. » Le même répondant a également commenté l'obligation pour les entreprises de renseigner le public :

> De grandes entreprises, par exemple les fournisseurs d'accès Internet (FAI), les banques ou même une agence comme INTERAC, pourraient mieux renseigner le public. Elles pourraient lancer plus souvent des alertes publiques de sécurité (notamment des annonces de services publics) pour rappeler aux gens que les banques ne leur envoient pas de courriels; tellement de gens sont victimes d'hameçonnage ou de détournement de domaine, sans se rendre compte que les grandes entreprises ne procèdent pas ainsi dans le cadre de leurs activités.

En fin de compte, il y a une énorme lacune dans les données sur la cyberfraude et la raison a été précisée par un répondant de l'application de la loi : « Environ 90 % des données sur les fraudes au Canada ne se retrouvent pas dans les bases de données policières; les banques sont informées, certains signalements sont communiqués à la police, tandis que d'autres sont simplement traités à l'interne ou carrément négligés. Il en va de même pour la fraude relative à la pension de retraite ou à l'invalidité; elle ne sort pas des organisations et n'est pas signalée à la police. »

Habituellement, les victimes individuelles sont trop embarrassées ou honteuses, ou jugent que leur faible perte ne justifie pas un signalement :

> Tous ne déposent pas plainte; dans le cas d'un vol d'identité, en particulier, les gens n'appellent pas la police. Beaucoup de cybercrimes ne sont pas signalés ou sont signalés seulement aux banques, qui, elles, ne les signalent pas à la police. Elles sont craintives et ne souhaitent ne pas ébruiter l'affaire; elles veulent protéger leur réputation et s'éviter toute publicité négative.

Pour ce qui est de mettre en commun renseignements et données, à l'instar des répondants du sous-échantillon de la TI, ceux de l'application de la loi ont semblé corroborer que ce serait une bonne pratique. L'un d'eux : « Les gens n'échangent pas assez leurs renseignements. Pas seulement les responsables de l'application de la loi; ceux des secteurs privé et public aussi. Le Royaume-Uni nous a appris qu'il est crucial d'échanger nos données sur les fraudes. » La présente recherche montre qu'on doit mieux éduquer les Canadiens à éviter eux-mêmes les différents stratagèmes de fraude. Le gouvernement du Canada, les banques et les FAI doivent assumer une plus grande responsabilité à ce chapitre. Il devrait y avoir davantage d'alertes publiques à leur sujet (par exemple des messages d'intérêt public) pour instruire les gens, de sorte qu'ils ne deviennent pas victimes des stratagèmes d'hameçonnage.

L'un des principaux objets de frustration mentionnés, c'est que les incidents de cyberfraude sont signalés à de nombreux corps policiers au Canada. La GRC ainsi que les corps de police municipaux et des provinces de tout le pays reçoivent tous des renseignements sur des cyberfraudes. Or on semble peu se soucier de rapprocher ces renseignements. Beaucoup semblent être conservés à l'interne et n'être communiqués à aucun organisme extérieur. Beaucoup de corps de police municipaux ne signalent pas les incidents de cyberfraudes au Centre antifraude du Canada ni à aucune autre entité. Bien que les délinquants violents et à risque élevé soient signalés par l'intermédiaire de la GRC, le signalement n'est pas obligatoire dans le cas de la cyberfraude. De plus, bon nombre de responsables de l'application de la loi se sont dits frustrés de la façon dont les données statistiques sont consignées dans la Déclaration uniforme de la criminalité. À leur dire, le système de consignation de cette déclaration manque de précision concernant la cyberfraude et, plus généralement, la cybercriminalité. Les données sur la cyberfraude sont regroupées sous la rubrique de la fraude, et rien ne permet de déterminer le genre de stratagème frauduleux utilisé dans chaque incident. Cela signifie qu'on perd de l'information qui pourrait être précieuse pour mieux comprendre la cyberfraude.

9.2.6 Suggestions relatives aux sources de données et solutions aux problèmes actuels

L'une des tendances marquantes dégagées dans le sous-échantillon des répondants de la TI visait à rendre obligatoires le signalement des incidents de cyberfraude et l'adoption d'une technique standard pour recueillir les données. Comme l'a observé l'un des répondants, « J'estime que le gouvernement emprunte la bonne voie en créant des bureaux de la GRC et en demandant aux gens de signaler ces incidents à la GRC; mais il faut faire davantage. Lorsque notre secteur d'activité est visé par une attaque, nous devons nous en informer mutuellement et il est très utile de disposer d'un cadre fédéral pour le faire. »

De plus, les répondants de la TI ont énoncé la nécessité d'échanger des renseignements dans le secteur de la sécurité TI et souhaité que le gouvernement participe aux tentatives de combattre la cybercriminalité. Le répondant de ce sous-échantillon a développé ainsi ses éléments :

> On doit disposer d'un mécanisme pour communiquer des renseignements et en faire part à d'autres membres du secteur; ce serait très utile. Ailleurs, il existe de bons exemples de tels mécanismes, notamment dans le secteur nucléaire et le contrôle de la

> circulation aérienne. Nous avons besoin de politiques et de règlements pour faire observer un tel signalement. C'est toujours plus facile avec une entité publique; c'est facile alors de faire observer une obligation, de mettre en commun des renseignements, d'atténuer des risques; mais les banques et les entreprises de télécommunications ne sont pas dans la même position. Elles craignent de perdre des clients. [Dans l'industrie électrique,] nous bénéficions d'un monopole en ce qui concerne la clientèle. Je constate qu'il n'y a pas de partenariat semblable dans le secteur privé, notamment parmi les banques.

