Sécurité publique Canada | Public Safety Canada

BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**

Sécurité publique Canada
Sites de médias sociaux :
De nouveaux forums pour des occasions de crimes, de communications et d'enquêtes

AOUT 2011
N^{o} SGDDI : 434480

Canada

Sites de médias sociaux : Nouveaux forums pour des occasions de crimes, de communications et d'enquêtes

par

Richard Frank, Ph. D.
Université Simon Fraser

Connie Cheng

et

Vito Pun

Document 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

Les opinions exprimées dans ce rapport sont celles des auteurs et ne reflètent pas nécessairement celles de Sécurité publique Canada.

Rapport nº 021, 2011

Nº de catalogue : PS14-5/2011F-PDF
Nº ISBN : 978-1-100-97862-8

Table des matières

Résumé

Au cours des deux dernières décennies, les progrès rapides dans le domaine des technologies des communications ont grandement augmenté l'efficacité et l'échange d'information. La prolifération des forums de discussions en ligne et, plus récemment, des sites Web de réseaux sociaux comme Facebook et Twitter ont contribué à raviver et à maintenir les liens entre les amis et les connaissances, à faciliter la création de diverses communautés virtuelles ayant des intérêts communs et à créer un nouvel espace pour l'entrepreneuriat et les transactions d'affaires. Les outils des médias sociaux aident à relier les personnes ayant des intérêts communs, et à faciliter un large éventail d'activités du secteur légal. Il s'en suit que des outils de communications et d'affaires d'une telle popularité peuvent aussi faciliter les activités du secteur illicite, peut-être même celles des organisations criminelles. Cette recherche vient compléter les données empiriques existantes qui ont trait à l'utilisation des médias sociaux par les organisations criminelles et les forces de l'ordre et prend appui sur ces données grâce à un examen de la littérature et à des entrevues de représentants des forces de l'ordre et d'experts des médias sociaux.

Tous les répondants du milieu de l'application de la loi et les experts des médias sociaux ont mentionné que le personnel et les organismes d'application de la loi ont utilisé et continuent d'utiliser les médias sociaux pour établir des liens avec les collectivités qu'ils desservent. Les répondants ont indiqué que, en utilisant les médias sociaux, les forces de l'ordre visent à établir des liens et à interagir avec la collectivité et à surveiller de façon proactive la collectivité pour relever les activités et les événements perturbateurs. Les répondants ont fait part des défis avec lesquels ils sont aux prises lorsqu'ils effectuent de telles enquêtes en ligne. Au nombre de ces défis, notons la capacité de trouver la bonne personne parmi un important nombre d'utilisateurs des médias sociaux en ligne, les difficultés procédurales associées à l'obtention de renseignements personnels auprès des propriétaires des données et l'aspect chronophage des procédures rigoureuses à suivre en matière d'expertise judiciaire lors de la collecte de preuves en ligne, notamment lorsque celle-ci est faite de façon à ne laisser aucune trace des activités policières.

Les répondants ont été nombreux à dire que les agents de police ont besoin de recevoir plus de formation de base sur l'utilisation des ordinateurs et d'Internet pour recueillir du renseignement à code source libre. La littérature abondait dans le même sens. Selon les répondants, il importe que le personnel d'application de la loi ait accès à différents ordinateurs, sites Web et logiciels afin qu'ils soient plus à l'aise avec eux et puissent utiliser une panoplie d'outils. Les répondants ont indiqué que le personnel d'application de la loi doit accepter que les agents de police veuillent utiliser les sites de médias sociaux à des fins personnelles. Ils avertissent toutefois qu'il faut obligatoirement séparer le travail policier des activités personnelles. Ils s'inquiètent du fait que de nombreux agents de police ne comprennent pas le danger associé à l'affichage de photos et de renseignements personnels sur les sites de médias sociaux, même s'ils fixent des paramètres rigoureux de protection de leurs renseignements. Certains répondants proposent la création et l'application d'un ensemble de principes sur la manière dont la police devrait et peut obtenir des preuves et sur ce qu'elle devrait ou ne devrait pas faire dans une scène de crime où un ordinateur est en cause. Selon les répondants, de telles lignes directrices permettraient au personnel des forces de l'ordre de faire preuve de plus d'efficacité et d'uniformité lorsqu'il collecte des preuves

dans des ordinateurs. Ces lignes directrices pourraient en outre contribuer à minimiser les traces laissées par la police pendant l'enquête.

La plupart des répondants s'entendaient pour dire que les personnes soupçonnées d'être impliquées dans le crime organisé n'avaient pas tendance à mentionner leurs activités illicites dans leurs profils sur les médias sociaux, mais qu'elles se servaient plutôt des médias sociaux pour rester en contact avec leurs réseaux. Les recoupements entre les caractéristiques démographiques des personnes utilisant les médias sociaux et celles des personnes impliquées dans le crime organisé pourraient s'avérer utiles pour orienter les enquêtes et les efforts de communication. Cette comparaison fait ressortir que, en général, les personnes impliquées dans le crime organisé tendent à être des délinquants à vocation tardive, d'un âge plus avancé que les personnes qui fréquentent les sites de médias sociaux, et qui sont peut-être moins susceptibles d'utiliser les médias sociaux. Les deux sites de blogues décrits dans le présent rapport, Blogger et Wordpress, semblent exceptionnellement avoir une cohorte plus âgée d'utilisateurs. Il est possible que les membres d'organisations criminelles, tout comme le public plus âgé, soient plus attirés par les sites de blogues que par Twitter, Facebook ou MySpace, et qu'ils deviennent par conséquent des utilisateurs ou des consommateurs de ces médias sociaux. Contrairement à un utilisateur type des médias sociaux, les femmes impliquées dans les organisations criminelles tendent à ne pas être de race blanche et à venir d'un milieu socio-économique défavorisé (Beare 2010). Ainsi, il est possible que les délinquantes du crime organisé soient moins susceptibles que leurs homologues masculins à utiliser les sites de médias sociaux.

Introduction

Au cours des deux dernières décennies, les progrès rapides dans le domaine des technologies des communications ont grandement augmenté l'efficacité et l'échange d'information. La prolifération des forums de discussions en ligne et, plus récemment, des sites Web de réseaux sociaux comme Facebook et Twitter ont contribué à raviver et à maintenir les liens entre les amis et les connaissances, à faciliter la création de diverses communautés virtuelles ayant des intérêts communs et à créer un nouvel espace pour l'entrepreneuriat et les transactions d'affaires. Les outils des médias sociaux aident à relier les personnes ayant des intérêts communs, et à faciliter un large éventail d'activités du secteur légal. Il s'en suit que des outils de communications et d'affaires d'une telle popularité peuvent aussi faciliter les activités du secteur illicite, peut-être même celles des organisations criminelles.

Puisque la prolifération de l'utilisation des médias sociaux est une tendance relativement nouvelle et émergente, il y a en ce moment un manque de recherche au Canada sur l'utilisation des médias sociaux pour commettre des infractions, y compris celles commises par des organisations criminelles. Selon le plus récent rapport (2010) du Service canadien de renseignements criminels (SCRC), les organisations criminelles utilisent la technologie « pour communiquer en toute sécurité, dissimuler leurs activités, cibler les victimes, trouver une main-d'œuvre qualifiée ainsi que des biens de valeur, dont d'énormes quantités de données personnelles et commerciales volées ». De plus, le même rapport note que « certains réseaux criminels sont exclusivement virtuels. Ils accomplissent leurs activités et communiquent uniquement en ligne. » Le rapport ne précise pas quels outils en ligne facilitent ces communications.

Cette recherche vient compléter les données empiriques existantes qui ont trait à l'utilisation des médias sociaux par les organisations criminelles et les forces de l'ordre et prend appui sur ces données grâce à un examen de la littérature et à des entrevues de représentants des forces de l'ordre et d'experts des médias sociaux. Le présent rapport traite également de l'utilisation que font les organismes d'application de la loi des médias sociaux. En effet, ce rapport vise trois objectifs :

1. fournir des preuves empiriques sur la manière dont les groupes du crime organisé se servent ou pourraient se servir des outils des médias sociaux;
2. montrer de quelle manière le milieu de l'application de la loi utilise ou pourrait utiliser les médias sociaux pour enquêter sur le crime organisé et pour effectuer d'autres tâches du travail policier;
3. formuler des recommandations destinées aux professionnels de l'application de la loi et aux décideurs sur les manières possibles de mobiliser les médias sociaux à des fins d'application de la loi ou de prévention du crime au Canada.

Le présent rapport décrit à cette fin les types d'outils des médias sociaux et donne des exemples de sites de médias sociaux populaires. Dans le cadre de cette discussion, on fournit des descriptions de la composition démographique du bassin d'utilisateurs de sites de médias sociaux choisis. Cette information vise à jeter les bases d'une discussion sur les occasions de crimes, de communications et d'enquêtes qu'offrent les sites de médias sociaux. Il s'en suit une description de la méthode d'entrevue et une discussion entourant les utilisations réelles et possibles des

médias sociaux par les forces de l'ordre de même que par les groupes criminels. Le rapport se termine par la formulation de conclusions ainsi que de certaines idées pour orienter la recherche dans le futur.

Description des outils des médias sociaux

Internet offre actuellement une vaste gamme d'outils de médias sociaux. Ces outils peuvent être divisés selon les catégories suivantes : microblogues, blogues, forums Web, sites de partage de signets, sites de réseautage social, sites de partage de médias et sites de contenu virtuel. De brèves descriptions de ces types de sites sont fournies ci-dessous.

