Sous la direction de
Francis Fortin

Cybercriminalité

Entre inconduite et crime organisé

PRESSES
INTERNATIONALES
POLYTECHNIQUE

Cybercriminalité – Entre inconduite et crime organisé
Francis Fortin (Sous la direction de)

Cet ouvrage a été réalisé à l'initiative de la Sûreté du Québec

Coordination éditoriale : Luce Venne-Forcione,
Révision et correction d'épreuves : Nicole Blanchette
Mise en pages : Danielle Motard
Couverture : Cyclone Design

Pour connaître nos distributeurs et nos points de vente, veuillez consulter notre site Web à l'adresse suivante : www.pressespoly.ca

Courriel des Presses internationales Polytechnique : pip@polymtl.ca

Nous reconnaissons l'aide financière du gouvernement du Canada par l'entremise du Fonds du livre du Canada pour nos activités d'édition.

Gouvernement du Québec – Programme de crédit d'impôt pour l'édition de livres – Gestion SODEC.

Dépôt légal : 1er trimestre 2013
Bibliothèque et Archives nationales du Québec
Bibliothèque et Archives Canada

ISBN 978-2-553-01647-9
Imprimé au Canada

Chapitre

12

Nouveaux habits de la vieille fraude : une vision « écosystémique » des fraudeurs, de leurs instruments et de leurs victimes

François Blanchard[1]
Francis Fortin[2]

On entend habituellement par « fraude » la sollicitation, sous un prétexte quelconque, dans le but d'obtenir un avantage ou de l'argent, comme certains utilisateurs d'Internet l'ont déjà expérimenté pour les variantes de la fraude dite « nigériane » ou encore « de la prisonnière espagnole ». Ce qui retiendra notre attention dans ce chapitre est la fraude où interviennent l'informatique et Internet : la cyberfraude. Nous ne traiterons donc pas du vol d'identité[3], souvent un préalable à la fraude, ni d'accès

1. Analyste stratégique, Sûreté du Québec.
2. Chercheur associé, Centre international de criminologie comparée, et candidat au doctorat, École de criminologie de l'Université de Montréal.
3. Voir le rapport de la Federal Trade Commission de 2006, à la page 23, où le vol d'identité est, pour les consommateurs, la première cause de plainte en matière de fraude : « Identity theft continues to be the top consumer fraud complaint received by the FTC. » www.ftc.gov/os/2006/03/ChaimanReportFinal2006.pdf.

aux comptes bancaires par révélation des données confidentielles, ni de vol.

12.1 Problématique

A priori, autant il peut sembler facile d'identifier des sortes de conduites répréhensibles, il faut bien reconnaître, *a posteriori*, que les délinquants empruntent (et combinent librement) toutes les sortes de schèmes opératoires qui leur paraissent profitables[4]. En ce domaine, la variabilité et l'épuisement des possibilités semblent la règle; les distinctions conceptuelles doivent être maniées avec souplesse pour s'adapter à la mouvance des conduites délictuelles. En d'autres termes, les fraudes réelles se conforment rarement à des types purs. Chaque « nouvelle » problématique, qu'on désigne comme fraude, est souvent la même recette avec quelques ingrédients différents.

Pourtant, il est difficile de peindre un portrait juste de la fraude, car bien des fraudeurs sont habiles à tourner de vieilles techniques vers de nouvelles directions et à combiner différentes méthodes de manière novatrice[5]. On doit les classer par type, en faire la filiation pour montrer à partir de la fraude originelle toutes les variantes, mais ce faisant, on échouerait probablement à épuiser toutes les possibilités tant la créativité, parfois naïve, des fraudeurs semble inépuisable. Ce que la migration de ces *modus operandi* (MO) frauduleux vers la contrée du cybercrime nous permet, c'est de passer à une approche qui décrit l'évolution de ces schèmes illégaux comme une population en évolution. L'infrastructure qui permet son expansion peut être analysée. On quitte alors le point de vue de la victime isolée d'un acte singulier pour apercevoir le côté historique et systémique de ces fraudes. Pour simplifier, on peut faire l'hypothèse que les cyberfraudes se trouvent au confluent de plusieurs domaines d'expertise : d'abord, le domaine des « fraudes à distance »,

4. Voir l'article suivant qui, pour dresser un bilan en dollars américains, doit agréger toutes les sortes d'arnaques, du vol d'identité, l'hameçonnage (*phishing*), jusqu'au logiciel malveillant : KEISER, Gregg (2007). « Phishers Pinch Billions from Consumers' Pockets », *New York Times*, 18 décembre.

5. Autrefois, on pouvait presque localiser l'origine des fraudes : ainsi, au XVIII^e siècle, les « lettres de Jérusalem » provenaient d'une prison parisienne et, au XX^e siècle, la fraude dite « nigériane » était issue du Nigéria. Internet a redistribué et multiplié les épicentres.

fraudes épistolaires dont le type primitif moderne est issu du schème de la prisonnière espagnole, en passant par les « lettres de Jérusalem » et le catalogue des fraudes postales dressé par Comstock à la fin du XIX^e siècle (Comstock, 1880); ensuite, le domaine des « pirates informatiques » proprement dits, c'est-à-dire celui de ces expérimentateurs qui explorèrent le réseau téléphonique avant même son informatisation; le domaine des pionniers de l'informatique, bricoleurs de code toujours prêts à démontrer que les concepts peuvent être exécutés par un processeur, qu'un automate peut se reproduire, qu'un programme peut en cacher un autre, qu'un ver informatique peut se répandre sur Internet; enfin, le domaine des industries du paiement qui ne cessent de privatiser les moyens de régler des transactions monétaires pour en prélever une plus-value, la piste magnétique qui orne les cartes étant le point de départ d'arrimages numériques allant bien au-delà de ce qui était envisagé et de ce qui est permis.

L'irrésistible montée en puissance et en nombre des ordinateurs personnels puis leurs interconnexions par le truchement du Web serviront alors de condition essentielle de propagation de ce qui n'était au début qu'expérimentation d'universitaires : des millions puis des milliards d'ordinateurs connectés transforment par leur nombre l'échelle des essais et des erreurs, qu'ils soient bienveillants ou non. Plus rapidement qu'auparavant, mues par mimétisme ou par un sentiment d'émulation, toutes les variantes des MO de fraudes peuvent être appliquées en visant plus ou moins aveuglément cette population. En même temps, cette jeune population d'ordinateurs se différencie et se stratifie rapidement en fonction des différentes versions des systèmes d'opération et du statut incomplet de la distribution de leurs diverses mises à jour.