D'autres répondants ont réclamé une accréditation en TI, des modèles de signalement standardisés ainsi qu'un leadership gouvernemental pour que soient adoptés les modèles en usage aux États-Unis. D'après l'un des répondants de la TI : « Nous avons besoin que le gouvernement du Canada fasse preuve de détermination; nous voyons que des unités de lutte à la cybercriminalité se créent aux États-Unis, et l'idéal serait que nous faisions la même chose. Je serais favorable au signalement obligatoire; on doit suivre l'exemple américain. »

Lorsqu'on a demandé à ces répondants ce qu'il faudrait faire à leur avis pour accroître le signalement, nombre d'entre eux ont maintenu que l'éducation et la sensibilisation sont essentielles. Autrement dit, les Canadiens doivent apprendre ce qu'est la cyberfraude et à qui la signaler. L'un des répondants : « Différentes possibilités s'offrent à nous en matière de signalement : les autorités d'application de la loi municipales, provinciales ou fédérales; PhoneBusters; des organisations fédérales s'occupant des questions reliées à la cybercriminalité. Mais qui devrait recevoir le signalement? Ce n'est pas clair. » Autrement dit, beaucoup ne savent pas quoi faire lorsqu'ils reçoivent un courriel frauduleux, encore moins à qui le signaler. Aspect plus positif, toutefois, la plupart des répondants de la TI ont affirmé que, bien que toutes les entreprises ne soient pas disposées à coopérer avec la police, on doit absolument faire preuve d'une plus grande ouverture et d'une meilleure volonté pour ce qui d'informer la police. Selon l'un deux :

> Règle générale, l'information dont nous disposons est principalement axée sur les États-Unis; nous sommes largement entourés d'entreprises américaines. Je ne connais aucune source d'information proprement canadienne (p. ex. concernant les tendances ainsi que les activités ou renseignements au sujet de fraudes) dans laquelle les gens vont verser d'eux-mêmes des données sur une fraude portée à leur connaissance. Si nous disposions d'une source canadienne, ce serait extrêmement utile… pour savoir quel types de fraudes sont perpétrées chez nous, pour obtenir des données propres aux secteurs de notre pays, pour comprendre quelles mesures de protection nous devrions adopter.

Nombre de répondants de la sécurité de la TI étaient fermement convaincus qu'on doit échanger plus efficacement les renseignements relatifs à la cyberfraude et la cybersécurité d'une façon générale entre les différents secteurs d'activité au sein d'un réseau fermé de participants. Le processus d'échange de renseignements « est utile et rassurant. C'est utile de savoir qu'on ne vient pas en tête de liste et qu'on n'est pas ciblé. » Dans l'ensemble, les répondants ont considéré qu'un organisme canadien était nécessaire pour consigner les cyberfraudes et diffuser des renseignements à leur sujet. Ils se sont dits très enthousiastes à l'idée d'un mécanisme qui obligerait à signaler régulièrement les cyberfraudes; un organisme gouvernemental, qui

recueillerait les renseignements, puis les rendrait publics. Cependant, on a laissé entendre que la collecte de données devrait être anonyme. Et aussi que ce genre de mécanisme de signalement et de mise en commun de renseignements serait le bienvenu, étant donné la méconnaissance de la cyberfraude au Canada.

> Nous avons besoin de statistiques canadiennes, de davantage de recherche… Telus, Deloitte et TPC effectuent chaque année de bonnes enquêtes sur la fraude et le respect de la vie privée. Les gens peuvent remplir un sondage en ligne. Telus le fait depuis longtemps. Chaque année, je suis invité à participer à un groupe pour discuter des questions à poser. Ces sondages nous sont très utiles : ils nous fournissent des repères et nous révèlent la tendance en gestion de la sécurité de la TI.

Dans le secteur de l'énergie, des statistiques sur la cybersécurité, y compris la cyberfraude, sont régulièrement communiquées à l'agent de liaison de la GRC à Ottawa, puis diffusées aux sociétés d'appareils électriques. Tout en ayant à l'esprit que ce réseautage serré est parrainé et mis en œuvre dans le cadre de l'initiative fédérale sur la protection des infrastructures essentielles, nous pourrions nous en servir comme prototype efficace contre la cyberfraude (c.-à-d. bénéficier de divers canaux à Ottawa pour recueillir des données statistiques sur la cyberfraude provenant de représentants des différents secteurs d'activité, puis pour diffuser le résultat aux divers intervenants du secteur). Ce genre d'initiative a obtenu beaucoup de faveur, un répondant affirmant : « qu'il est nécessaire d'obtenir des renseignements propres à chaque secteur ainsi que de tenir des réunions pour se renseigner et collaborer en matière de pratiques exemplaires. Un mécanisme permettant de prendre part à quelque chose du genre serait utile. »

À la question *Comment mieux évaluer la cyberfraude au Canada?*, les répondants de l'application de la loi ont formulé certaines suggestions intéressantes. Celles-ci tournaient autour de thèmes communs : argent et ressources; Déclaration uniforme de la criminalité; nécessité de stimuler le signalement et l'échange de renseignements sur la cyberfraude; enfin, création d'un carrefour national de données doté d'une banque de données perfectionnée qui évaluerait la cyberfraude et ferait le suivi des incidents au Canada.