- **Blogues** : Aussi appelés carnets Web, ces sites Web facilitent le partage d'entrées périodiques où les personnes donnent des détails sur leur vie ou formulent des commentaires sur des sujets ou des événements précis. Les entrées dans les blogues peuvent contenir des photos, du son et des vidéos.
- **Microblogues** : Ces services, comme Twitter, permettent aux utilisateurs de bloguer, mais seulement à l'aide d'un contenu limité, p. ex. de courtes phrases ou des liens vers d'autres sites. Les gens peuvent alors répondre aux messages des autres ou republier un message s'ils le souhaitent.
- **Forums Web** : Version en ligne d'une salle de discussion, on peut y voir une conversation échelonnée sur une certaine période de temps. Les forums Web catégorisent chaque discussion en fonction d'un « fil de discussion », une discussion chronologique sur un sujet donné où les gens peuvent répondre à toutes contributions antérieures. Le forum est organisé en une hiérarchie de sous-forums, qui portent en général sur un sujet précis.
- **Sites de partage de signets** : Ces sites ne facilitent pas l'échange de fichiers ou d'autres formes de média, mais plutôt de références (ou de signets) vers des ressources (c.-à-d. des liens vers des médias, des fichiers ou des pages Web). Chaque signet peut être classé sous un certain nombre de sujets. La capacité de l'utilisateur de coter la qualité d'un signet ou de faire des commentaires représente l'aspect social de ce type de sites.
- **Sites de réseautage social** : Un site en ligne où on peut établir et partager des liens entre des utilisateurs ayant des intérêts communs ou des amis. Chaque utilisateur peut avoir un profil où il peut mettre de l'information à son sujet et ainsi tenir au courant son réseau d'amis de ses activités. Le site de réseautage social le plus populaire est Facebook.
- **Sites de partage de médias** : Ces sites permettent généralement le partage de sons, de vidéos, de photos et de textes avec d'autres personnes. Une fois un média partagé, les utilisateurs sont invités à commenter, répondre ou réagir (peut-être en partageant un autre élément). L'exemple le plus populaire de ce type de service est YouTube.com.
- **Wikis** : Les wikis peuvent ressembler à toute autre page Web, à la différence que ces sites sont créés, modifiés et tenus à jour bénévolement par un ensemble d'utilisateurs. L'exemple le plus populaire de ce type de sites est Wikipedia.
- **Sites de mondes virtuels** : Ces sites ne sont pas des sites Web en tant que tels, mais plutôt des collectivités en ligne qui peuvent interagir dans le cadre d'un environnement virtuel simulé par ordinateur où les utilisateurs sont représentés par des avatars. Second Life en est un exemple populaire.

Les catégories énumérées ci-dessus ne s'excluent pas entre elles. À titre d'exemple, FaceBook peut être considéré comme un site de réseautage social, un service de mises à jour et un site de partage de médias, tout en offrant des outils de partage de signets et des applications qui peuvent être considérés comme du contenu de monde virtuel. Le présent document s'intéresse principalement aux blogues, aux sites de réseautage social, aux microblogues et aux sites de partage de médias.

En vue de comprendre de quelle manière la police et les organisations criminelles utilisent ou pourraient utiliser les médias sociaux, il convient d'abord de connaître les outils de médias sociaux populaires et les caractéristiques démographiques de leurs utilisateurs. Ainsi, on peut en apprendre davantage sur les données démographiques des victimes possibles et sur les méthodes que peut utiliser le crime organisé pour atteindre ses objectifs. Par conséquent, on a choisi plusieurs outils de médias sociaux populaires chez les internautes aux fins de ce rapport. Ces outils de médias sociaux sont décrits ci-dessous.

Twitter

Le service Twitter (www.twitter.com) a été lancé en 2006 et est devenu depuis la norme en matière de microblogage. Les utilisateurs affichent des messages-textes appelés « tweets » ou « gazouillis », renfermant au plus 140 caractères. À l'heure actuelle, on estime que 190 millions d'utilisateurs produisent 65 millions de gazouillis sur Twitter. Ce service peut être utilisé pour échanger des images, des fichiers de son ou des vidéos, mais seulement si ces éléments se trouvent sur un autre site Web (comme YouTube ou Twitpic). Les utilisateurs peuvent accéder à Twitter pour visualiser de nouveaux gazouillis ou envoyer leurs propres gazouillis à l'aide d'un service de messagerie instantanée ou d'une application sur téléphone intelligent. Cheng et Evans (2009) se sont penchés sur les liens entre les utilisateurs de Twitter et en sont arrivés à la conclusion que seuls 5 % des utilisateurs de Twitter avaient plus de 100 personnes qui suivaient leurs gazouillis, que 5 % de tous les utilisateurs produisaient environ 75 % de la circulation sur Twitter, alors que sur l'ensemble des comptes, 20 % étaient inactifs.

Blogger

Lancé en 1999, Blogger est un service de publication de blogues qui permet aux utilisateurs d'afficher des entrées horodatées, comme du texte, des photos et des vidéos. Largement utilisés à titre de média de masse pour exprimer des opinions et créer des liens à d'autres documents sur le Web, les blogues sont devenus un mode de communication très populaire (McIntosh 2003). Blogger a été établi par Pyra Labs, une entreprise achetée par Google en 2003. Aux États-Unis, environ 53 millions d'utilisateurs accèdent à des blogues sur Blogger chaque mois. Dans une analyse de 100 millions de blogues pris au hasard effectuée par Jasra (2010), le pays ayant le plus grand nombre de blogues était les États-Unis (29,22 %), alors que 3,93 % des blogues proviennent du Canada (la population des États-Unis est plus ou moins dix fois plus élevée que celle du Canada, alors cette présence Web est comparable).

WordPress

À la différence de nombreuses entreprises d'hébergement de blogues, WordPress offre à ses utilisateurs un système de gestion de contenu (SGC) à code source libre[1]. Le SGC, une application servant à la gestion et à la création de contenu dans un site Web, propose des gabarits et permet aussi aux utilisateurs ayant des connaissances de base en codage de créer sans contrainte de nouveaux designs ou d'adopter des gabarits. Les utilisateurs peuvent donc en toute liberté personnaliser leurs propres pages Web ou blogues.

Facebook

Facebook est actuellement le réseau de médias sociaux le plus populaire sur la planète. À l'échelle mondiale, il compte 600 millions d'utilisateurs (CheckFacebook.com 2011). Bien que le Canada ne représente que 2,82 % de la population de Facebook, cela représente 16 millions d'utilisateurs de Facebook au Canada, dont 53,8 sont des femmes (CheckFacebook.com 2011; Litwinka 2010). Alors que les autres sites de médias sociaux ciblent des groupes démographiques précis, Facebook semble intéresser des groupes d'âge variés au Canada, où le plus important bassin d'utilisateurs se trouve dans la tranche d'âge des 18 à 34 ans (53 %) (Litwinka 2010). Il y a une population importante de 606 000 (3,6 %) de Canadiens de plus de 65 ans sur Facebook et plus de 1,4 million d'adolescents âgés entre 14 et 17 ans.

MySpace

MySpace, une propriété de News Corporation, est devenu le plus important réseau social en Amérique du Nord en juin 2006, mais a dû concéder ce titre à Facebook en avril 2008 (Techtree 2008). Ce site cible principalement les jeunes et donne la possibilité d'établir des liens avec des marques de commerce et des groupes musicaux, de rencontrer d'autres amis et de connaître d'autres médias de divertissement. Probablement en raison des modifications apportées, le tableau démographique de MySpace a changé depuis ses débuts. Le site n'essaie plus de faire concurrence à Facebook (Ostrow 2010) et s'est maintenant transformé en un service axé sur la musique et les jeunes (Oreskovic 2010). Bon nombre de ses utilisateurs viennent de l'Amérique du Nord, dont la plupart des États-Unis. Par contre, selon une évaluation plus récente de l'utilisation de MySpace au Canada, il n'y a que 830 000 utilisateurs qui se rendent sur MySpace par mois (Google, Inc. 2011). En date de mars 2010, MySpace.com recevait 28,6 millions de visiteurs par mois.

[1] Le terme « code source libre » décrit une philosophie de développement et de production où le code source est mis à la disposition de grand public aux fins de modifications et de distribution ultérieures.

Flickr

Flickr est une collectivité d'hébergement d'images en ligne qui a suscité un vif intérêt auprès des passionnés d'images, des photographes et des technologues. Il permet à chaque utilisateur de télécharger des photos dans leurs propres albums, puis de gérer les albums et les photos qu'ils contiennent. Les amis peuvent alors visionner les albums de photos et formuler des commentaires sur le contenu. Depuis 2008, Flickr a connu un déclin dans le volume de fréquentation Web, alors que d'autres réseaux sociaux, comme Facebook, continuent de croître.

YouTube

Lors de son lancement en 2005, il a donné aux utilisateurs moyens d'Internet la capacité de charger et de partager des vidéos entre eux, et il a depuis facilité l'intégration de vidéos dans d'autres sites Web. Grâce à YouTube, les internautes de partout dans le monde peuvent voir et partager des vidéos entre eux. Les utilisateurs inscrits peuvent créer des « chaînes », auxquelles les autres utilisateurs peuvent s'abonner pour être informés des nouveautés mises en ligne. La consultation de chaque vidéo peut être limitée de sorte que seulement certaines personnes ayant des liens directs aux vidéos peuvent les regarder. Le site et les vidéos qui s'y trouvent sont accessibles à l'aide de nombreux appareils, comme des ordinateurs et des téléphones intelligents (Google, Inc.(b) 2011). À l'heure actuelle, il s'agit du plus important site de partage de vidéos sur Internet, où deux milliards de vidéos sont vus et des centaines de milliers mis en ligne chaque jour (Youtube.com 2011) par les 123 millions de visiteurs mensuels. Après avoir regardé une vidéo, les autres utilisateurs peuvent afficher leurs commentaires et coter chaque vidéo, ou répondre à ceux-ci par la mise en ligne d'autres vidéos.