Ainsi, lorsqu'on observe les variations des cyberfraudes réelles, on constate que beaucoup d'entre elles échappent à des modèles purs. Les fraudes apparaissent alors comme toutes sortes de croisements opportunistes entre des MO traditionnels et des MO propres au cybercrime ou entre les types de cybercrimes.

Si on tente d'épurer cette recette pour n'en garder que les éléments absolument essentiels, on découvre que trois grandes étapes sont nécessaires à la fraude sur Internet. D'abord, puisqu'Internet permet de joindre un très grand nombre de personnes en peu de temps, la première étape est d'entrer en contact avec la victime. On tente ici de joindre le plus grand

nombre d'utilisateurs possible puisque la loi de la probabilité fera bien « tomber » une infime fraction des personnes contactées (Berberi et coll., 2003). Ensuite, il faut trouver le baratin nécessaire pour pousser la victime à accomplir le geste attendu. Il peut s'agir d'un premier paiement, de la communication des identifiants, des mots de passe ou de toute autre autorisation nécessaire à l'exploitation. À ce sujet, les exemples abondent sur Internet et vont de l'oncle héritier qui veut donner son argent aux victimes de cataclysmes récents en échange d'informations personnelles jusqu'à l'offre de changement urgent de mots de passe de la part d'une banque. Notons qu'il peut aussi s'agir de capturer des images compromettantes de la victime, la menace de diffusion des images constituant une raison valable aux yeux de la victime de donner de l'argent à son assaillant virtuel. La fraude pourrait donc migrer alors vers l'extorsion. La dernière étape, celle de l'exploitation, permettra au suspect d'obtenir le montant ou le bénéfice recherché. Dans la prochaine partie, nous aborderons les différentes phases des schèmes frauduleux observés sur Internet.

12.1.1 Rejoindre l'utilisateur

Pourriel. Le premier canal de distribution pour les fraudes Internet, à l'instar des logiciels malveillants, demeure probablement le courriel non sollicité. À partir du premier ver à avoir frappé Internet par le biais d'une attaque visant la fonction « sendmail » en 1988, l'innovation pour rejoindre les utilisateurs a toujours été au rendez-vous. Depuis, le virus « I love you » et plusieurs autres se sont propagés grâce à l'utilisation des carnets d'adresses des usagers. Les fraudeurs, à partir d'une banque d'adresses constituée pour l'occasion, ou plus simplement achetée chez un grossiste, lancent des centaines de milliers de messages semblables. Ces messages peuvent reprendre le schème d'une fraude nigériane, offrir de vrais médicaments au rabais ou des médicaments qui s'avéreront altérés. Ils peuvent aussi s'afficher comme une alerte de sécurité provenant d'une institution bancaire, offrir des occasions d'affaires uniques ou encore annoncer des « actions » sous-évaluées de compagnies minières qui viennent de faire des découvertes importantes. Tous ne sont pas directement assimilables à une tentative de fraude : ils peuvent n'être que l'hameçon destiné soit à extirper des informations confidentielles, soit à induire la victime à pénétrer plus avant dans un schème

frauduleux. Souvent, ces messages renvoient explicitement à des sites Internet, mais beaucoup y réfèrent également de manière implicite ou totalement cachée par le biais des fonctions avancées des courriels en format HTML : le simple fait d'ouvrir le message déclenche par exemple la lecture (et le téléchargement) d'une image transparente d'un pixel. L'émetteur du pourriel reçoit alors confirmation que le message a été lu et que l'adresse est fonctionnelle.

L'étude de Kanich et coll. (2008) nous permet de présenter l'essentiel de ce type d'opérations. Elle décrit deux campagnes de livraisons de pourriels (*spam*) utilisant un réseau de botnets mis en place par le virus « Storm » : la première vise à recruter des clients pour un site de pharmacie et la seconde a pour but, sous le couvert d'un site de cartes postales virtuelles, de distribuer un cheval de Troie porteur d'une variante du virus « Storm ». À proprement parler, l'opération frauduleuse est de petite ampleur : quelques millions de messages expédiés pour quelques dizaines de nouveaux clients ou de nouvelles recrues. L'opération ne serait rentable, à la hauteur de 3,5 millions de dollars de revenus bruts par année, que si les maîtres de « Storm » étaient verticalement intégrés : ils devraient aussi être « pharmaciens » (Kanich et coll., 2008).

Cette hypothèse semble se maintenir, car la catégorisation[6] des sujets des messages transmis comme pourriels pendant les neuf derniers mois de 2011 indique qu'une forte majorité de ceux-ci concernent la vente de médicaments.

Navigateur : un nouvel eldorado. Le second canal de distribution passe par la consultation de sites Internet « infectés » : il s'agit du phénomène du téléchargement furtif (*drive-by download*), puisque réalisé à l'insu de la personne qui consulte le site Internet, dont l'étendue a été mise en lumière récemment par une équipe de Google (Provos et coll., 2007). Après l'analyse de plus de quatre millions d'URL, cette équipe a constaté que plus de 10 % des sites visités déclenchaient de tels téléchargements furtifs; donc, 10 % des sites étaient malveillants. Dans une étude complémentaire publiée en février 2008[7], ils prétendaient avoir identifié plus

6. Voir M86 Security Labs (2012). *Security Labs Report, July – December 2011 Recap*, janvier, p. 11.
7. Voir N. Provos et coll. (2008). « All Your IFRAMES Point to US », *Google Technical Report*, Mountain View, CA.

de trois millions d'URL susceptibles de déclencher des téléchargements furtifs.

Ce n'est pas le lieu pour approfondir les méthodes utilisées pour transformer des pages inoffensives en sites de retransmission de codes malveillants. Selon ces auteurs, il suffit d'écrire que l'on en dénombre quatre types qui finissent presque toujours par entraîner le téléchargement de cadres (*frame*) malicieux :

- l'exploitation des failles des serveurs et particulièrement de leur gabarit de création de pages;
- l'exploitation des mécanismes qui permettent aux usagers de contribuer à un site, à un forum ou à un blogue;
- l'expansion du marché de la revente de publicité[8] et l'activation en cascade de ces publicités qui, éventuellement, débouchent sur un « iFrame » compromis;
- l'exploitation des possibilités d'incorporer aux pages de petites applications externes pour obtenir des fonctionnalités supplémentaires aussi simples qu'un comptage des visiteurs, ces applications pouvant passer soudainement de bénignes à malveillantes.