Concernant les questions d'argent et de ressources, les répondants de l'application de la loi ont surtout souligné le besoin d'un plus grand nombre d'agents de police pour s'occuper de la cyberfraude, particulièrement au niveau municipal et dans la rue. De plus, certains répondants ont suggéré au gouvernement fédéral d'attribuer davantage d'argent à l'échelon municipal pour s'occuper de ces problèmes, parce que ceux-ci comportent des volets qu'on peut estimer être liés à la sécurité nationale. Il s'agit actuellement d'un phénomène s'étendant à tout le pays et, a-t-on rapporté, les fraudeurs transfèrent leurs activités depuis les grandes agglomérations urbaines vers le milieu rural du Canada. D'autres répondants renchérissent : des intervenants en sécurité de la TI doivent œuvrer dans les secteurs ruraux aussi bien que dans les grandes villes du pays. Par ailleurs, la présente recherche montre clairement que la police canadienne ne peut donner suite à toutes les plaintes de fraude, particulièrement lorsque les fraudeurs se trouvent à l'étranger ou opèrent à partir d'un compte anonyme ou encore lorsqu'elle doit obtenir des renseignements d'un fournisseur de messagerie ou d'accès Internet d'en dehors du Canada.

La recherche a révélé en outre que les organismes d'application de la loi doivent échanger davantage leurs renseignements entre eux sur la cyberfraude. Selon les répondants de ce sous-groupe, on pourrait également exiger des grands FAI, mais aussi de l'industrie privée, qu'ils dévoilent l'information qu'ils possèdent sur la cyberfraude. La relation entre l'échange de renseignements et la disponibilité des ressources a été résumée ainsi par un répondant du sous groupe :

> Des groupes mixtes venant de la police, des banques et des entreprises privées sont nécessaires pour un échange de renseignements. Ce genre de relations est intéressant; ce peut être un moyen de mieux connaître le problème. Cependant, on doit garantir l'anonymat. C'est à l'avantage de tous que de garantir l'anonymat.

On s'est dit également favorable à l'idée de créer un mécanisme par lequel les intervenants des secteurs tant privé que public pourraient anonymement dévoiler leurs pertes par fraude à une source centrale. Au dire d'un répondant, « il faut joindre les gens par Internet. C'est la façon la plus simple de les sonder. Il faut accroître les communications interorganismes dans tout le pays; nous devons encourager et favoriser cela. Nous avons besoin de liens d'un bout à l'autre du Canada. »

Par ailleurs, on a semblé très désireux de trouver le moyen d'obliger les corps policiers du pays à mettre en commun leurs renseignements sur la cyberfraude et de déterminer si des groupes ciblent de nombreuses villes. D'après la présente recherche, le gouvernement du Canada tirerait profit d'une stratégie nationale visant à recueillir anonymement des données auprès des agents de police, des banques ainsi que d'entités des secteurs privé et public concernant la cyberfraude. Cela revient à encourager les corps de police à communiquer entre eux et à persuader l'industrie à signaler ses pertes réelles. Les répondants appuient fortement le signalement obligatoire. L'un d'entre eux :

> À mes yeux, si les entreprises étaient obligées de signaler les cyberfraudes, cela aiderait. Il y a eu des cas où un serveur entier a été mis en panne et personne n'en a rien su. Selon moi, la législation antipourriel entrée en vigueur récemment (projet de loi C-28) devrait venir en aide aux Canadiens, mais la majorité des pourriels proviennent de l'étranger.

Selon le sous-groupe d'application de la loi, Statistique Canada doit trouver une nouvelle façon d'évaluer les données policières sur la cyberfraude recueillies grâce à la Déclaration uniforme de la criminalité, car les catégories ne reflètent pas adéquatement les changements survenus dans la société et la criminalité au cours des dix dernières années. Actuellement, une fois les données dénombrées, rien ne permet de les ventiler par type de fraude, p. ex. marketing de masse ou stratagème 419; par conséquent, les résultats ne sont pas aussi utiles à la police qu'ils pourraient l'être autrement.

Il a été question de créer une banque de données centrale qui servirait à enregistrer et à évaluer celles qui se rapportent à la cyberfraude de tout le Canada. Mais également à mener des enquêtes ou des sondages en ligne auprès de Canadiens pour recueillir des renseignements à ce sujet. À l'heure actuelle, les différents corps policiers canadiens ont chacun leur manière de recueillir leurs données et de tenir leurs dossiers; beaucoup ne consignent pas les seules plaintes, préférant

assurer le suivi des seuls incidents menant à une enquête officielle. Il serait plus efficace de créer un organisme central pour recueillir et compiler les données. Les corps policiers seraient assurés d'une meilleure communication sur la cyberfraude, parce qu'un tel organisme pourrait transmettre les renseignements pertinents aux différents organismes chargés de l'application de la loi partout au Canada. Disposer d'une banque de données centrale sur les cyberfraudes et les cyberfraudeurs connus de tout le pays aiderait aussi à identifier des suspects dans des affaires de cette nature et permettrait aux chercheurs de relever et d'évaluer les différents types d'incidents qui se produisent couramment.

Aux yeux des répondants, il serait avantageux de créer un mécanisme national qui recueillerait les données et suivrait efficacement les signalements de cyberfraude. Vu que la plupart des renseignements sur ce genre de fraude sont soit acheminés vers différentes organisations, notamment des banques, des organismes de réglementation ou divers corps policiers, soit simplement non consignés, il faudrait des unités du renseignement qui transmettraient l'information à un organisme national capable de compiler toutes les informations sur la cyberfraude dans une banque de données centrale.