Le paysage démographique d'ensemble des médias sociaux

Les résumés démographiques de chaque média social reposent sur des statistiques produites par Quantcast.com.[2] Les statistiques démographiques de chaque site de médias sociaux n'étaient disponibles que pour les États-Unis. En ce qui a trait aux visiteurs uniques mensuels, Facebook était au sommet du palmarès, au deuxième rang derrière Google. Des sites de médias sociaux dont

[2] Quantcast.com produit des statistiques démographiques en surveillant ce que font les utilisateurs sur chaque site Web (par exemple télécharger un MP3, répondre à une annonce ou jouer des jeux en ligne) et de quelle manière ils passent d'un site Web à un autre. À partir de cette information, l'entreprise crée un graphique des visites qui analyse les liens dynamiques entre l'auditoire des médias Internet et leurs interactions en fonction d'un vaste ensemble de biens médiatiques numériques, notamment les sites Web, les blogues, les vidéos, les gadgets logiciels et les campagnes de publicité (Quantcast 2008). Le principal objectif de ce type de calcul démographique consiste à avoir une meilleure idée du visiteur, et lui offrir de la publicité qu'il considérera pertinente. Selon Technology Review (2010), Quantcast mesure et analyse les statistiques sur les utilisateurs à l'aide de techniques complexes d'apprentissage automatique. En 2008, l'entreprise utilisait plus d'un billion d'observations pour constituer leurs modèles (Quantcast 2008). En 2010, ses statistiques reposaient sur les données d'un milliard d'internautes (Technology Review 2010). Quantcast s'est classé au troisième rang des entreprises les plus novatrices sur le Web en 2010 (Fast Company 2010). De nombreuses autres entreprises offrent des services semblables, mais on a utilisé la même entreprise (Quantcast) pour obtenir toutes les données démographiques en vue d'assurer l'intégrité des comparaisons démographiques.

il est question dans le présent rapport, Facebook était également celui ayant le plus grand nombre de visiteurs, soit 134 millions de personnes par mois.

Différents groupes d'âge s'intéressent à différents sites de médias sociaux. MySpace a des utilisateurs beaucoup plus jeunes (71 % des utilisateurs sont âgés entre 13 et 34 ans) que Wordpress (69 % des utilisateurs sont âgés entre 18 et 49 ans) ou Blogger (72 % des utilisateurs sont âgés entre 18 et 49 ans). Ces données pourraient indiquer que les groupes d'utilisateurs plus jeunes tendent à préférer MySpace, alors que les sites de blogues servent à des utilisateurs plus âgés. La plus grande partie des gens qui visitent ces sites sont âgés entre 18 et 24 ans, le groupe d'âge le plus important pour tous les sites de médias sociaux mentionnés dans cette analyse. En ce qui a trait aux différences selon les sexes, la représentation des utilisateurs de tous les sites se divise de façon relativement égale entre les hommes et les femmes (50 % et 50 %).

Selon Quantcast.com, la grande majorité des utilisateurs de médias sociaux est de race blanche, et ce, dans au moins 65 % des cas. Les personnes d'origines hispanique et africaine se situaient respectivement au deuxième et au troisième rang des groupes d'utilisateurs les plus représentés. Au Canada, la distribution des utilisateurs devrait être différente en raison de la composition démographique différente du pays.

Quantcast.com évalue le revenu attendu du visiteur par induction statistique. Dans tous les cas, le visiteur gagne probablement plus de 60 000 $ par année; plus de la moitié des visiteurs de l'ensemble des sites de médias sociaux se situaient dans cette tranche de revenu attendu. Cette tranche de revenu n'est pas représentative du Canadien moyen : la famille moyenne a un revenu de 91 500 $ par année, et la personne seule moyenne gagne 37 800 $ par année (Gerlsbeck 2009).

Des personnes de différents niveaux de scolarité sont attirées par différents sites de médias sociaux. MySpace a le pourcentage le plus élevé d'utilisateurs sans diplôme d'études postsecondaires. Les utilisateurs de MySpace sont également plus jeunes que l'utilisateur moyen, ce qui peut avoir eu une incidence sur cette statistique. WordPress et Blogger étaient les seuls sites dont le segment d'utilisateurs ayant un diplôme d'études postsecondaires était plus important que celui des utilisateurs sans diplôme d'études postsecondaires.

Dans l'ensemble, les différents détails démographiques présentés par Quantcast.com sont constants : MySpace a tendance à avoir des utilisateurs plus jeunes et moins scolarisés, tandis que les sites de blogues tendent à avoir des utilisateurs plus scolarisés et plus âgés. Pour les autres sites, les autres variables démographiques utilisées aux fins du présent rapport étaient réparties de façon relativement égale.

Méthode

Dans le but d'atteindre les objectifs du projet, on a procédé à une étude de la littérature et à une série d'entrevues avec des responsables de l'application de la loi et des experts en médias sociaux. Divers guides d'entrevue ont été adaptés en fonction des différents groupes. Le guide d'entrevue utilisé pour les deux groupes comportait des questions sur les thèmes suivants :

- les avantages et les difficultés associés à l'utilisation des médias sociaux à des fins d'enquêtes par les forces de l'ordre;
- la manière dont les médias sociaux sont utilisés pour faciliter les activités des organisations criminelles;
- les pratiques exemplaires destinées aux professionnels de l'application de la loi en ce qui a trait à l'utilisation des outils de médias sociaux aux fins d'enquête ou d'autres fins;
- des recommandations à l'intention des professionnels de l'application de la loi et des décideurs quant aux moyens possibles pour mobiliser les médias sociaux à des fins d'application de la loi ou de prévention du crime au Canada.

L'échantillon de commodité et du sondage cumulatif a commencé en compagnie de trois experts connus du milieu de l'application de la loi. Il en a découlé des entrevues avec 11 répondants. Tous les répondants avaient des antécédents qui les rendaient aptes à discuter des thèmes susmentionnés. Entre le 15 février et le 1er mars 2011, on a mené dix entrevues (une d'entre elles s'est déroulée avec deux répondants).

L'échantillon des responsables de l'application de la loi comptait quatre agents de police spécialisés dans les crimes informatiques et les enquêtes menées à l'aide d'Internet. Un répondant était originaire du Royaume-Uni, et les trois autres répondants étaient issus de services de police municipaux, provinciaux et fédéraux du Canada. De plus, trois répondants étaient des instructeurs spécialistes du domaine des enquêtes utilisant des renseignements de sources ouvertes (information à laquelle le public a accès sur Internet). Dans l'échantillon des responsables de l'application de la loi, il y avait aussi des répondants travaillant au privé; une des entrevues a été réalisée auprès d'un détective privé spécialisé dans les enquêtes utilisant des renseignements de sources ouvertes, et une autre avec une personne travaillant dans le milieu de la sécurité informatique, notamment les enquêtes sur les cybercrimes et la protection contre les cybercrimes.

L'échantillon des experts en médias sociaux était petit et n'était composé que d'un seul civil travaillant à temps plein à offrir du mentorat aux agents de police sur leur utilisation des médias sociaux ainsi que du vice-président d'un service canadien de médias sociaux.

Utilisations réelles et possibles des médias sociaux par les organismes d'application de la loi

L'utilisation des sites de médias sociaux en ligne a eu une croissance très rapide au cours des dernières années, et, bien que de nombreuses études indiquent de quelle manière le grand public se sert de ces services (Marsico 2010; Cheng 2009), il y a peu d'ouvrages traitant de la façon dont ces services peuvent être utilisés pour commettre des crimes et lutter contre la criminalité. Par contre, les responsables de l'application de la loi ont adopté des méthodes d'enquêtes communes partout dans le monde. À titre d'exemple, le service de police de l'Irlande du Nord a utilisé Facebook comme un outil pour mener des sondages locaux en vue d'en apprendre davantage sur ses citoyens (Alderson 2011). Au Canada, la Gendarmerie royale du Canada (GRC) et les services de police de Victoria, de Vancouver et de Toronto ont tous une page Facebook.

Les entrevues ont fait ressortir plusieurs thèmes au sujet des utilisations possibles des médias sociaux pour commettre des crimes, enquêter sur des crimes et communiquer avec le public. Ces thèmes ont été regroupés en fonction des thèmes plus larges suivants : établissement de liens avec les collectivités, collecte de renseignements, défis liés aux enquêtes et recommandations des répondants.

Établissement de liens avec les collectivités

Tous les répondants s'entendent pour dire que les responsables de l'application de la loi ont employé et continuent d'employer les médias sociaux pour établir des liens avec les collectivités qu'ils desservent. Cette conclusion illustre peut-être un biais de l'échantillon de répondants.

On a demandé aux répondants si leur service ou leur organisme avait des objectifs à atteindre à l'aide des médias sociaux. Les objectifs organisationnels avancés par les répondants étaient semblables. Parmi les points mentionnés par les répondants, notons l'établissement de liens et l'interaction avec la collectivité et la surveillance proactive de la collectivité pour trouver les activités perturbatrices. Un répondant a indiqué qu'une rave (type de fête où il y a de la danse et de la musique et où il peut y avoir de la consommation de drogues, p. ex. ecstasy, méthamphétamine et autres stimulants) avait été surveillée et contrôlée à l'aide de renseignements obtenus sur Facebook.

On a ensuite demandé aux répondants de décrire comment ils, ou leurs équipes, se servaient des médias sociaux pour faire participer le public. Tel que cela a été mentionné précédemment, le service de police de Toronto est actif sur Facebook et il se trouve aussi sur Twitter et YouTube (Masterman 2010). Selon un répondant, les sites de médias sociaux ont permis à ce service de police d'être plus en contact avec des personnes n'ayant pas accès aux méthodes habituelles de mobilisation communautaire. De plus, ce même répondant avance que les sites de médias sociaux permettent à la police de rejoindre un auditoire plus jeune et différent de celui auquel elle a habituellement accès. Parallèlement, on a aussi affirmé que l'information affichée sur les sites de médias sociaux peut faciliter le signalement de crime pour les jeunes qui cherchent à poser des gestes positifs.

Pour établir un parallèle à partir de l'information disponible sur l'utilisation policière des médias sociaux, le service de police de l'Irlande du Nord a aussi créé une page d'essai Facebook, qui, une fois lancée, a servi à mener une étude pour connaître l'opinion du public sur le service de police. Sur l'ensemble des participants à l'étude, 85 % d'entre eux étaient d'avis que la page Facebook donnait une tribune aux citoyens pour qu'ils aident à rendre le quartier plus sécuritaire; 83 % des répondants étaient d'avis que cet outil permettait d'augmenter l'appréciation de l'activité policière; 82 % pensaient que l'information fournie sur le site favorisait la prévention du crime; 75 % ont affirmé que le service de police s'était amélioré après le lancement de la page; et 70 % ont dit que leur confiance dans la police locale avait augmenté. Il est intéressant de noter qu'une confiance accrue du public dans les forces de l'ordre peut diminuer la crainte du crime (Skogan 2009), mais aussi augmenter la sensibilisation au crime. À l'aide des sites de médias sociaux, la police peut désormais diffuser instantanément des messages sur des crimes et des conseils en matière de prévention locale du crime.