Le résultat de ces intrusions n'est pas nécessairement ni immédiatement frauduleux (si ce n'est que des étrangers obtiennent l'accès à un ordinateur sans droit), mais ces intrusions sont la condition pour que les ordinateurs compromis se joignent à un réseau de botnets et ainsi répercutent des campagnes de pourriels et de fraudes, réactivant la séquence frauduleuse.

Réseaux sociaux. Dans une étude sur la fraude impliquant les réseaux sociaux réalisée en 2011 (Ryan, Lavoie, Fortin et Dupont, 2011), les résultats suggèrent que les fraudes ne constituent qu'une faible minorité des affaires de déviance observées sur le Web 2.0 rapportées dans les médias. La grande majorité des incidents rapportés par les médias

8. Dans le cadre d'accords commerciaux, pour générer des revenus, les auteurs de pages, les blogueurs par exemple, ou de sites Web peuvent réserver des espaces stratégiques dans leurs pages pour des publicités. Ces espaces seront vendus à des grossistes ou grâce à des enchères, et se transformeront ainsi en une nouvelle sorte de panneaux publicitaires, sur lesquels les titulaires des pages n'ont aucun contrôle, ni sur le contenu ni sur le lien hypertextuel.

se sont produits sur les sites de petites annonces, telles des fraudes élaborées sur Craigslist, par exemple. Il semble, selon cette étude, que la nouvelle génération d'applications Internet ne soit pas à l'origine d'une véritable révolution sur la fraude en ligne. Elle constitue plutôt un support pour celle-ci permettant l'emploi d'anciennes méthodes dans un contexte renouvelé. Dans cet environnement en constante évolution, les fraudeurs apprennent à personnaliser leurs attaques, à utiliser la confiance des utilisateurs envers les autres utilisateurs comme levier pour les amener à commettre des erreurs de jugement et à exploiter la prolifération des données personnelles pour commettre des vols d'identité qui ne sont pas exclusivement motivés par l'appât du gain.

Il n'en demeure pas moins qu'ils constituent une nouvelle porte d'entrée pour joindre les utilisateurs. Si le courriel était la meilleure façon de joindre des victimes dans les débuts d'Internet, cette méthode a diminué dès l'apparition des sites de petites annonces en ligne qui offraient une plateforme plus directe et un auditoire plus attentif. En effet, l'individu voulant vendre sa marchandise ou son bien lira à coup sûr l'offre proposée par un éventuel fraudeur. Joindre un individu sur Facebook constitue une façon très personnelle et beaucoup plus ciblée pour le manipuler. L'envoi de liens malicieux a aussi été observé récemment et exploite maintenant les outils de raccourcissement d'adresse comme « bit.ly » ou « goo.gl » (Chhabra, Aggarwal, Benevenuto et Kumaraguru, 2011). Toutefois, les sites de réseaux sociaux peuvent aussi servir à créer des entités fictives et renforcer la crédibilité d'un interlocuteur. C'est cette question que nous aborderons dans le prochain article.

12.1.2 Déployer le baratin

En tant que personne honnête, respectueuse des lois et soucieuse d'équité, comment ne pas se laisser convaincre à la lecture d'une lettre à en-tête qui nous est personnellement adressée? La situation décrite est tragique : un homme, devenu riche dans l'industrie du pétrole, a laissé à son frère, à la suite d'un décès accidentel, une somme importante que celui-ci ne peut pas déclarer de peur que d'autres héritiers n'accaparent cette fortune. Il nous convie à contribuer à ce qu'il puisse enfin jouir en paix de cette fortune en l'aidant à l'investir en pays plus sûr. Voilà, comme un idéal type, en quoi consiste l'arnaque baptisée « fraude

nigériane », en raison de la grande quantité de lettres issues de ce pays dans le dernier tiers du XX^{e} siècle. Le modèle remonte à plusieurs siècles et serait aussi connu sous le nom de l'arnaque « de la prisonnière espagnole ». À ce chapitre, il semble que les fraudeurs nigérians aient raffiné, remanié et rebaptisé une fraude qui existait depuis plus de cent ans et l'aient élevée pratiquement au rang d'art tout en repoussant les limites en internationalisant sa portée (Onyebadi et Park, 2012).

Le développement du courriel a donc favorisé l'expansion de cette arnaque épistolaire, le coût d'entrée en étant abaissé : plus besoin de timbre, la lettre peut être copiée-collée des centaines de fois et plus. L'accroche peut tenter de bénéficier de la couverture médiatique entourant des événements marquants de l'actualité. L'exemple du tsunami est intéressant :

> Bonjour,
>
> Un de nos clients qui pourrait être de votre famille à Singapour est décédé il y a quatre ans, dans la tragédie du Tsunami en Indonésie, en laissant derrière lui un capital foncier de (38,9 millions de dollars américains, y compris les intérêts) ici, dans cette banque qui m'emploie comme auditeur externe. À ce jour, personne n'a réclamé ou entamé de démarche pour récupérer l'argent. Pour plus d'informations sur la tragédie du Tsunami, allez visiter le site suivant : http ://www.asianews.it/index.php?l=en&art=2375.
>
> Au cours de la recherche privée menée récemment par la banque pour localiser des parents de l'homme décédé, vos nom et adresse de courriel furent parmi ceux trouvés ayant un nom de famille identique au disparu (nom supprimé pour raison de sécurité) qui nous a quitté [sic] sans laisser de testament ou de proches parents. Pour des raisons de sécurité, j'ai volontairement omis les détails finaux.
>
> Je vous invite à vous manifester de manière à ce que je puisse vous fournir tous les détails pour que vous récupériez ces capitaux et qu'ainsi nous recevions nos émoluments, suivant la répartition suivante : 11 670 000 $ pour vous, 23 340 000 $ pour nous et 3 890 000 pour les diverses dépenses liées à ce projet. Cela nous permettrait, à moi et à mes collègues, de finaliser les étapes cruciales, afin que vous disposiez de l'héritage rapidement[9].