10.0 Conclusion et recommandations

Les enjeux et les préoccupations soulevés dans le présent rapport doivent être considérés de façon cyclique. Le fait que les victimes (particuliers, entreprises, gouvernements) s'abstiennent de signaler les incidents de cyberfraude dont elles ont été la cible signifie que de nombreux cas ne sont pas consignés dans les statistiques criminelles. Par conséquent, les organismes d'application de la loi ne reçoivent pas suffisamment de ressources dans ce domaine, car le nombre réel de victimes de cyberfraude n'est ni consigné ni mesuré. Les répondants estiment que l'on n'accorde peu d'importance à la cyberfraude étant donné que l'on ne dispose pas des ressources nécessaires pour intervenir. Il arrive à l'occasion que des services de police doivent renoncer à aider des victimes de cyberfraude, car ils ne possèdent pas suffisamment de ressources pour traiter les plaintes. Les particuliers et les entreprises sont donc frustrés et refusent de demander de l'aide aux responsables de l'application de la loi ou de signaler officiellement la cyberfraude dont ils ont été victimes.

Bon nombre de répondants ont également ajouté qu'il faudrait établir un processus mieux défini et créer une seule entité qui sera responsable de recueillir les renseignements liés à la cyberfraude. À l'heure actuelle, on peut signaler la cyberfraude à un trop grand nombre d'intervenants différents (les services de police municipaux, provinciaux et fédéraux ainsi que le Centre antifraude du Canada) et il n'est pas établi clairement qui est l'organisation responsable de la collecte de ce type de renseignements. Les répondants ont également recommandé de mettre au point une procédure permettant de signaler les incidents de façon anonyme à un seul organisme. Les renseignements sur la cyberfraude semblent être une source de préoccupation pour les deux groupes de répondants. Le manque de formation pour les responsables de l'application de la loi et le personnel de la TI semble également être un enjeu. Comme l'a indiqué un répondant du sous-échantillon du personnel de la TI, il serait utile de mettre sur pied un organisme d'accréditation (enquêteurs TI du secteur privé), car on a besoin d'une structure de gouvernance, une organisation professionnelle, pour assurer la sécurité de la TI.

Le personnel de la TI et les responsables de l'application de la loi ont confirmé les soupçons à savoir que les particuliers et les entreprises risquent de ne pas signaler la cyberfraude dont ils ont été victimes, soit parce qu'ils sont embarrassés, soit pour d'autres raisons. Même si l'on peut observer des tendances, de nombreux résultats étaient ambivalents. C'est d'ailleurs ce que l'on peut observer dans les sous-échantillons. Par exemple, les participants du sous-échantillon de la TI (à l'exception d'une minorité de répondants de la TI) et des responsables de l'application s'entendent pour dire qu'il existe peu d'information sur la cyberfraude au Canada et qu'il faut prendre des mesures pour remédier à la situation.

Les répondants croient qu'il faut adopter de nouvelles mesures stratégiques pour centraliser la collecte de données. Les sous-échantillons de la TI et des responsables de l'application de la loi ont suggéré d'avoir recours à des sondages anonymes pour obtenir des données auprès des particuliers et des entreprises qui n'ont pas signalé la cyberfraude parce qu'ils étaient embarrassés. En ce qui concerne les entreprises, il existe également un soutien pour le signalement obligatoire. Selon certains répondants du sous-échantillon des responsables de l'application de la loi, la normalisation des procédures de signalement dans l'ensemble des organismes de l'application de loi permettrait de combler les lacunes actuelles liées à la Déclaration uniforme de la criminalité. Les répondants ont ajouté que l'absence d'information nuit à la collecte des données et qu'il est essentiel de sensibiliser le public à la situation.

Afin de mesurer l'importance de la cyberfraude au Canada et la façon selon laquelle elle risque de changer l'avenir, il faut recueillir des éléments de preuve pour consigner la portée du problème. Bien que certains délinquants commettent leurs méfaits à partir du Canada, on constate que de nombreux auteurs de cyberfraude se trouvent dans d'autres pays. Certains éléments de preuve indiquent que des groupes du crime organisé seraient impliqués dans la cyberfraude et le blanchiment de biens illicites à l'échelle transnationale. L'économie clandestine ne cesse de gagner en maturité sur le marché international; on peut acheter des compétences techniques et des données qui permettront de mener des attaques précises. Symantec signale que les pirates novices peuvent facilement compromettre la sécurité des ordinateurs et voler des données en se procurant des trousses de codes ou de logiciels criminels, que l'on trouve largement dans l'économie clandestine (Symantec 2010, p. 11). Afin de déterminer dans quelle mesure un secteur d'activités ou des consommateurs particuliers sont touchés par la cyberfraude au Canada à partir de données limitées, il faut mettre en place une approche beaucoup plus perfectionnée que celle qui est fréquemment utilisée.

En raison du manque de connaissances générales sur les réseaux criminels impliqués dans la cyberfraude, il semblerait que la meilleure source d'informations supplémentaires sur la cyberfraude soit la communauté des fraudeurs. Ce type d'information aiderait à découvrir la structure d'un réseau caché et permettre d'identifier les intervenants clés au sein du groupe. Afin de recueillir des données préliminaires sur la cyberfraude, on pourrait estimer le nombre de membres de cette population clandestine en employant des techniques normalisées en matière d'estimation de données mentionnées précédemment. Parmi les options disponibles pour mettre au jour cette population clandestine, un modèle tronqué de Poisson semble le plus efficace. Ce modèle contribuerait à régler un grand nombre des problèmes auxquels sont confrontés les responsables de l'application de la loi qui ont donné lieu à l'absence de rapports et aux défis liés à la tenue d'enquête sur la cyberfraude et à sa prévention.