Lorsqu'on leur a demandé de décrire de quelle manière ils, ou leurs équipes, se servaient des médias sociaux pour faire participer le public, deux répondants ont dit que l'utilisation policière des médias sociaux peut aider à diffuser des directives en cas d'urgence et des bulletins de circulation de même qu'à faire la promotion d'activités spéciales et à demander de l'aide pour la recherche de personnes disparues. Un répondant des forces de l'ordre du Royaume-Uni a mentionné que son organisme utilisait régulièrement Facebook et Twitter pour interagir avec la collectivité d'autres façons, par exemple en créant un registre de condoléances lors du décès d'agents de police ou en menant des consultations publiques (lesquelles n'ont pas un taux élevé de participation lorsqu'elles se déroulent hors ligne, mais remportent un franc succès en ligne).

En général, les répondants conviennent que plus grande est l'interaction des forces de l'ordre avec la collectivité, meilleures seront leurs relations avec celle-ci. Les répondants sont d'avis qu'en leur offrant plus de possibilités d'interagir avec la police, comme la diffusion de nouveaux renseignements sur une page de profil que les membres peuvent consulter régulièrement, les citoyens peuvent être plus enclins à demander de l'aide, de même qu'à fournir des pistes utiles pour résoudre des crimes. Selon les répondants, la seule façon de tirer profit des sites de médias sociaux consiste à informer la police et le public sur l'utilisation de ces services de façon à ce qu'ils soient habitués à leur potentiel.

Collecte de renseignements

On a demandé aux répondants de dire comment ils, ou leurs équipes, se servent des médias sociaux lors d'une enquête, notamment pour les enquêtes liées au crime organisé, et de donner un exemple concret de la manière dont les outils de médias sociaux ont contribué à une enquête. Deux répondants ont avancé des raisons de sécurité pour expliquer leur refus de discuter de stratégies d'enquête précises. Quant aux autres répondants, cinq d'entre eux ont indiqué avoir déjà utilisé les médias sociaux dans le cadre d'enquêtes sur le crime organisé, et ils avaient tous de l'expérience dans la collecte de renseignements pour des délits non liés au crime organisé.

Tous les répondants de l'échantillon des responsables de l'application de la loi ont indiqué qu'ils commençaient maintenant souvent une enquête par l'ouverture d'un navigateur Web et la collecte d'information en ligne. Bien que les enquêtes en ligne et hors ligne aient leur utilité, on peut

recueillir beaucoup d'informations à partir de sources publiques, une activité appelée « collecte de renseignements de sources ouvertes ». Voici la description de cette méthode d'enquête donnée par l'un des répondants :

> La collecte de renseignements de sources ouvertes consiste à chercher de l'information accessible au public, mais à trouver de l'information que le public ne sait pas comment obtenir et à l'analyser d'une manière que le public ne connaît pas.

Pris dans leur ensemble, les répondants ont décrit comme suit un exercice typique de collecte de renseignements de sources ouvertes. D'abord, on identifie une personne ou un groupe de personnes (ci-après appelée un suspect). On cherche le profil du suspect sur de nombreux sites de médias sociaux dans l'espoir de le trouver au moins à un endroit. Le réseau d'amis, de collègues de travail, de collaborateurs et de membres de la famille du suspect est établi grâce à ses liens à d'autres personnes ou organisations (y compris des gangs) sur les sites de médias sociaux. À la même occasion, on recueille de l'information propre au suspect, comme ses numéros de téléphone, ses pseudonymes, son âge, sa ville, les intersections les plus près, ou les adresses qu'il fréquente. Cette information peut être obtenue, par exemple, à l'aide de coordonnées de GPS intégrées dans des photos. Certaines personnes indiquent que cette information est privée sur les sites de médias sociaux qu'ils fréquentent. Les agents de police et les détectives privés peuvent essayer de devenir l'ami du suspect en utilisant de faux comptes pour tenter d'infiltrer le réseau du suspect. Les faux comptes peuvent représenter des efforts à long terme, dont l'objectif consiste à établir des liens avec le suspect pour gagner sa confiance. Lorsqu'on a obtenu suffisamment de renseignements sur le suspect, les forces de l'ordre peuvent porter des accusations contre l'individu ou les membres du réseau.

Selon deux répondants, malgré les liens établis par l'enquêteur avec le suspect, l'exercice peut s'avérer inutile puisque les suspects n'ont pas tendance à se servir des sites de médias sociaux pour discuter de leurs crimes, mais plutôt pour les mêmes raisons que le grand public, c'est-à-dire se tenir au courant des activités de leurs amis et de leurs familles. Par conséquent, en vue d'obtenir de l'information utile, il faut parfois axer l'enquête en ligne sur le réseau du suspect, y compris ses petites amies, les membres de sa famille et les connaissances proches. Une anecdote donnée par un instructeur en collecte de renseignements de sources ouvertes illustre bien l'utilité de la surveillance du réseau d'un suspect. Le chef d'un cartel de la drogue mexicain a été trouvé et arrêté, car on a pu déterminer son emplacement grâce à la surveillance policière du compte Facebook de sa petite amie qu'elle utilisait pour rester en contact avec ses amis et sa famille.

Il ressort clairement des réponses d'entrevue que le renseignement peut être obtenu de ressources inattendues. Par exemple, un répondant a mentionné que son organisme cherche la présence d'un suspect sur les sites de généalogie[3], car, selon son expérience, les criminels tendent à avoir des membres de leurs familles qui sont également des criminels. De plus, certains sites permettent aux utilisateurs de mentionner leurs passe-temps, ce qui diriger les enquêteurs vers, par exemple, des clubs et des associations fréquentés par le suspect. En connaissant un endroit précis que fréquente

[3] Les sites Web de généalogie permettent aux utilisateurs de constituer des arbres généalogiques où figurent leurs ancêtres, leur lignée et leur histoire.

un suspect, les forces de l'ordre peuvent établir des liens avec des amis de ce suspect ou trouver le suspect à cet endroit.

Les répondants ont noté que les renseignements pouvaient être involontairement fournis par le suspect sur les sites de médias sociaux. À titre d'exemple, un répondant a souligné que les téléphones modernes possèdent des GPS intégrés, et que, si un suspect transmet un gazouillis, le lieu sera intégré dans le message, permettant ainsi aux responsables de l'application de la loi de retrouver le suspect. De plus, comme on l'a mentionné précédemment, selon un des répondants, les métadonnées contenues dans les images versées sur les sites de médias sociaux peuvent servir à établir un lieu grâce aux coordonnées de GPS. Les images peuvent aussi être utilisées pour trouver rapidement la même personne dans d'autres images à l'aide d'un logiciel de reconnaissance de visage (comme celui qui est intégré dans le gratuiciel Picasa de Google).

Bien que tous les répondants aient dit que la collecte de renseignements de sources ouvertes fait partie intégrante des enquêtes, les répondants de l'échantillon des responsables de l'application de la loi ont indiqué que leurs enquêtes étaient parfois limitées par les politiques de leurs organismes. Un des répondants a mentionné que son organisme appuie sans réserve les enquêtes ayant recours à la collecte de renseignements de sources ouvertes et encourage le personnel à utiliser ce mode d'enquêtes tant à des fins privées que professionnelles (assujetties à des contrôles quant à leur moment et à leur pertinence) puisque l'on vise à intégrer ce type de collecte de renseignements dans leurs activités professionnelles et quotidiennes. Un autre répondant a indiqué que son organisme avait, en théorie, le même objectif, mais que les restrictions quant au matériel disponible pour le travail minaient leur capacité à utiliser pleinement ce mode de collecte de renseignements. Par exemple, certains organismes n'ont pas Mozilla FireFox, qui est, selon quatre des répondants, le navigateur Internet de choix pour la collecte de renseignements de sources ouvertes puisqu'il offre des utilitaires qui peuvent réduire considérablement les efforts déployés par les enquêteurs.

Défis concernant l'utilisation des médias sociaux aux fins d'enquêtes

On a demandé aux répondants de discuter de certains des défis liés à l'utilisation des sites de médias sociaux pour faire participer les collectivités. Selon un des répondants, certains services de police utilisent, à tort, les médias sociaux comme un outil de diffusion. Les médias sociaux sont par définition *sociaux.* Leur but ou leur avantage n'est pas de diffuser, par exemple, des messages des organismes d'application de la loi à la collectivité, mais plutôt de faciliter l'interaction et le renforcement des liens entre les gens et les organismes. De plus, bien que le personnel de l'application de la loi puisse entamer des discussions à l'aide des médias sociaux, mais au dire des répondants, la participation de la collectivité variera.

Les répondants ont mentionné un certain nombre de problèmes très importants nuisant à la collecte de renseignements de sources ouvertes. D'abord, selon tous les répondants, la plupart des responsables de l'application de la loi n'ont pas les connaissances informatiques de base nécessaires pour poser les bonnes questions, ni les compétences pour mener des enquêtes sur Internet. Ils ne sont pas non plus conscients du nombre de renseignements personnels qu'ils laissent derrière eux au cours d'une enquête numérique. Au dire des répondants qui donnent des

cours sur la collecte de renseignements de sources ouvertes, les policiers n'ont pas tendance à avoir des connaissances informatiques et ne sont pas aussi à l'aise avec les médias sociaux qu'ils le devraient. La plupart des répondants conviennent que les technologies changent rapidement, et que les services de police doivent tirer profit des technologies les plus récentes, car un nombre accru d'occasions de commettre des actes illégaux se présentera sur ces forums. Bien que les agents de police reçoivent de la formation pour s'adapter aux dernières technologies de télécommunications et de l'information, ils perdront les compétences acquises s'ils ne les utilisent pas. Les répondants ont en outre souligné qu'il était difficile pour les enquêteurs de rester au courant de l'évolution des technologies, de même que des périodes de validité et des processus juridiques, tout en s'acquittant de leurs autres tâches de policiers.