9. Courriel reçu par l'auteur en date du 15 janvier 2009; l'expéditeur en serait *Nicholas Fay, pacfish10@googlemail.com.*

Au Canada, il faut signaler l'affaire Asmelash, qui visait Katherine Brown, une résidente sourde du Kentucky, à partir de Toronto[10]. À l'été 2004, madame Brown a reçu un courriel d'une dame Jones du Koweït, qui prétendait, étant à l'article de la mort, vouloir distribuer l'héritage de son mari, de huit millions de dollars, à des personnes nécessiteuses. Pour ce faire, madame Brown dut ouvrir un compte chez un négociant de Toronto, y déposer de l'argent pour l'activer, puis transférer des sommes pour payer soi-disant des frais de non-résidence, des frais de timbres et finalement une somme de plus de 25 000 $ pour un certificat « stupéfiant/antiterroriste ». Ne recevant pas l'argent promis, madame Brown finit par porter plainte au FBI, qui découvrit le pot aux roses. Un des comptes vers lequel l'argent versé par madame Brown fut transféré appartenait à madame Asmelash qui soutenait, quant à elle, qu'on s'en était servi sans qu'elle en ait été informée. Bien que le juge fût convaincu que madame Asmelash n'avait certainement pas agi seule, il la déclara coupable, car c'était elle qui avait retiré l'argent de son compte, à plus d'une occasion, dans des transactions au comptoir qui correspondaient aux sommes versées par madame Brown.

Au-delà des histoires créées de toutes pièces dans un courriel, les sites d'enchères constituent une infrastructure intéressante pour le fraudeur. Ainsi, dans le cyberespace, les ventes aux enchères deviennent littéralement virtuelles : les acquéreurs potentiels ne sont plus en présence ni de l'encanteur, ni des autres acquéreurs, ni même du bien qui est mis à l'encan. Cette dématérialisation permet la résurgence de schèmes frauduleux classiques : le vendeur s'entendant avec des complices pour manipuler les prix, ne pas livrer le bien, ou faire de la fausse représentation dudit bien. Grâce aux nombreux canaux de communication simultanés offerts par le Net, il est plus facile de coordonner l'effort de ceux qui enchérissent. Les sites d'échanges de biens et de mises en vente par encan sont très populaires. À elle seule, eBay revendiquait 181 millions de comptes d'utilisateurs et un chiffre d'affaires de plus de 44 milliards de dollars américains[11] à la fin de 2005. Ces sites attirent toutefois toutes

10. Voir *R.* c. *Asmelash* 2008oncj548.

11. Voir M. Calkins, A. Nikitov et V. Richardson (2008). « Mineshafts on Treasure Island : A Relief Map of the eBay Fraud Landscape », *The University of Pittsburgh Journal of Technology Law & Policy*, vol. 8, nº 1, p. 1-47.

sortes de mécréants. Et c'est ainsi que le nombre de plaintes pour fraudes et de crimes allégués dans ce domaine est également allé en s'accentuant[12]. On y retrouve la plupart des sortes de fraudes.

Il existe plusieurs manières de manipuler le prix de biens mis à l'encan. Nous ne mentionnons ici que les plus astucieuses.

- Le « siphonnage » des mises consiste à offrir de vendre le même type de bien, mais à un prix inférieur que le bien sur le site de l'encan, pour attirer des acheteurs hors de celui-ci et obtenir qu'ils perdent ainsi toute protection contre les malversations.
- On peut aussi proposer une seconde chance d'achat : cette fraude consiste à offrir directement aux personnes qui ont participé à un encan de leur vendre le bien qu'elles désiraient acquérir hors du site officiel, donc sans aucune protection.
- Avec l'augmentation artificielle du montant de la mise, on a recours à un schème assez classique qui se prête à toutes sortes d'adaptations : il repose sur la participation de plusieurs associés du vendeur qui peuvent agir comme autant d'acheteurs pour tenter de gonfler la valeur des mises.
- Le schème inverse cible plutôt les vendeurs : plusieurs acheteurs sont acoquinés, l'un mise un montant trop élevé, ce qui gèle les mises, et se retire au dernier instant pour qu'un second acheteur obtienne le bien à vil prix.

Une nouvelle façon d'augmenter la crédibilité d'une histoire ou d'une offre est de manipuler les outils eux-mêmes. Il peut s'agir de vendre un profil eBay de vendeur ou d'acheteur fiable, et même de s'acheter des abonnés (*followers*) sur Twitter et des amis sur Facebook. Cette technique est déjà bien implantée et utilisée par certaines entreprises de marketing (Van Buskirk, 2010) peu scrupuleuses. Or, puisque la crédibilité du suspect repose entièrement sur la présence et l'appréciation dont il fait l'objet en ligne, la victime potentielle, à la recherche de plus amples détails sur l'auteur de l'offre alléchante, verra irrémédiablement une image parfaite du fraudeur : un individu normal avec des amis qui le

12. Selon Dolan, dès 2001, le nombre de plaintes pour fraudes lors d'encans représentait déjà 70 % des plaintes rapportées à l'organisme Internet Fraud Watch. Voir K. M. Dolan (2004). « Internet Auction Fraud : The Silent Victims », *Journal of Economic Crime Management*, vol. 2, nº 1, p. 1-22.

disent fiable. Ces amis fiables sont évidemment des comptes contrôlés ou achetés par l'arnaqueur. L'étude de la confiance basée sur la réputation comporte certainement une part de risque.

Toutefois, il semble que les systèmes basés sur la réputation qu'on retrouve sur eBay soient un moindre mal. C'est en effet ce qu'on peut conclure à la lecture d'une récente étude qui y voit plusieurs avantages (Gregg et Scott, 2006). D'abord, le nombre d'allégations de fraude trouvées dans ces systèmes dépasse largement les allégations de fraude par des plaintes officielles. Ensuite, les rétroactions négatives sont un bon prédicteur de l'activité frauduleuse future d'un utilisateur. Finalement, les personnes expérimentées dans l'utilisation du système sont en meilleure position pour éviter les ventes potentiellement frauduleuses (Gregg et Scott, 2006).