En résumé, les recommandations suivantes pourraient s'avérer extrêmement efficaces pour lutter contre la cyberfraude au Canada :

- On doit mieux éduquer les Canadiens à éviter eux-mêmes les différents stratagèmes de fraude. Le gouvernement du Canada, les banques et les FAI doivent assumer une plus grande responsabilité à ce chapitre. Il devrait y avoir davantage d'alertes publiques à leur sujet (par exemple des messages d'intérêt public) pour instruire les gens, de sorte qu'ils ne deviennent pas victimes des stratagèmes d'hameçonnage.
- De nouvelles initiatives, notamment créer une base de données en ligne des pratiques exemplaires que pourraient enrichir et consulter ces experts, mettre en place une communauté en ligne (p. ex. pour faire part de conseils et d'astuces) ou tenir des séances ou conférences d'information sur ces pratiques exemplaires pour chaque secteur d'activité, permettraient de contrer de façon proactive les menaces de cyberfraude et aussi de recueillir des renseignements fiables sur les menaces et les vulnérabilités existantes.
- Le gouvernement du Canada tirerait profit d'une stratégie nationale visant à recueillir anonymement des données auprès des agents de police, des banques ainsi que d'entités des secteurs privé et public concernant la cyberfraude. Cela revient à encourager les corps de police à communiquer entre eux et à persuader l'industrie à signaler ses pertes réelles. Les répondants appuient le signalement obligatoire de la cyberfraude et ils préconisent l'adoption d'une méthode normalisée de collecte de données. Les répondants ont également réclamé une accréditation en TI, des modèles de signalement normalisés ainsi qu'un leadership gouvernemental pour que soient adoptés les modèles en usage aux États-Unis.
- On a besoin d'un plus grand nombre d'agents de police pour s'occuper de la cyberfraude, particulièrement au niveau municipal et dans la rue. De plus, certains répondants ont suggéré au gouvernement fédéral d'attribuer davantage d'argent à l'échelon municipal pour s'occuper de ces problèmes, parce que ceux-ci comportent des volets qu'on peut estimer être liés à la sécurité nationale. Il s'agit actuellement d'un phénomène s'étendant à tout le pays et, a-t-on rapporté, les fraudeurs transfèrent leurs activités depuis les grandes agglomérations urbaines vers le milieu rural du Canada. D'autres répondants renchérissent : des intervenants en sécurité de la TI doivent œuvrer dans les secteurs ruraux aussi bien que dans les grandes villes du pays.
- Statistique Canada doit trouver une nouvelle façon d'évaluer les données policières sur la cyberfraude recueillies grâce à la Déclaration uniforme de la criminalité, car les catégories ne permettent pas d'analyser les types de cyberfraude.
- Il a été question de créer une banque de données centrale qui servirait à enregistrer et à évaluer celles qui se rapportent à la cyberfraude de tout le Canada. Mais également à mener des enquêtes ou des sondages en ligne auprès de Canadiens pour recueillir des renseignements à ce sujet. Il serait avantageux de créer un mécanisme national qui recueillerait les données et suivrait efficacement les signalements de cyberfraude.

La cybercriminalité peut traverser les frontières et les activités d'un délinquant donnent souvent lieu à la perpétration d'un crime dans plusieurs pays simultanément. C'est pourquoi il est important d'atteindre les objectifs suivants à l'échelle internationale :

- harmonisation des infractions substantielles commises à l'aide d'un ordinateur dans les lois nationales;
- harmonisation des dispositions de procédure liées aux enquêtes sur les crimes informatiques et la poursuite en juste de leurs auteurs;
    - mise en place de mesures de collaboration qui faciliteront la communication d'éléments de preuve et d'information ainsi que l'extradition de suspects (Schjolberg, 2008, p. 1).

Des ressources sont également nécessaires pour veiller à ce que les tribunaux soient en mesure de saisir des cas intergouvernementaux complexes de fraude.

BIBLIOGRAPHIE

Albanese, J. S. (2005). « Fraud: The Characteristic Crime of the Twenty-First Century », *Trends in Organized Crime,* vol. 8, n° 4, p. 6-14.

Loi modifiant le Code criminal (vol d'identité et inconduites connexes)
Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, ch.5.

Begin, N. N. Dezhkam, R. Etges et W. Hejazi (2010a). « Managing the risk of social networking: Additional findings and analysis from the 2010 Rotman-TELUS Joint Study on Canadian IT Security Practices », Toronto, Telus Security Solutions.

– – – ., Dezhkam, N., R. Etges et W. Hejazi (2010b). « 2010 Executive Briefing - Rotman-Telus Joint Study on Canadian IT Security », Toronto, Telus Security Solutions.

Berg, S. (2009). « Identity Theft Causes, Correlates and Factors: A Content Analysis », Crimes of the Internet, Frank Schmalleger et Michael Pittaro (éditeurs), Upper Saddle River, NJ, Pearson Education Inc.

Hache, B., A. Carolina, et N. Ryder (2011). « Tis the Season to (Be Jolly?) Wise-up to Online Fraudsters. Criminals on the Web Lurking to Scam shoppers this Christmas: A Critical Analysis of the United Kingdom's Legislative Provisions and Policies to Tackle Online Fraud », *Information & Communications Technology Law,* vol. 20, n° 1, p. 35-56.