En ce qui a trait aux agents de police qui possèdent les compétences nécessaires, les répondants ont souligné une autre difficulté liée aux enquêtes en ligne, à savoir qu'il faut s'assurer qu'un profil donné appartient bel et bien au suspect en question. La plupart des répondants ont signalé qu'il était difficile de trouver le bon profil d'un suspect. Par exemple, la recherche officieuse d'un nom commun sur Facebook peut facilement donner plus de 200 résultats. En l'absence de plus de détails sur le suspect, une recherche approfondie fondée uniquement sur le nom demande énormément de temps ou peut s'avérer vaine à moins que le nom soit extrêmement inhabituel. Il peut aussi y avoir de la confusion quant aux noms en raison des fautes d'orthographe, des surnoms, des langues différentes, des pseudonymes ou d'autres facteurs. Par conséquent, la recherche doit être combinée à de l'information la plus précise possible, notamment les numéros de téléphone, les noms de rue et les intersections ou les stations de métro les plus proches. Selon les répondants qui ont décrit ce processus, lorsqu'un suspect a été identifié dans un site de médias sociaux, on peut obtenir d'autres renseignements qui peuvent être utilisés pour d'autres enquêtes et pour créer un portrait plus détaillé du suspect et de son réseau.

Les répondants ont noté un autre problème, à savoir les politiques rigoureuses de certains sites de médias sociaux en matière de protection des renseignements privés. Les répondants ont signalé que des sites populaires, comme Twitter et Facebook, acceptent de donner un accès à l'information d'un titulaire de compte à la condition qu'un mandat perquisition soit présenté. Facebook a même un guide à l'intention des membres des forces de l'ordre sur les procédures à suivre pour demander de l'information sur un utilisateur. De plus, puisque la plupart des sites de médias sociaux sont hébergés à l'extérieur du Canada, il faut présenter des demandes d'entraide juridique pour avoir accès à de l'information juridique sur les comptes ciblés aux fins de présentation aux tribunaux. Les répondants ont indiqué que cela peut prendre jusqu'à six mois avant de recevoir l'information demandée en raison des procédures qu'il faut suivre lorsque deux pays sont en cause. Les répondants ont également mentionné que la collecte d'éléments de preuve à partir de ces services est problématique. Tous les éléments de preuve doivent être obtenus conformément aux normes en matière d'expertise judiciaire. Le contenu du site Web doit être produit sous forme de document PDF et des captures d'écran doivent être faites advenant des différences entre la présentation réelle du contenu et le PDF. Pour bien exécuter ce processus, il faut des ressources, du temps et des efforts. Un des répondants étant un instructeur dans le domaine de la collecte de renseignements de sources ouvertes a mentionné qu'il importe que les agents de police comprennent les lois associées à la collecte d'information en vue de présenter des preuves pertinentes aux tribunaux.

Il y a des exceptions à la règle; certains sites de médias sociaux ont choisi de contribuer aux enquêtes en répondant rapidement aux demandes des organismes d'application de la loi, et ce, même en l'absence d'un mandat de perquisition. C'est notamment le cas du site de réseautage social canadien de l'un des répondants. Comme l'a mentionné le répondant en question, les services de police doivent avoir leurs raisons de demander cette information, voilà pourquoi ils obtempéreront habituellement même s'il n'y a pas de mandat de perquisition.

Enfin, un des répondants s'est dit préoccupé par le danger que peuvent présenter les sites de médias sociaux pour les agents de police. La littérature empirique vient appuyer cette préoccupation. Selon Weimann, les délinquants surveillent constamment les services en ligne pour obtenir de l'information sur les forces de l'ordre (2010). On conseille aux agents de police de ne pas mêler leur vie personnelle à leur vie professionnelle en les dissuadant d'utiliser les sites de médias sociaux à des fins personnelles, notamment sur leurs téléphones (en raison des fonctions de GPS). On conseille aussi fortement aux agents de police de ne pas afficher des photos, particulièrement celles qui sont récentes, et de s'assurer que leurs amis n'affichent pas d'information à leur sujet. D'après un des répondants, s'il est possible d'obtenir facilement de l'information sur un agent de police en ligne, cette personne pourrait ne pas être en mesure de faire du travail d'infiltration, et sa crédibilité en tant qu'agent de police pourrait être attaquée devant les tribunaux.

Recommandations des répondants

On a demandé aux répondants de formuler des recommandations sur la manière dont les forces de l'ordre pourraient utiliser les services de médias sociaux. Parmi les recommandations faites le plus souvent et que l'on retrouve aussi dans la littérature, notons le besoin des agents de police d'avoir davantage de formation de base en informatique et sur l'utilisation d'Internet pour la collecte de renseignements de sources ouvertes. Presque tous les répondants ont fait cette suggestion. Selon un des répondants, le fait d'avoir des connaissances générales et actuelles sur la manière d'utiliser efficacement Internet aide aux enquêtes sur les suspects possibles. Quatre répondants s'entendaient pour dire qu'il faudrait créer un ensemble de principes sur la manière dont la police devrait et peut obtenir des preuves et sur ce qu'elle devrait ou ne devrait pas faire dans une scène de crime où un ordinateur est en cause. Selon les répondants, de telles lignes directrices permettraient au personnel des forces de l'ordre de faire preuve de plus d'efficacité et d'uniformité lorsqu'il collecte des preuves dans des ordinateurs. Ces lignes directrices pourraient en outre contribuer à minimiser les traces laissées par la police pendant l'enquête.

D'après les répondants, il importe que le personnel d'application de la loi ait accès à différents ordinateurs, sites Web et logiciels afin qu'ils soient plus à l'aise avec eux et puissent utiliser une panoplie d'outils. Les répondants qui donnent de la formation sur la collecte de renseignements de sources ouvertes ont indiqué que la plupart des cours qu'ils offrent sont adaptés en fonction de ce besoin, mais que les courses ne durent que quelques jours. Ils ont recommandé que tous les membres des forces de l'ordre suivent ces cours périodiquement. En fait, cela correspond à la situation réelle. Tous les instructeurs ayant participé aux entrevues ont mentionné qu'il y avait des listes d'attente pour leurs cours et que des personnes de toutes les administrations et de tous postes essayaient d'y participer. Les répondants ont indiqué qu'il pourrait y avoir un problème du côté de

l'offre et qu'il pourrait s'avérer prudent d'augmenter le nombre de cours offerts pour répondre à la demande grandissante.

La plupart des membres de l'échantillon des responsables de l'application de la loi ont mentionné que les responsables de l'application de la loi doivent accepter que les agents de police veuillent utiliser les sites de médias sociaux à des fins personnelles. Ils émettent toutefois un avertissement : il faut obligatoirement séparer le travail policier des activités personnelles. Ils s'inquiètent du fait que de nombreux agents de police ne comprennent pas le danger associé à l'affichage de photos et de renseignements personnels sur les sites de médias sociaux, même s'ils fixent des paramètres rigoureux de protection de leurs renseignements. En utilisant des sites de médias sociaux, les agents de police peuvent éliminer leurs chances futures de faire du travail d'infiltration de même que de mettre leur vie en danger ainsi que celle des membres de leurs familles et de leurs amis. Des personnes peuvent recueillir de l'information sur les agents de police en utilisant les mêmes méthodes qu'utilisent les organismes d'application de la loi pour obtenir des renseignements sur des suspects. En vue d'éliminer toute zone grise quant à l'utilisation des sites de médias sociaux, les répondants préconisent l'élaboration de politiques qui décrivent en détail les activités auxquelles les membres de la force de l'ordre peuvent et ne peuvent pas participer en ligne.

Utilisations réelles et possibles des médias sociaux par les organisations criminelles

Le débat fait rage dans la littérature universitaire sur le crime organisé quant à savoir ce qui constitue une organisation criminelle. Une vaste panoplie de termes a été utilisée pour décrire des groupes qui participent à des activités du crime organisé, notamment mafia, bande de motards criminalisée, triade, réseau de vol de voiture, gang criminel, groupe motivé par le crime haineux, gang de jeunes, gang en milieu urbain, gang en milieu rural, gang ethnique, gang de filles, gang de trafic de drogue, gang autochtone, cellule terroriste et groupe de jeunes délinquants (Wortley 2010, p. 5). Ces étiquettes reposent sur les caractéristiques démographiques du groupe, de même que sur leurs activités criminelles. À titre d'exemple, certains ouvrages font une distinction entre les gangs et les organisations criminelles, le premier étant souvent considéré comme ayant des membres plus jeunes ou étant moins organisé. Les définitions du crime organisé tendent à varier en fonction des circonstances et des besoins locaux (Wortley 2010, p. 5). Contrairement à l'image véhiculée dans les médias populaires, de récents ouvrages reposant sur l'analyse des réseaux sociaux avancent que les organisations criminelles sont plutôt flexibles, peu structurées et composées de nombreux petits réseaux (Morseilli, Gabor et Kiedrowski 2010, p. 9). Le *Code criminel* du Canada définit une organisation criminelle comme suit :

> Groupe, quelqu'en soit le mode d'organisation : composé d'au moins trois personnes se trouvant au Canada ou à l'étranger; 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 à une personne qui en fait partie –, directement ou indirectement, un avantage matériel, notamment financier.

Pour les besoins du présent rapport, on a adopté une définition plus large de l'organisation criminelle qui inclut les réseaux plus ou moins criminels.

Les personnes impliquées dans le crime organisé ont été décrites comme étant des personnes qui s'organisent elles-mêmes, qui surgissent dans des lieux où des vulnérabilités créent de nombreuses possibilités et qui interagissent dans des milieux qui touchent plus d'un pays, d'un marché ou d'une industrie (Morselli, Turcotte et Tenti, 2010, p. 10). Selon la théorie axée sur les activités routinières, les occasions de crime se présenteront lorsqu'une victime rencontre un délinquant motivé par le moment et le lieu en l'absence d'un gardien compétent (Felson et Clarke 1998). Tant la présence de victimes innocentes et l'absence de gardiens compétents se retrouvent dans l'environnement des services de médias sociaux en ligne. Comme l'a mentionné un des répondants, de toutes les catégories de crime, le cybercrime est le plus populaire, car les risques sont très faibles et les gains possibles très élevés.