Or, il semble que la qualité du baratin étalé soit largement tributaire de l'ingéniosité de l'arnaqueur tant par l'offre elle-même que par les moyens techniques déployés en soutien à son histoire. Bien que les gestionnaires des écosystèmes virtuels essaient de contrer et de bloquer ces offres frauduleuses, il incombe à l'utilisateur de faire preuve de jugement devant ces dernières. Ce qu'on observe dans les plus récentes études sur le sujet, c'est la crédulité de certains utilisateurs pour, entre autres, le schème d'avance de fonds (*advanced fee scheme*) [Ross et Smith, 2011] et l'hameçonnage (*phishing*) [Dhamija et Tygar, 2005; Sheng, Holbrook, Kumaraguru, Cranor et Downs, 2010]. À ce titre, on y souligne aussi l'importance de la prévention et de l'éducation (Sheng et coll., 2010).

12.1.3 Exploiter la situation

Après avoir joint une victime et déployé le rationnel pour lui demander une action, bien souvent compromettante, l'attaquant doit exploiter la situation à son avantage. Évidemment, les étapes précédentes influenceront grandement le déroulement de la présente étape. Plus les éléments sont crédibles et réalistes aux yeux de la victime, meilleure sera la suite. La première possibilité sera l'exploitation humaine ou ce que plusieurs ont appelé le « social engineering », ou « ingénierie sociale » (chap. 10). La deuxième sera l'exploitation technologique qui est la résultante d'une faille ou tout simplement de la conception technique. Il va sans dire qu'il arrive fréquemment qu'on assiste à un mélange efficace de ces deux chemins.

L'exemple le plus probant d'exploitation technique est sans doute la fraude par avance de fonds, qui exploite la façon de fonctionner du système bancaire. Pour payer des transactions en ligne, l'acheteur peut frauder en utilisant des chèques visés ou certifiés, ou des mandats-postes, pour payer le bien convoité. La fraude consiste à expédier un chèque dont la somme excède le prix de vente et à demander le remboursement de la différence au vendeur, le tout avant que la banque ne découvre que le chèque est un faux : le fraudeur obtient ainsi non seulement le bien, mais une somme supplémentaire. Plus simplement, le fraudeur se contentera de payer la transaction avec un instrument financier sans valeur : chèque sans provision, faux chèque, lettre de change factice, faux mandat-poste, mandat-poste volé ou détourné.

Par ailleurs, il faut souligner que si le fraudeur solitaire n'est pas une espèce en voie de disparition, la grande majorité des fraudes prospèrent grâce à un riche écosystème planétaire de moyens informatiques qui favorisent la réutilisation de schèmes frauduleux anciens en de nouvelles variations. En bref, ce qu'il y a de plus constant dans la fraude, c'est le caractère interchangeable des moyens utilisés pour franchir les différentes étapes présentées plus haut.

12.2 Exemples

La littérature abonde en exemples de toutes sortes. Nous n'avons retenu ici que quelques cas qui ont été soumis aux enquêteurs du Bureau de coordination des délits informatiques de la Sûreté du Québec :

- Un Québécois veut acheter un bateau sur le site d'annonces Kijiji : à la demande du vendeur, situé en Norvège, il transfère le paiement par l'intermédiaire d'un courtier en devises (*money broker*) sis au Royaume-Uni et n'a plus de nouvelles du vendeur. L'enquête révèle que l'adresse IP utilisée par l'entreprise Moneybookers.net est associée au FAI America Online aux États-Unis.
- Toujours à partir du site Kijiji, un résident du Bas-du-Fleuve remarque une voiture : il envoie une somme de 3 750 $ à Moneybookers par l'entremise du comptoir MoneyGram de Rimouski. La voiture n'a jamais été livrée.

- Une dame est attirée par l'annonce d'un chien sur le site Merkado. Elle échange plusieurs courriels, puis expédie 250 $ par MoneyGram à l'attention de Thierry Ngoue à Nimbe, au Cameroun. Après de nouveaux échanges épistolaires, elle expédie des paiements additionnels de 1 000 $ et de 500 $. Elle reste sans nouvelles du chien.
- Après avoir mis un carrosse en vente sur le site Lespacs.com, le plaignant reçoit un chèque de 4 500 $ d'un acheteur avec pour instruction de l'encaisser et d'expédier la différence dans un compte en Grande-Bretagne. Selon son institution bancaire, le chèque n'est probablement pas valide.

Sans vouloir généraliser à outrance à partir d'un échantillon de si petite taille, on remarque quelques faits notables : les fraudeurs utilisent des services de transfert d'argent moins rigoureux que les banques; ils misent sur les différences de juridiction et semblent ainsi vouloir profiter des lenteurs inhérentes à la coopération policière outre-frontière qui dépend de l'application du Mutual Legal Assistance Treaty.

12.3 Dispositions législatives et cadre réglementaire

Dans ce qui suit, nous indiquons les principales dispositions qui peuvent viser la fraude en les commentant, parfois de manière succincte. Nous commençons par les dispositions du seul traité en la matière, donc ce qui est plus général, pour nous pencher ensuite sur le Code criminel canadien.

12.3.1 Convention du Conseil de l'Europe sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité (entrée en vigueur le 1er juillet 2004, mais offerte à la signature dès le 23 novembre 2001) est le premier traité permettant de lutter contre certaines infractions pénales commises sur le réseau Internet.

Dans le chapitre II, qui porte sur les mesures à prendre au niveau national, on trouve l'article 8 sur la fraude informatique :

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

a) par toute introduction, altération, effacement ou suppression de données informatiques;

b) par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

12.3.2 Code criminel

Bien qu'aux yeux de certains la liste des « cybercrimes » présents dans le Code criminel canadien ait pu paraître assez complète au tournant du siècle, il n'en est peut-être plus ainsi. Ce qui apparaît de plus en plus clairement, c'est l'inadéquation entre l'approche traditionnellement microscopique du Code et la nature écosystémique du cybercrime. En effet, l'interprétation restrictive des textes, qui est de mise en matière criminelle, comme l'évolution des mises à jour, d'ailleurs, favorise une description de plus en plus ciblée, de plus en plus minutieuse, de chaque crime, et ce, pour le cerner au plus près. Or, comme on commence à s'en apercevoir, la cyberfraude n'est généralement qu'un des aspects d'un ensemble de gestes qui visent à s'enrichir. Nous présentons donc ici l'état des crimes inscrits. Pour l'exemple, on notera que l'interprétation restrictive en matière criminelle empêchera l'utilisation de l'article 381 pour poursuivre les fraudes par courriel, la poste n'étant pas le courrier électronique, pas plus d'ailleurs que l'impression de matériel obscène visée par l'article 163(1) ne permet de poursuivre ceux qui « impriment » des documents sur leur « imprimante » personnelle et non sur leur presse offset, puisqu'imprimer préexistait dans le Code à l'invention des imprimantes personnelles.