B¨ohning, D., B. Suppawattanabodee, W. Kusolvisitkul et C. Viwatwongkasem (2004). « Estimating the Number of Drug Users in Bangkok 2001: A Capture-Recapture Approach Using Repeated Entries in One List », *European Journal of* Epidemiology, vol. 19, p. 1075-1083.

Bouchard, M. (2007). « A Capture–Recapture Model to Estimate the Size of Criminal Populations and the Risks of Detection in a Marijuana Cultivation Industry », *Journal of Quantitative Criminology,* vol. 23, p. 221-241.

– – – . et P. Tremblay, (2005). « Risks of Arrest Across Markets: a Capture–Recapture Analysis of 'Hidden'Dealer and User Populations », *Journal of Drug Issues,* vol. 34, p. 733-754.

Brecht, M-L. et T.D. Wickens (1993). « Application of Multiple-Capture Methods for Estimating Drug Use Prevalence, *Journal of Drug Issues,* vol. 23, p. 229-250.

Brenner, S. W. (2002). « Organized Crime? How Cyberspace May Affect the Structure of Criminal Relationships », *North Carolina Journal of Law and Technology,* vol. 4, no 1, p. 1-50.

Calkins RF, GB Atkan. (2000) « Estimation of Heroin Prevalence in Michigan Using Capture-Recapture and Heroin Problem Index Methods », *Journal of Drug Issues,* vol. 30, p. 187-204.

Campbell, D. S. (2002). « Focus on Cyberfraud » *Internal Auditor*, février, p. 28-33.

Canada. Service canadien de renseignements criminels (SCRC). (2010). « Rapport sur le crime organisé 2010 ». Ottawa, SCRC.

– – – . (2005). Centre canadien de la statistique juridique. « Rapport sur la faisabilité d'améliorer la mesure de la fraude au Canada ». Ottawa, ministre de l'Industrie.

Canadian Anti-Fraud Centre (2010). « Annual Statistical Report 2010 - Mass Marketing Fraud and ID Theft Activities ». Sur Internet : http://www.antifraudcentre-centreantifraude.ca (consulté le 19 avril 2011).

Association des banquiers canadiens (ABC). (2011). « Statistiques ». Sur Internet : http://www.cba.ca/fr/component/%20content/publication/69-statistics (consulté le 9 avril 2011).

Chawki, M. (2009). « Nigeria Tackles Advance Fee Fraud », *Journal of Information, Law and Technology 1.* Sur Internet : http://go.warwick.ac.uk/jilt/2009_1/chawki (consulté le 9 avril 2011).

Chellappa, R.K. et R. Sin (2005). « Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma », *Information Technology and Management*, vol. 6, n^{os} 2-3, p. 181-202.

Choi, Y. et C. Comiskey (2003) « Methods for Providing the First Prevalence Estimates of Opiate Use in Western Australia », *International Journal of Drug Policy,* vol. 14, p. 297-305.

Choo, K.K.R., (2008). « Organized Crime Groups in Cyberspsace: A Typology », *Trends in Organized Crime,* vol. 11, n^{o} 3, p. 270-295.

Collins MF, Wilson RM (1990) « Automobile Theft: Estimating the Size of the Criminal Population », *Journal of Quantitative Criminology,* vol. 6, p. 395-409.

Controlling the Assault of Non-Solicited Pornography and Marketing Act and Telephone Consumer Protection Act (the "CAN-SPAM Act), 18 U.S.C. § 1037.

Crimes Legislation Amendment (*Telecommunications Offences and Other Measures) Act* (*No. 2*) *2004*. No. 127, 2004.

Code criminel du Canada L.R.,1985, ch. C-46.

Cukier, W. and Levin, A. (2009) « Internet Fraud and Cyber Crime », Crimes of the Internet. Frank Schmalleger et Michael Pittaro (éditeurs), Upper Saddle River, NJ, Pearson Education Inc.

Cybercrime Act 2001 No. 161, 2001.

David, F.N., et N.L. Johnson (1952). « The Truncated Poisson Distribution », *Biometrics,* vol. 8, n° 4, p. 275-285.

Davis, E. S. (2003). « A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft ». Sur Internet : http://law.wustl.edu/Journal/12/p201%20Davis.pdf. (consulté le 19 avril 2011).

Dhamija, R., Tygar, J.D. et M. Hearst, M. (2006). « Why Phishing Works », CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Special Interest Group on Computer-Human Interaction.

Deloitte. (2010a). « Cyber Crime: A Clear and Present Danger: Combating the Fastest Growing Cyber Security Threat », New York, Deloitte Development LLC.

– – – . (2010b). « 2010 TMT Global Security Study – Key Findings – Bounce Back », New York, Deloitte Development LLC.

Etges, R., and Sutcliffe, E. (2008). « An Overview of Transnational Organized Cybercrime » *Information Security Journal: A Global Perspective,* vol. 17, p. 87.

Everett, C. (2003). « Credit Card Fraud Funds Terrorism », *Computer Fraud and Security*, mai, p. 1-20.

Federal Trade Commission Act (15 U.S.C. §§ 41-58, as amended).

Gabrosky, P. (2006). « Editor's Postscript », *Crime, Law, Social Change,* vol. *46*, p. 275-276.

Gordon, S. et R. Ford (2006). « On the Definition and Classification of Cybercrime », *Journal in Computer Virology,* vol. *2*, p. 13-20.

Gottschalk, P. (2010). « Knowledge Management Technology for Organized Crime Risk Assessment », *Information Systems Frontiers,* vol. 12, p. 267-275.

Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (12 novembre 1999).

Hilley, S. (2006). « The Shadowcrew – Organized, Yes, but 'Organized Crime'? », *Infosecurity Today,* vol. 3, n° 1. p. 10.

Hejazi,W., A. LeFort, R. Etges, B. Sapiro (2010). « The 2009 Rotman-TELUS Joint Study on IT Security Best Practices: Compared to the United States, How Well is the Canadian Industry Doing? », Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications, T. Holt, B. Schell (éditeurs), Hershey, PA, IGI Global.

Hickman, M., S. Cox, J. Harvey, S. Howes, M. Farrell, M. Frischer, G. Stimson, C. Taylor, K. Tilling, (1999). « Estimating the Prevalence of Problem Drug Use in Inner London: A Discussion of Three Capture–Recapture Studies », *Addiction* vol. 94, p. 1653-1662.

Howard, R. (2009). Cyber Fraud: Tactics, Techniques and Procedures. Boca Raton, FL: Auerbach Publications.

Hser Y. (1993). « Population Estimation of Illicit Drug Users in Los Angeles County », *J Drug Issues* vol. 23, p. 323-334.

Huey, L. et Rosenberg, R.S. (2004). « Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention », *Revue canadienne de criminologie et de justice pénale*, vol. 46, p. 597-631.

Identity Theft and *Assumption Deterrence Act*, Pub. L. No. 105-318, 112 Stat. 3007 (30 octobre 1998).

Ipsos Reid, (2009). « CSA Investor Index 2009 », Prepared for Canadian Securities Administrators Investor Education Committee, Ottawa, Ipsos Reid.

Kendall, L.W. (1999). « Robustness of Closed Capture–Recapture Methods to Violations of the Closure Assumption », Ecology, vol. 80, p. 2517-2525.

King, A. et Thomas, J. (2009). « You Can't Cheat An Honest Man: Making ($$$ and) Sense of the Nigerian Email Scams », Crimes of the Internet, Frank Schmalleger, Michael Pittaro. Upper Saddle River, NJ, Pearson Education Inc.

Kowalski, M. (2002). « Cybercriminalité : enjeux, sources de données et faisabilité de la collecte de recueillir des données auprès de la police ». Ottawa, ministre de l'Industrie.

Lee, B., H. Cho, M. Chae, S. Shim (2010). « Empirical Analysis of Auction Fraud: Credit Card Phantom Transactions », *Expert Systems with Applications,* vol. 37, p. 2991-2999.

Levi, M. and Burrows, J. (2008). « Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey », *British Journal of Criminology,* vol. 48, p. 293-318.

– – – . et M. H. Fleming, M Hopkins, avec l'aide de K. Matthews (2007). « The Nature, Extent and Economic Impact of Fraud in the UK », Report for the Association of Chief Police Officers' Economic Crime Portfolio. Sur Internet : http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.108.8217&rep=rep1&type=pdf. (consulté le 19 avril 2011).

Li, X. (2007). « International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene », *Webology,* vol. 4, n° 3, p. 1-45.

Longe, O.B., F. Wada, A. Anadi, C. Jones, C. et V. Mbarika (2010). « Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities », *International Journal of Computer Science and Information Security,* vol. 6, n° 3, p. 124-135.

Malm, A. et G. Bichler (sous presse). « Networks of Collaborating Criminals: Assessing the

Structural Vulnerability of Drug Markets ».

McAfee. (2010a). « A Good Decade for Cybercrime: McAfee's Look Back at Ten Years of Cybercrime », Santa Clara: McAfee Inc.

– – – . (2010b). « 2010 Threat Predictions », Santa Clara, McAfee Inc.

Menn, J. (2010). Fatal System Error – The Hunt for the New Crime Lords Who are Bringing Down the Internet, New York, PublicAffairs.

Microsoft (2005). « Tool Thwarts Online Predators ». Sur Internet : http://www.microsoft.com/presspass/features/2005/apr05/04-07CETS.mspx. (consulté le 7 avril 2011).

Morselli, C., Gabor, T. et Kiedrowski, J. (2010). « Les facteurs qui façonnent le crime organisé », préparé pour la Division de la recherche et de la coordination nationale sur le crime organisé, Secteur de la police et de l'application de la loi, Sécurité publique Canada.

Morselli, C. (2009). *Inside Criminal Networks*, New York, Springer.

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité (2002). Sur Internet : http://www.oecd.org/document/48/0,3746,fr_2649_34255_15584624_1_1_1_1,00.html.

O'Neill, M. (2000). « Old Crimes New Bottles: Sanctioning Cybercrime », *George Mason Law Review,* vol. 9, p. 237-241.

Paget, F. (2009). « Financial Fraud and Internet Banking: Threats and Countermeasures », Santa Clara, McAfee Inc.

Panda Security (2010). « The Cyber-Crime Black Market: Uncovered », Markham, Ontario, Panda Security.

Riccio, L.J., R. Flinkestein (1985). « Using Police Arrest Data to Estimate the Number of Burglars Operating in a Suburban County », *Journal of Criminal Justice,* vol. 13, p. 65-73.

Rider, P.R. (1953). « Truncated Poisson Distributions », *Journal of the American Statistical Association,* vol. 48, n° 264, p. 826-830.

Roberts, J.M., et D.D Brewer (2006). « Estimating the Prevalence of Male Clients of Prostitute Women in Vancouver with a Simple Capture–Recapture Method », *Journal of the Royal Statistical Society Series A,* vol. 169, p. 1-12.