On a demandé aux répondants de quelle manière les organisations criminelles utilisent ou pourraient utiliser les sites de médias sociaux. Aux fins de l'analyse, leurs réponses ont été divisées selon les thèmes suivants : établissement de liens et recrutement (ou non) à l'aide des médias sociaux, coordination des activités criminelles à l'aide des médias sociaux et victimisation au moyen des médias sociaux. Les réponses ont été jumelées aux renseignements issus de la littérature universitaire et des médias d'information pour brosser un portrait plus clair des sujets abordés par les répondants.

Établissement de liens et recrutement (ou non) à l'aide des médias sociaux

Les sites des médias sociaux donnent l'occasion aux personnes d'interagir avec d'autres personnes et d'autres organisations partout dans le monde. De nombreuses personnes impliquées dans le crime organisé sont conscientes du risque que leur vraie identité soit liée à leur présence en ligne et, par conséquent, sont réticentes à utiliser les sites de médias sociaux à titre d'outils de communication (Weimann 2010, p. 48). Un des répondants a mentionné que l'on peut facilement trouver en ligne de nombreux groupes criminels bien connus, comme les Hell's Angels, parce que ces derniers utilisent les sites de médias sociaux. Cet énoncé est étayé par les travaux de Morselli et Décary-Hétu (2010), lesquels ont trouvé des groupes criminels bien connus comme les Crips, les Hell's Angels et les Latin Kings sur les principaux sites de médias sociaux en utilisant des recherches par mots-clés sur Twitter, Facebook et MySpace. Selon un répondant faisant des enquêtes en cybersécurité, les membres des Hell's Angels ne discutent pas d'activités criminelles en ligne. Ce répondant a indiqué que les Hell's Angels se servent des sites de médias sociaux pour faire la promotion de leur organisation en donnant son appui à la sous-culture des motards criminalisés. Le groupe ne publicise pas sa participation à des activités illégales sur les sites de médias sociaux. Bien qu'il ne puisse pas donner de détails, un des répondants de l'échantillon des responsables de l'application de la loi prétend que certains membres importants de gangs de rue utilisent les sites de médias sociaux. Ils s'en servent à des fins sociales et exposent très rarement des détails liés à des activités criminelles. Ces constatations correspondent aussi aux travaux effectués précédemment dans le domaine des cyberactivités de gangs (Morselli et Décary-Hétu 2010).

Contrairement aux travaux de recherche antérieurs (Morselli et Décary-Hétu 2010), deux répondants participant à l'étude actuelle ont indiqué que les membres de gangs utilisent les sites de médias sociaux en vue d'intimider d'autres gangs, de commettre de la fraude et de recruter des membres. Qu'il s'agisse de recrutement ou de promotion de la sous-culture des gangs, certains répondants conviennent que les organisations criminelles pourraient utiliser les sites de médias sociaux pour rendre plus efficaces leurs activités de recrutement et étendre leurs opérations en rejoignant un plus grand auditoire.

Le recrutement effectué à l'aide des médias sociaux est plus évident dans le monde du terrorisme. À titre d'exemple, en 2009, les Tigres de libération de l'Eelam tamoul, un groupe utilisateur de Youtube, ont diffusé plus de 100 vidéos de propagande; les plus récents vidéos ont été doublés ou sous-titrés en anglais. La recherche démontre que les vidéos dont le contenu fait la promotion du terrorisme ont une vaste diffusion, ce qui peut contribuer à la croissance d'une base d'appui en dehors du Moyen-Orient et de l'Afrique du Nord (Weimann 2010).

Coordination des activités criminelles à l'aide des médias sociaux

Certaines données portent à croire que les sites de médias sociaux servent depuis longtemps aux fins de planification et d'organisation des activités criminelles. Selon un rapport du 304^{e} bataillon de renseignement de l'armée des États-Unis, les sites de médias sociaux, comme Twitter, pourraient devenir un outil de coordination efficace pour les terroristes en vue de lancer des attaques (Weimann 2010, p. 48). La capacité d'actualisation instantanée permet aux personnes impliquées dans le terrorisme d'organiser des attaques plus précises en facilitant des mises à jour en temps réel. Selon Weimann (2010), 90 % des activités terroristes menées sur Internet sont organisées à l'aide d'outils de réseautage social. De plus, un répondant a indiqué qu'au Mexique YouTube est un outil publicitaire puissant utilisé pour idéaliser les activités du crime organisé et pour diffuser des messages de menace aux forces de l'ordre et aux cartels de la drogue.

Bien que cette question n'ait pas été abordée par les répondants, il existe des preuves que des réseaux criminels sont actifs dans les forums Web et les services de clavardage IRC (voir, par exemple, Smyth 2011).

Victimisation au moyen des médias sociaux

De tous les cybercrimes signalés au Internet Crime Complaint Center du FBI[4] (Internet Crime Complaint Centre 2010), le type de plainte le plus courant est la fraude; 8 des 10 principaux types de crimes signalés au centre étaient de la fraude. Sur l'ensemble des victimes de fraudes, 70 % d'entre elles avaient été victimisées dans le cadre d'activités en ligne (Internet Crime Complaint Centre 2010). Traditionnellement, la fraude est commise par des personnes travaillant seules (Kapardis et Krambia-Kapardis 2004). Ce n'est plus le cas; une grande partie de la fraude est commise à l'aide du pollupostage, de l'hameçonnage et de l'escroquerie. À titre d'exemple très courant d'escroquerie contemporaine, notons la fraude 419 commise à l'aide d'un courriel en

[4] Bien que ce centre soit géré par le FBI, il reçoit des plaintes de partout dans le monde.

provenance du Nigéria où on demandait au destinataire d'envoyer une avance (Buchanan et Grant 2001).

Ce qui suit est un exemple d'une telle escroquerie. D'importantes sommes d'argent étaient supposément disponibles en vue d'un héritage, mais elles devaient être envoyées dans un autre pays, ce qui nécessitait un paiement préalable. La victime qui aidait à la transaction aurait une part de l'héritage. Les frais d'administration, dont le paiement est demandé à la victime, retardent la transaction et d'autres frais s'en suivent. Quelques détails ont été fournis par un des répondants du milieu de l'application de la loi qui a fait une enquête sur une telle escroquerie. L'enquête a démontré que le courriel de la fraude 419 avait été envoyé à partir de l'Afrique de l'Ouest et ciblait des gens partout dans le monde. Quiconque répondait au courriel était renvoyé à des complices au Canada aux fins de communications subséquentes. Les frais payés par la victime étaient envoyés en Chine. Toute somme reçue était alors transférée de la Chine au Canada, puis au Royaume-Uni et enfin en Afrique. Des entreprises criminelles nigériennes sont habituellement derrière ces escroqueries. Ces organisations criminelles ne possèdent pas une structure hiérarchique (Buchanan et Grant 2001). Comme bon nombre d'organisations criminelles contemporaines, les entreprises criminelles nigériennes n'affichent pas une chaîne précise de commandement ou de communication, mais elles sont créées et interconnectées en fonction de leur pertinence, de leurs compétences et de leur rentabilité. Les responsables de cette escroquerie se sont rencontrées dans un forum Internet où les participants étaient cotés par leurs collègues à la lumière d'expériences antérieures.

Parmi les autres types communs de fraude relevés par le Internet Crime Complaint Centre, notons la fraude des rencontres en ligne ou l'escroquerie du cœur. Dans ce type de fraude, les fraudeurs trouvent leurs victimes sur un site populaire de rencontre en ligne, les approchent et commencent une histoire sentimentale. Le but consiste à faire croire à la victime, probablement pendant une longue période de temps, qu'ils éprouvent des sentiments profonds l'un envers l'autre, puis à essayer d'obtenir de l'argent de la victime sous forme de cadeaux ou de prêts. Ce type de fraude tire profit des sentiments amoureux plutôt que d'une promesse de gains financiers pour obtenir frauduleusement des fonds (en moyenne 3 000 $) de la victime (Rege 2009). Bien que certaines de ces escroqueries soient perpétrées par des personnes seules, certaines sont gérées d'une manière semblable à celle des fraudes 419 du Nigéria. Le réseau a tendance à être souple et à recruter des membres au besoin. Certaines personnes sont responsables de créer de faux profils sur les sites de rencontres en ligne. Pour établir un contact avec les victimes possibles, d'autres membres (appelé des « communicateurs ») travaillent la nuit dans des cafés virtuels pour extraire des milliers d'adresses courriel américaines et pour envoyer à chacune d'entre elles un message frauduleux rédigé par des membres (appelés des « exécuteurs ») du même groupe du crime organisé qui sont à l'aise pour s'exprimer dans des langues étrangères de façon à ce qu'ils puissent composer des lettres et des messages appropriés ou avoir des conversations au téléphone. Des « brasseurs de fonds » se chargent de l'aspect financier, et des « transfuges » fournissent à l'organisation criminelle des documents gouvernementaux, financiers et commerciaux légaux, comme des en-têtes officiels, afin de donner des allures de véracité à l'escroquerie. Selon Rege (2009), ce réseau d'escroquerie reçoit sept réponses chaque jour, et les chances qu'elles produisent des gains sont de 70 %.

Certains cambrioleurs professionnels surveillent les comptes Facebook à la recherche d'éventuelles victimes en vacances afin de trouver des occasions de cambriolage. Par exemple, une femme a été victime d'un cambriolage, car un de ses amis s'est introduit chez elle après avoir vu son statut Facebook disant qu'elle serait à un concert le soir même. Le cambrioleur en question a été attrapé après que quelqu'un sur Facebook l'eut reconnu dans la séquence vidéo du vol (Indiana News 2010).

Au dire de deux des répondants, il s'avère maintenant beaucoup plus facile de créer de meilleurs profils et de gagner la confiance des victimes ciblées qu'avant l'avènement des sites de médias sociaux en raison de la quantité phénoménale de renseignements et de photos personnels partagés. Cette constatation correspond à la littérature empirique (Timm et Perez 2010). Les gens sont en mesure d'utiliser cette information pour convaincre les victimes qu'ils se connaissent et pour leur soutirer de l'information en vue de faire des gains financiers. Le cas Bryan Rutberg illustre bien de quelle manière les criminels tirent profit de l'information obtenue des sites de médias sociaux à des fins d'escroquerie.