Fraude : art. 380

380. (1) Quiconque, par supercherie, mensonge ou autre moyen dolosif, constituant ou non un faux semblant au sens de la présente loi, frustre le public ou toute personne, déterminée ou non, de quelque bien, service, argent ou valeur :

a) est coupable d'un acte criminel et passible d'un emprisonnement maximal de quatorze ans, si l'objet de l'infraction est un titre testamentaire ou si la valeur de l'objet de l'infraction dépasse cinq mille dollars;

Il faut signaler aussi l'article 381, comme par défaut, puisqu'une interprétation restrictive du Code criminel ne permettrait peut-être pas de l'utiliser pour les fraudes par courriel :

Emploi de la poste pour frauder

381. Est coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans quiconque se sert de la poste pour transmettre ou livrer des lettres ou circulaires concernant des projets conçus ou formés pour leurrer ou frauder le public, ou dans le dessein d'obtenir de l'argent par de faux semblants.

Escroquerie : art. 362

Escroquerie : faux semblant ou fausse déclaration

362. (1) Commet une infraction quiconque, selon le cas :

a) par un faux semblant, soit directement, soit par l'intermédiaire d'un contrat obtenu par un faux semblant, obtient une chose à l'égard de laquelle l'infraction de vol peut être commise ou la fait livrer à une autre personne;

b) obtient du crédit par un faux semblant ou par fraude;

c) sciemment fait ou fait faire, directement ou indirectement, une fausse déclaration par écrit avec l'intention qu'on y ajoute foi, en ce qui regarde sa situation financière ou ses moyens ou sa capacité de payer, ou la situation financière, les moyens ou la capacité de payer de toute personne ou organisation dans laquelle il est intéressé ou pour laquelle il agit, en vue d'obtenir, sous quelque forme que ce soit, à son avantage ou pour le bénéfice de cette personne ou organisation :

(i) soit la livraison de biens meubles,

(ii) soit le paiement d'une somme d'argent.

12.3.3 Inadéquation du cadre législatif et de la réglementation

Pour montrer les limites des lois criminelles ainsi que les difficultés inhérentes à leur application, nous allons analyser deux affaires qui,

quoiqu'assez uniques[13] dans toute la jurisprudence, sont significatives pour notre propos.

L'affaire Hamilton, expliquée dans le chapitre 4, « Usages problématiques d'Internet », entraîne plusieurs commentaires qu'il est important de souligner à la lumière de ce type de crime : d'abord qu'il semble difficile, au Canada en 2002, d'obtenir la condamnation de quelqu'un qui s'engage dans la distribution d'outils, lorsque ces outils sont des textes[14], pour commettre des fraudes. Ensuite, il faut bien saisir qu'Hamilton n'était qu'un petit artisan : aux yeux de la juge de première instance, il a « paru dénué de toute subtilité et naïf »; il a affirmé de manière crédible n'avoir jamais ouvert les fichiers contenant des recettes pour fabriquer des bombes, ce qui entraîna son acquittement sous ce chef d'accusation : il n'avait pas l'intention coupable que l'on fabrique des bombes. Hamilton était donc assez loin de ceux qui pratiquent l'arnaque électronique à l'échelle de la planète.

Il faut surtout reconnaître que le cadre législatif canadien, bien que salué par certains comme étant à l'avant-garde en 2001[15], n'est peut-être plus tout à fait adéquat. On peut même s'interroger sur la possibilité d'appliquer à des crimes minuscules commis à grande échelle et sur tout le globe une philosophie de répression qui vise essentiellement des crimes graves commis par des personnes individualisables en des lieux précis. Il

13. Au sens de « rares » : il y a très peu de décisions.

14. Ou des logiciels qui sont présentés comme des fichiers, sans les distinguer de fichiers textes.

15. « Le Canada a été l'un des premiers pays à se doter de lois pénales dans le domaine de la criminalité informatique (Convention sur la cybercriminalité, 2001). D'après une étude réalisée par un réseau à parrainage onusien de responsables des politiques Internet, le Canada devance près des deux tiers des 52 pays observés pour ce qui est de la promulgation de lois destinées à combattre la cybercriminalité (Chu, 2000). Par des modifications apportées en 1985 au Code criminel, il a donné force de loi à ce qui était généralement considéré à l'époque comme tout un train de modificatifs portant sur la criminalité informatique : articles 342.1 (Utilisation non autorisée d'ordinateur), 430.(1.1) (Méfait concernant des données), 327 (Possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunication) et 326 (Vol de service de télécommunication). En 1997, il a apporté diverses modifications à son code pénal, ce qui comprend l'article 342.2 (Possession de moyens permettant d'utiliser un service d'ordinateur), par la *Loi visant à améliorer la législation pénale*. » Voir Statistique Canada, Centre canadien de la statistique juridique (2002). *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Ottawa, p. 7.

se pourrait même qu'il s'agisse d'un problème plus complexe : les normes seraient nouvelles, méconnues et difficiles à appliquer.

L'affaire *R.* c. *Alexander*[16] est un bon exemple de ces difficultés, même si la fraude n'était pas qu'informatique. L'avocat de madame Alexander contestait les résultats de l'enquête préliminaire qui ordonnait à celle-ci de subir un procès sous quatre chefs d'accusation : conspiration pour commettre une fraude, fraude de plus de 5 000 $, obtention frauduleuse de crédit et utilisation non autorisée d'un ordinateur.

Dans les faits, on poursuivait une employée de la Banque Royale qui participait à un réseau de voleurs de cartes de crédit, réseau comprenant entre autres un employé des postes qui détournait les cartes au moment de leur livraison; le rôle de madame Alexander se limitait, semble-t-il, à consulter les dossiers des clients pour obtenir les informations confidentielles nécessaires à l'activation des cartes. La décision ne retint pas l'accusation de conspiration, faute de preuve, ni celle d'utilisation non autorisée d'ordinateur à cause d'une erreur dans la rédaction de l'accusation, la Couronne étant tenue de prouver l'accusation telle qu'elle est spécifiée. Dans ce cas-ci, on l'accusait :

> d'avoir frauduleusement et sans apparence de droit obtenu, directement ou indirectement, un service d'ordinateur à savoir : l'ordinateur du Groupe Financier de la Banque Royale avec l'intention de commettre le crime de MÉFAIT contrairement à l'article 430 du Code criminel en ayant intentionnellement volé des données clients de la base de données, et ce, contrairement au Code criminel[17].