Rossmo, D.K., et R. Routledge (1990). « Estimating the Size of Criminal Populations », *Journal of Quantitative Criminology,* vol. 6, p,. 293-314.

Gendarmerie royale du Canada (GRC). « La GRC, le service de police de Toronto et les organismes canadiens chargés de l'application de la loi s'unissent pour lutter contre l'exploitation sexuelle des enfants en ligne – Le président de Microsoft Canada, David Hemler, et les services nationaux de

police participent au lancement du Système d'analyse contre la pornographie juvénile », Sur Internet : http://www.rcmp-grc.gc.ca/news /2005/n_0510_f.htm. [consulté le 19 2011].

Schjolberg, S. (2008). « The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva ». Sur Internet : http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. [consulté le 19 avril 2011).

Schwarz, C. J. et G. A. F. Seber (1999), « A Review of Estimating Animal Abundance. III. », *Statistical Science,* vol. 14, p. 427-456.

Sheehan, K.B. and M.G. Hoy, (2000). « Dimensions of Privacy Concern Among Online Consumers », *Journal of Public Policy and Marketing,* vol. 19, n° 1, p. 63-73.

Smit, F., J. Toet, et P. van der Heijden (1997). « Estimating the Number of Opiate Users in Rotterdam Using Statistical Models for Incomplete Count Data In European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), 1997 Methodological Pilot Study of Local Prevalence Estimates ». EMCDDA, Lisbonne.

Smith, R. G. (2008). « Coordinating Individual and Organizational Responses to Fraud », *Crime, Law and Social Change,* vol. 49, p. 379-396.

– – – . et Gregor Urbas. (2001). « Controlling Fraud on the Internet: A CAPA Perspective: Report for the Confederation of Asian and Pacific Accountants, Research and Public Policy Series No. 39. », Canberra, Australian Institute of Criminology.

Spam Act 2003. Act No. 129 of 2003, as amended.

Spiekermann, S., J. Grossklags et B. Berendt (2002). « E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior », Proceedings of the Third AMC Conference on Electronic Commerce, p. 38-47.

Stroik, A. et W. Huang (2009). « Nature and Distribution of Phishing », Crimes of the Internet, Frank Schmalleger et Michael Pittaro, Upper Saddle River, NJ, Pearson Education Inc.

Symantec, (2010). « Symantec Global Internet Security Threat Report: Trends for 2009 », Mountain View, CA, Symantec Corporation.

– – – .(2009). « Symantec Report on Rogue Security Software », juillet 2008-juin 2009, Mountain View, CA, Symantec Corporation.

– – – .(2008). « Symantec Report on the Underground Economy », juillet 2007-juin 2008. Mountain View, CA, Symantec Corporation.

Taylor-Butts, A., et S. Perreault (2008). « Les fraudes contre les entreprises au Canada : résultats d'une enquête nationale », Ottawa, Statistique Canada.

The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.

Conseil de l'Europe. *Convention sur la cybercriminalité*, Budapest, 23.X1.2001. Sur Internet : http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm.

The Fair and Accurate Credit Transactions Act of 2003, Pub.L. p. 108-159.

*The Fair Credit Reporting Act***,** 15 U.S.C. § 1681 et seq.

The Fraud Act 2006 (2006 c.35).

Royaume-Uni. (2010). Home Office. « Cyber Crime Strategy », Norwich, Royaume-Uni, The Stationary Office.

United Nations Office on Drugs and Crime (UNDOC). (2010). « The Globalization of Crime: A Transnational Organized Crime Threat Assessment ». Vienne, Office des Nations Unies contre la drogue et le crime.

United States Code, Title 18, §1029 (Access Device Fraud).

Urbas, G. et Choo, K.K.R. (2008). « Resource Materials on Technology-Enabled Crime: Technical and Background Paper No.28. », Canberra, Australian Institute of Criminology.

van der Heijden, P., M. Cruyff, et van Houwelingen H., (2003). « Estimating the Size of a Criminal Population from Police Records Using the Truncated Poisson Regression Model », *Statistica Neerlandica,* vol. 57, p. 289-304.

Wagner, C. G. « Internet Fraud on the Rise », *The Futurist*, juillet-août, 2009.

Wall, D. S. (2010a).« Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age », Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications, T. Holt, B. Schell (éditeurs), p. 68-85, Hershey, PA, IGI Global.

– – – . (2010b). « Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders », Mountain View, CA, Symantec Corporation.

– – – . (2009). « The Organization of Cybercrime and Organized Crime », un document preparé pour le Centre for Excellence in Police Studies, Australian National University, Canberra, Australie, 28 avril 2009.

Walther, J. (2004). « Meeting the Challenge of Automated Patch Management », Bethesda, Maryland: SANS Institute.

Weaver, R. et M.P. Collins (2007). « Fishing for Phishes: Applying Capture-Recapture Methods to Estimate Phishing Populations », APWG eCrime Researcher Summit, 4-5 octobre 2007, Pittsburgh, PA, États-Unis.

Wennekes, K. (2008). « A Report of Canadian Executive and Frontline IT Security Professionals on Their Information Sources, Security Challenges, and Career Advantages », Ottawa: CATAAlliance.

White, M. D. et C. Fisher (2008). « Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts », *Criminal Justice Policy Review*, vol. 19, n° 1, p. 3-24.

Zambo, S. (2007). « Digital La Costa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime », *New England Journal on Crime and Civil Confinement,* vol. 33, p. 551-575.