Le compte Facebook de Bryan Rutberg a été piraté, et le fraudeur a affiché le statut « BRIAN A UN URGENT BESOIN D'AIDE!! » (Timm et Perez 2010). Après la publication du statut, le fraudeur a envoyé des courriels au cercle d'amis Facebook de Ryan disant que ce dernier avait été victime d'un vol pendant son séjour au Royaume-Uni et qu'il avait besoin d'argent pour revenir à la maison (Timm et Perez 2010). Plusieurs amis de Bryan ont subi des pertes financières à la suite de cet incident, car ils ont cru l'histoire et envoyé de l'argent. Au moins deux autres personnes ont été victimes d'un incident semblable : Paul Émile d'Entremont et Scherrman (CBC News 2011; Daily Mail Reporter 2008). Dans le cas de Paul Émile d'Entremont, le fraudeur a trouvé son nom par l'entremise d'une connaissance Facebook et utilisé ce lien pour gagner la confiance de M. d'Entremont. Le fraudeur du cas Scherrman a été jusqu'à faire passer une autre personne comme un agent d'immigration ayant un accent anglais, et a appelé la victime afin qu'elle envoie plus d'argent pour libérer son ami de prison.

De plus, les applications et les fils de nouvelles intégrés dans les sites de médias sociaux peuvent aussi servir à propager des logiciels malveillants, ce qui permet d'exécuter plus rapidement que jamais des attaques d'hameçonnage (Timm et Perez 2010). D'après un des répondants, le seul défi auquel font face les personnes désireuses d'utiliser les médias sociaux à des fins illicites consiste à créer quelque chose qui correspond à ce que veulent les gens ou du contenu avec lequel les gens sympathiseront. En fait, un groupe de voleurs d'identités du Brésil ayant eu recours à des chevaux de Troie bancaires pour voler de l'information à des fins de vol d'identité et de gains financiers s'est servi de Twitter pour créer un réseau de zombies[5] (Timm et Perez 2010). Les intrus ont fait des mises à jour de statut qu'ils ont envoyées à tous les abonnés, faisant de ces derniers les zombies du réseau. Un groupe a également créé un nouveau type de réseau de zombies, le réseau de marionnettes, qui utilise l'interface de programmation de Facebook (Timm et Perez 2010). Les agresseurs ont créé une application qui, lorsque l'utilisateur clique sur un lien dans l'application, lance une attaque contre l'ordinateur ciblé à partir du navigateur de l'utilisateur.

[5] Un réseau de zombies est un réseau d'ordinateurs infectés d'un logiciel malveillant contrôlé pour commettre certains actes (p. ex. du pollupostage), et ce, souvent sans que les propriétaires des ordinateurs en aient conscience.

En ce qui a trait à la propagation des logiciels malveillants, le ver Samy a été en mesure d'infecter plus d'un million de profils d'utilisateur sur MySpace en 24 heures (Timm et Perez 2010). Il a commencé par le profil de Samy, où se trouvait un code malveillant qui pouvait modifier le profil du visiteur. Après une visite du profil de Samy, le code force le visiteur à ajouter Samy dans ses amis et ajoute l'étiquette « Samy est avant tout mon héros » (Timm et Perez 2010). Le code se propage au fil des visites de pages infectées, visites encouragées par des recommandations d'amis, eux-mêmes des victimes. Facebook a subi des attaques de logiciels malveillants semblables en 2009 (Timm et Perez 2010). Une vulnérabilité de l'interface de programmation de Facebook permettait au code malveillant de recueillir les renseignements personnels des utilisateurs sans que l'utilisateur ne le sache.

Discussion

Il y a très peu de recherche sur les caractéristiques démographiques des personnes impliquées dans le crime organisé (Van Koppen 2010). Selon les travaux de Motiuk, au Canada, les délinquants déclarés coupables ayant des liens avec des gangs sont principalement des hommes (98 %), non Autochtones (95 %) et âgés entre 19 et 64 ans. Au moment de l'étude, l'âge moyen de ce groupe était 36 ans. La plupart d'entre eux possédaient déjà un dossier criminel en tant qu'adultes (85 %). Plus des deux tiers avaient purgé des peines d'emprisonnement dans des prisons provinciales et environ 25 % dans des prisons fédérales (Motiuk et Vuong 2005). En raison du manque d'études sur les données démographiques des personnes impliquées dans le crime organisé au Canada, on a aussi étudié les groupes démographiques du crime organisé aux Pays-Bas afin de mieux comprendre les infractions du crime organisé.

Selon les résultats obtenus par Van Koppen et ses collaborateurs, les personnes impliquées dans le crime organisé sont en moyenne âgées de 38 ans au moment de l'infraction, et 70 % d'entre elles étaient âgées entre 30 et 50 ans. L'échantillon ne comptait qu'un seul jeune contrevenant. Les travaux de Van Koppen et ses collaborateurs donnent à penser que ces personnes sont en général des délinquants chevronnés puisque, en moyenne, bon nombre des délinquants plus âgés avaient commis leur première infraction 26 ans auparavant. Les délinquants faisant partie de l'échantillon sont demeurés actifs sur le plan criminel en moyenne pendant une période de 12 ans avant d'être reconnus coupables d'une infraction. En fait, les sujets de l'échantillon étaient en majorité des délinquants adultes dont les activités criminelles n'avaient commencé qu'à l'âge adulte et avaient atteint leur sommet à 40 ans. Leurs principales activités étaient le trafic illégal de divers produits, notamment la drogue, les personnes, les automobiles et les armes à feu.

En ce qui a trait au sexe des délinquants reconnus coupables ayant des liens avec des gangs, la grande majorité (98 %) était des hommes (Motiuk et Vuong 2005). Beare (2010) brosse un portrait général des femmes impliquées dans le crime organisé au Canada. Selon les travaux de recherche de cette dernière, les données démographiques des femmes reconnues coupables d'une infraction liée au crime organisé sont les mêmes que celles d'une délinquante type, c'est-à-dire que ces délinquantes ne sont pas de race blanche, viennent de milieux socio-économiques défavorisés et ont été souvent des victimes d'abus. Beare avance que de plus en plus de femmes ont des rôles de leader dans le crime organisé, mais qu'elles représentent seulement une minorité des délinquants qui sont reconnus coupables.

Les recoupements entre les caractéristiques démographiques des personnes utilisant les médias sociaux et celles impliquées dans le crime organisé peuvent s'avérer utiles pour orienter les enquêtes et les efforts de communication. Une telle comparaison démontre que les personnes impliquées dans le crime organisé ont tendance en général à être des délinquants ayant commencé leurs activités criminelles plus tard et à être plus âgées que celles qui fréquentent les sites de médias sociaux. Ces délinquants sont peut-être moins susceptibles d'utiliser les médias sociaux. Par exemple, comme cela a été démontré, le plus important groupe d'âge des utilisateurs de médias sociaux en ligne était celui des 18 à 34 ans, alors que 70 % des membres de groupes du crime organisé aux Pays-Bas étaient âgés entre 30 et 50 ans (Van Koppen 2010). Dans un contexte canadien, il faut se rappeler que Motiuk et Vuong (2005) ont constaté que l'âge moyen des délinquants ayant des liens avec des gangs était 36 ans. Cette donnée affiche encore une fois une différence par rapport à l'utilisateur type des médias sociaux en ligne, dont l'âge tend à être inférieur à 35 ans. Les deux sites de blogues décrits dans le présent rapport, Blogger et Wordpress, semblent exceptionnellement avoir une cohorte plus âgée d'utilisateurs. Il est possible que les membres d'organisations criminelles, tout comme le public plus âgé, soient plus attirés par les sites de blogues que par Twitter, Facebook ou MySpace, et qu'ils deviennent par conséquent des utilisateurs ou des consommateurs de ces médias sociaux.

Par contre, comme l'ont décrit Morselli et Décary-Hétu (2010), les membres des gangs de rue ont tendance à être âgés entre 18 et 24 ans et font partie de la tranche d'âge type des utilisateurs de médias sociaux. Morselli et Décary-Hétu se sont penchés sur les affirmations des médias selon lesquelles les gangs de rue et les organisations criminelles se servent des sites de médias sociaux. Les auteurs ont constaté que les gangs de rue n'utilisent pas directement les médias sociaux à des fins de recrutement. Les résultats d'une recherche par mots-clés de plus de 50 noms de gangs sur Twitter, FaceBook et MySpace ont démontré que la présence de gangs sur les sites de réseautage social est principalement liée à la promotion d'une culture générale des gangs et de la rue grâce à des témoignages individuels. Dans la plupart des cas, les sites sont conçus et gérés par des membres et des collaborateurs qui mettent l'accent sur leur allégeance aux groupes comme les MS-13, les Crips, les Bloods ou les Latin Kings. L'utilisation de réseaux sociaux sur Internet pour mettre en évidence des exploits illicites, des menaces, des crimes d'honneur ou des membres emprisonnés a été décrite par Gutierrez (2006) comme de la cyberactivité de gangs. Morselli et Décary-Hétu supposent que les sites de cyberactivité de gangs permettent aux gangs de créer un nouveau lieu de convergence afin que les membres puissent interagir avec un plus grand nombre de personnes qui n'auraient probablement jamais été exposées à ce style de vie et d'exploits en situation réelle. Ces sites rendent aussi plus accessible le phénomène des gangs de rue à une plus grande partie de la population. Il est intéressant de noter que, contrairement aux gangs de rue étudiés dans la présente recherche, le groupe de motards criminalisé des Hell's Angels n'utilise pas les réseaux de réseautage social pour décrire des actes criminels ou violents, bien que ce groupe ait une présence importante sur le Web.

Enfin, contrairement à l'utilisateur type des médias sociaux, les femmes impliquées dans des organisations criminelles tendent à ne pas être de race blanche et à venir d'un milieu socio-économique défavorisé (Beare 2010). Ainsi, il est possible que les délinquantes du crime organisé soient moins susceptibles que leurs homologues masculins à utiliser les sites de médias sociaux.