À première vue, l'accusation reprend les termes de l'article 342.1(1)c du Code criminel, mais elle est plus spécifique également en désignant le vol de données. Le juge conclut que, d'une part, depuis l'affaire Stewart[18], on ne peut pas voler des données simplement en y ayant accès et que, d'autre part, il n'y a pas de preuve que le vol de données constituerait un méfait contre les données, selon l'article 430. Ainsi, en ordonnant la tenue du procès sous l'accusation telle que formulée, le juge de l'enquête

16. Voir *R.* c. *Alexander*, 2006 CanLII 26480 (ON S.C.).
17. Voir *R.* c. *Alexander*, 2006 CanLII 26480 (ON S.C.) au paragraphe 54. Traduction de l'auteur.
18. Voir *R.* c. *Stewart* (1988) C.S.C. 481.

préliminaire avait excédé sa juridiction. Toutefois, madame Alexander devra subir son procès sous l'accusation de fraude.

On pourrait en conclure, avec le juge[19], que l'accusation d'avoir obtenu les services d'un ordinateur pour commettre une fraude aurait sans doute tenu la route; la Couronne s'est fourvoyée en un excès de « précision », qui manifeste en fait le peu d'usage que l'on fait de l'article 430.

12.4 Statistiques

Bien que les crimes rapportés aux autorités comportent certains biais (Thomassin, 2000), une des meilleures estimations qu'on ait sur la prévalence de fraude sur Internet est colligée par l'Internet Crime Complaint Centre des États-Unis. Cette entité a notamment pour mandat de recueillir les plaintes des citoyens américains pour ce type de crime. La figure 12.1 présente les cinq fraudes les plus rapportées à l'organisme. Nous avons évoqué précédemment l'importance de la crédibilité pour maximiser les chances de succès d'une opération de fraude. Or, les dernières années ont vu apparaître une forme inusitée de fraude. Les escroqueries dans lesquelles un criminel pose comme un représentant du Federal Bureau of Investigation pour frauder les victimes figurent parmi la liste des cinq fraudes les plus populaires de 2011. On observe que 27 % des fraudes impliquaient un tel stratagème. Suit le vol d'identité, qui constitue l'utilisation non autorisée des renseignements personnels d'une victime pour commettre des fraudes ou autres délits, avec 22 %.

La fraude par avance de fonds occupe le troisième rang (21 %). Les deux derniers types sont la marchandise non livrée, avec 17 %, et la fraude par paiement en trop (14 %). Ce dernier type de fraude se caractérise par un incident au cours duquel le plaignant reçoit un véhicule monétaire (généralement un chèque) avec instructions de le déposer dans un compte bancaire. Par la suite, les indications lui sont données pour envoyer les fonds excédentaires ou un pourcentage de l'argent déposé à l'expéditeur. Ce genre de stratagème s'observe entre autres lors de ventes sur un site d'enchères.

19. Voir *R.* c. *Alexander*, 2006 CanLII 26480 (ON S.C.) au paragraphe 62.

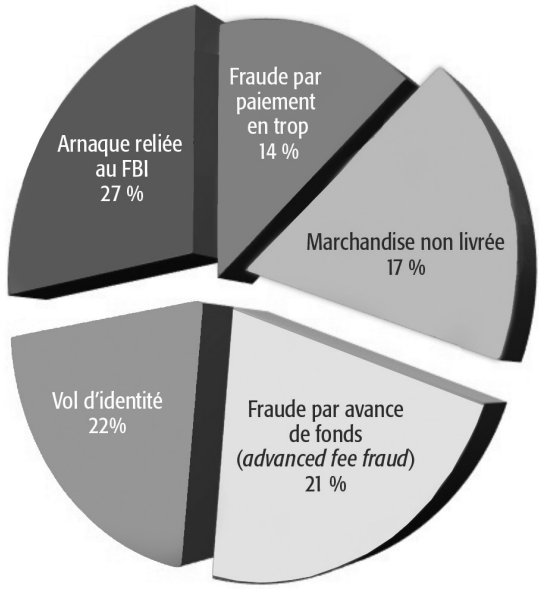

Figure 12.1 Les cinq fraudes sur Internet les plus rapportées en 2011. (Source : Rapport annuel du IC3.)

12.5 Perspectives d'avenir

12.5.1 Automatisation du réseau : un changement d'échelle et une transformation qualitative

Si les manifestations singulières des fraudes qui visent des individus retiennent notre attention, c'est sans doute que nous ne parvenons pas à concevoir que, derrière presque toutes ces tentatives, il existe un réseau de plusieurs centaines de milliers, voire de plusieurs millions d'ordinateurs, dont une fraction de la puissance computationnelle est utilisée à mauvais escient. Peu de recherches semblent avoir été menées sur le comportement réseau de cette énorme population d'ordinateurs compromis. Quelle en est la structure de commandement, de contrôle et d'exécution? Quel est le cycle de vie des logiciels malveillants qui infectent tant de PC? C'est entre autres à ces questions que les recherches actuelles tentent de répondre.

Pendant une période de deux mois, au début de 2008, l'équipe de Polychronakis[20] a analysé près de 6 millions de noms d'hôte pour en retenir un peu plus de 300 000 qui semblaient malicieux. De ce nombre, la moitié déclenchait d'emblée un trafic non relié à un navigateur Web, trafic qui pouvait être lié à un balayage de l'environnement du nouvel ordinateur infecté pour découvrir d'autres PC liés sur LAN ou sur Internet. Une autre partie du trafic semblait constituée de données recueillies par exfiltration, soit l'exportation de données vers d'autres ordinateurs. Enfin, une dernière partie était associée à l'intégration de chaque PC dans un réseau de commande et de contrôle de botnets. On cherche ainsi à construire et à maintenir la pierre angulaire de réseaux capables de réaliser de la fraude à grande échelle, mais à faible empreinte pour éviter d'attirer l'attention et les poursuites.

Ultimement, ces botnets permettent, par l'échange de fichiers, de conduire de grandes campagnes de pourriel à peu de frais. Les auteurs rapportent qu'un chercheur a pu ainsi capturer une liste de 250 millions d'adresses de courriel de ces botnets en 24 heures.

12.5.2 Capacité

Les capacités d'agression des bandes criminelles semblent augmenter plus rapidement que la capacité du réseau :

> Les chercheurs du Arbor Networks ont déclaré qu'une attaque de 40 gigaoctets a eu lieu cette année quand deux cyberclans criminels rivaux se sont disputé le contrôle d'un système Ponzi en ligne[21]. (traduction libre)

Il s'agit d'attaques de 40 gigaoctets par seconde[22]. Il ne fait plus de doute que la compétition/collaboration qui animait le monde des pirates a été remplacée par des groupes criminels de mieux en mieux instruits, non seulement des failles exploitables dans les systèmes, mais surtout

20. Voir M. Polychronakis, M. Panayiotis et N. Provos (2008). *Ghost turns Zombie : Exploring the Life Cycle of Web-based Malware*, First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET'08).
21. Voir J. Markoff (2008). « Internet Attacks Grow More Potent », *New York Times*, 10 novembre.
22. Voir Arbor Networks, Inc. (2008). *Worldwide Infrastructure Security Report*, Volume IV, Chelmsford, MA, p. 3.

chez les usagers, car une proportion importante de ces derniers peuvent être décrits comme des utilisateurs techniquement naïfs et donc « corvéables » à souhait. L'expérience démontre que même les utilisateurs aguerris s'y laissent prendre[23].

Parmi ces failles, notons les tentatives réussies de détournement de trafic sécurisé vers des sites financiers en s'emparant de serveurs DNS :

> Dans un dossier déposé au Wisconsin's Office of Privacy Protection, Check Free déclare qu'au moins 160 000 personnes ont visité le site durant neuf heures pendant lesquelles les visiteurs ont été détournés sur un site en Ukraine. Une analyse de ce site ukrainien indique qu'il essayait d'exploiter des faiblesses dans la sécurité d'Adobe Acrobat et d'Adobe Reader, en tentant d'installer une variante de cheval de Troie Gozi, qui est le plus sophistiqué des programmes de vol de mots de passe utilisé de nos jours. Check Free contrôle de 70 à 80 % de la facturation en ligne du marché des compagnies aériennes américaines[24]. (traduction libre)

À ce titre, l'innovation dans les techniques déployées continuera de surprendre les agences d'application de la loi. Là où les plus astucieux auront la large part du gâteau, il restera toujours des restes pour les « adopteurs » tardifs.

Bibliographie

BERBERI, S., BOULANGER, S., FORTIN, F., MALEZA, D., OUELLET, G., PAQUIN, J., et RODRIGUE, S. (2003). *La cybercriminalité au Québec. Rapport d'analyse stratégique*, Sûreté du Québec, Service du renseignement criminel, Ministère de la Sécurité publique, p. 1-96.

CHHABRA, S., AGGARWAL, A., BENEVENUTO, F., et KUMARAGURU, P. (2011). « Phi.sh/$oCiaL : the phishing landscape through short URLs », *Proceedings of CEAS '11*, p. 92-101.

COMSTOCK, A. (1880). *Frauds exposed*, Montclair, NJ, Patterson Smith, 576 p.

23. Voir R. DHAMIJA, J. D. TYGAR et M. HEARST (2006). « Why Phishing Works », *Proceedings of CHI 2006* (22 au 27 avril, Montréal, Québec), p. 581-590.

24. Voir B. KREBS (2008). « Digging Deeper Into the CheckFree Attack », *The Washington Post*, 6 décembre [En ligne] voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html (consulté le 13 novembre 2012).

DHAMIJA, R., et TYGAR, J. (2005). « Human Interactive Proofs », *Lecture Notes in Computer Science*, vol. 3517, p. 69-83.

GREGG, D. G., et SCOTT, J. E. (2006). « The Role of Reputation Systems in Reducing On-Line Auction Fraud », *International Journal of Electronic Commerce*, vol. 10, nº 3, p. 95-120.

KANICH, C., KREIBICH, C., LEVCHENKO, K., ENRIGHT, B., VOELKER, G. M., PAXSON, V., et SAVAGE, S. (2008). « Spamalytics : An Empirical Analysis of Spam Marketing Conversion », *Proceedings of the 15th ACM conference on Computer and communications security*, p. 3-14

ONYEBADI, U., et PARK, J. (2012). « "I'm Sister Maria. Please help me" : A lexical study of 4-1-9 international advance fee fraud email communications », *International Communication Gazette*, vol. 74, nº 2, p. 181-199.

PROVOS, N., McNAMEE, D., PANAYIOTIS, M., et coll. (2007). « The ghost in the browser : analysis of Web-based malware », *USENIX, HotBots'07*, Cambridge, MA, p. 4.

ROSS, S., et SMITH, R. G. (2011). « Risk factors for advance fee fraud victimisation », *Trends Issues in Crime and Criminal Justice*, nº 420, p. 1-6 [En ligne] apo.org.au/research/risk-factors-advance-fee-fraud-victimisation (consulté le 7 janvier 2013).

RYAN, N., LAVOIE, P.-E., FORTIN, F., et DUPONT, B. (2011). *La fraude via les médias sociaux*, Note de recherche nº 13, p. 1-16 [En ligne] www.benoitdupont.net/sites/www.benoitdupont.net/files/Fraude%20médias%20sociaux%202011_0.pdf (consulté le 13 novembre 2012).

SHENG, S., HOLBROOK, M., KUMARAGURU, P., CRANOR, L. F., et DOWNS, J. (2010). « Who falls for phish? : A demographic analysis of phishing susceptibility and effectiveness of interventions », *Proceedings of the 28th international conference on Human factors in computing systems*, p. 373-382.

THOMASSIN, K. (2000). « La mesure de la criminalité », *Bulletin d'information sur la criminalité et l'organisation policière*, vol. 2, nº 2, p. 1-16.

VAN BUSKIRK, E. (2010). « Gaming the System : How Marketers Rig the Social Media Machine », *Wired Business*, 7 juillet [En ligne] www.wired.com/business/2010/07/gaming-the-system-how-marketers-rig-the-social-media-machine (consulté le 13 novembre 2012).