Conclusion

Les sites de médias sociaux en ligne peuvent permettre le renouement d'anciennes amitiés et la participation active dans des discussions d'intérêt commun. Ces sites permettent aux gens de communiquer leurs passe-temps, leurs intérêts, leurs lieux préférés de rassemblement, leurs préférences, leurs aversions, leurs photos, le nom de leurs amis, leur emplacement actuel et d'autres renseignements très personnels. Les sites de médias sociaux ont créé un grand espace pour l'établissement de liens et l'échange d'information. Les gens transmettent beaucoup de renseignements à leurs communautés en ligne, de façon intentionnelle et sans une compréhension explicite. Cette information peut servir à différents protagonistes de diverses manières. À l'aide d'entrevues avec des responsables de l'application de la loi et des experts des médias sociaux de même qu'un examen de la littérature, la présente étude s'est penchée sur les manières dont les organisations criminelles et le milieu de l'application de la loi utilisent et pourraient utiliser les sites de médias sociaux.

Tout comme l'utilisateur moyen des médias sociaux, les personnes impliquées dans le crime organisé utilisent les sites de médias sociaux. À l'instar de travaux de recherche antérieurs, cette étude laisse à penser que les groupes du crime organisé se servent des sites de médias sociaux aux fins de cyberactivité de gang, c'est-à-dire la valorisation ou la promotion de la sous-culture de gang. Contrairement aux travaux de recherche antérieurs, deux répondants participant à l'étude actuelle ont indiqué que les membres de gangs utilisent les sites de médias sociaux en vue d'intimider d'autres gangs ou des personnes, de commettre de la fraude et de recruter des membres.

Les sites de médias sociaux peuvent servir pour coordonner des activités criminelles dans des réseaux de personnes qui ne se sont jamais rencontrées hors ligne, pour trouver des occasions de crime et pour soutirer frauduleusement de l'argent à des gens à l'aide de divers mécanismes. On peut recueillir de l'information sur les réseaux des victimes, sur les personnes soupçonnées d'avoir commis des activités criminelles et sur les agents de police qui communiquent de l'information en ligne.

Les entrevues menées démontrent que les responsables de l'application de la loi utilisent couramment les sites de médias sociaux dans le but de recueillir de l'information qui servira à établir le profil d'un suspect. Les sites de médias sociaux représentent des outils incroyables pour atteindre cet objectif, car, selon la plupart des répondants, les gens ont tendance à faire trop confiance à ces sites et à y mettre trop d'information. L'établissement du profil d'un suspect ne constitue qu'une seule des activités des forces de l'ordre. Les responsables de l'application de la loi se servent aussi de ces sites pour rester en contact avec les collectivités qu'ils desservent et pour être à l'affût d'activités dans la collectivité qu'ils devraient connaître, comme des événements perturbateurs à venir. Les répondants ont aussi mentionné que les médias sociaux peuvent aider à diffuser des directives en cas d'urgence et des bulletins de circulation de même qu'à faire la promotion d'activités spéciales et à demander de l'aide pour la recherche de personnes disparues. Les sites de médias sociaux peuvent aussi servir pour interagir avec la collectivité d'autres façons, par exemple en créant un registre de condoléances lors du décès d'agents de police ou en menant des consultations publiques. En général, les répondants

conviennent que plus grande est l'interaction des forces de l'ordre avec la collectivité, meilleures seront leurs relations avec celle-ci.

La plupart des répondants ont convenu que le personnel des forces de l'ordre doit intégrer les sites de médias sociaux dans leurs activités quotidiennes, tant à des fins d'enquête que de communication. Bien que certains organismes permettent l'utilisation des sites de médias sociaux, les répondants recommandent que l'adoption de telles méthodes soit généralisée et avancent que la prochaine génération de suspects aura fort probablement été exposée aux sites de médias sociaux et qu'elle sera plus susceptible de les utiliser à des fins criminelles et personnelles.

La présente étude comporte certaines limites. Seulement dix entrevues ont été menées auprès de 11 personnes, dont la plupart d'entre elles travaillent dans un contexte canadien. Ce document se concentre sur les blogues, les sites de réseautage social, les microblogues et les sites de partage de médias, ce qui limite nécessairement la portée de la recherche. Enfin, certains répondants étaient réticents à parler des activités des groupes du crime organisé. D'autres travaux de recherche pourraient être entrepris où on interviewerait des personnes reconnues coupables de cybercrimes dans le but d'obtenir plus de données sur ce domaine émergent d'occasions de crime et de communication.

Bibliographie

Alderson, M. « Facebook: a Useful Tool for Police? », *Connectedcops*, 25 janvier 2011. Consulté sur Internet le 3 février 2011 : <http://connectedcops.net/?p=3637>.

Buchanan, Jim et Alex J. Grant. « Investigating and Prosecuting Nigerian Fraud », *United States Attorney's Bulletin*, novembre 2001.

CBC News. « Beware Facebook scams: police », CBC, 6 janvier 2011. Consulté sur Internet le 8 février 2011 : <http://www.cbc.ca/canada/nova-scotia/story/2011/01/06/ns-facebook-scam.html#socialcomments>.

CheckFacebook.com. « Facebook Statistics and Breakdowns », CheckFacebook.com. Consulté sur Internet le 26 janvier 2011 : <http://www.checkfacebook.com/>.

Cheng, Alex et Mark Evans. « Inside Twitter – An In-Depth Look Inside the Twitter World », Sysomos: a Marketwire Company, juin 2009. Sur Internet : <http://sysomos.com/insidetwitter/>.

Daily Mail Reporter. « Facebook hijacked by cyber criminals in scam to con 'friends' out of cash », *Associated Newspapers Ltd*, 11 novembre 2008. Consulté sur Internet le 8 février 2011 : <http://www.dailymail.co.uk/sciencetech/article-1084669/Facebook-hijacked-cyber-criminals-scam-friends-cash.html>.

Felson, Marcus, Ronald V. Clarke. *Opportunity Makes the Thief: Practical Theory for Crime Prevention, Police Research Series, Paper 98*, Barry Webb (éditeur), Londres, Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 1998.

Gerlsbeck, Rob. « The All-Canadian Wealth Test », *MoneySense Magazine*, octobre 2009.

Google, Inc.(a) « Site Profile: domain: myspace.com » Google, Inc. Consulté sur Internet le 26 janvier 2011 : https://www.google.com/adplanner/planning/spite_profile#siteDetails?identifier=myspace.com&geo=CA&trait_type=1&lp=true>.

Google, Inc.(b) « À propos de YouTube », Google, Inc. Consulté sur Internet le 5 février 2011. <http://www.youtube.com/static?hl=fr&template=about_youtube>.

Internet Crime Complaint Centre. *2010 Internet Crime Report*. États-Unis, National White Collar Crime Center, 2011, Consulté sur Internet le 11 mars 2011 :<http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf>

Indiana News. « Woman's Facebook 'Friend' Suspected In Burglary », McGraw-Hill Broadcasting Company, 6 août 2010. Consulté sur Internet le 10 mars 2011. <http://www.theindychannel.com/news/24537182/detail.html>.

Jasra, Manoj. « Blogger Demographic Study by Sysomos », *Web Analytics World*, le 5 juin 2010. Consulté sur Internet le 6 février 2011 : <http://www.webanalyticsworld.net/2010/06/blogger-demographic-study-by-sysomos.html>.

Kapardis, Andreas et Maria Krambia-Kapardis. « Enhancing fraud prevention and detection by profiling fraud offenders », *Criminal Behaviour and Mental Health*, vol. 14, n° 3 (mars 2006), p. 189-201.

Marsico, Edward M., Jr. « Social Networking Websites: Are MySpace and Facebook the fingerprints of the twenty-first century? », *Widener Law Journal*, vol. 19, n° 3 (2010), p. 967-976.

Masterman, Kevin. « Les médias sociaux mis à profit dans la répression du crime », *Gazette*, vol. 72, n° 2, p. 38. Gendarmerie royale du Canada, 2010.

McIntosh, Neil. « Google buys Blogger web service », *The Guardian*. 18 février 2003. Sur Internet : <http://www.guardian.co.uk/business/2003/feb/18/digitalmedia.citynews>.

Morselli, Carlo, et David Décary-Hétu. *L'utilisation des sites de réseautage social à des fins criminelles : étude et analyse du phénomène de « cyberbanging »*. Ottawa, Sécurité publique Canada, 2010.

Motiuk, Laurence et Ben Vuong. *Les délinquants sous responsabilité fédérale condamnés pour une infraction d'organisation criminelle : profil.* Ottawa, Service correctionnel Canada, 2005. Consulté sur Internet : < http://www.csc-scc.gc.ca/text/rsrch/briefs/b38/b38-fra.pdf>.

Oreskovic, Alexei. « MySpace launching new version of website », Reuters, 27 octobre 2010. Consulté sur Internet le 31 octobre 2010 : <http://www.reuters.com/article/2010/10/27/us-myspace-idUSTRE69Q11M20101027>.

Ostrow, Adam. « You can now login to Myspace with Facebook », Mashable, Inc, 18 novembre 2010. Sur Internet : <http://mashable.com/2010/11/18/you-can-now-login-to-myspace-with-facebook/>.

Quantcast. Renseignement recueillis sur Internet le 1er février 2011 : http://www.quantcast.com/.

Quantcast. *Quantcast Methodology Overview*. 2008. Consulté sur Internet le 1er février 2011 : <www.quantcast.com/white-papers/quantcast-methodology.pdf>.

Rege, Aunshul. « What's Love Got to Do with It? Exploring Online Dating Scams and Identity », *International Journal of Cyber Criminology*, vol. 3, 2 (2009): p. 494-512.

Smyth, Sara et Rebecca Carleton. *Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources*. Ottawa, Sécurité publique Canada, 2011.

Timm, Carl et Richard Perez. *Seven deadliest social network attacks*. Rockland, Massachusetts: Syngress, 2010.

Weimann, Gabriel. « Terror on Facebook, Twitter, and Youtube », *The Brown Journal of World Affairs*, vol. 16, n^{o} 2 (2010), p. 45-54.