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

2

Réseaux sans fil et éléments criminogènes

Karine Baillargeon-Audet[1]
Francis Fortin[2]

Depuis son apparition au début des années 2000, Internet sans fil n'a cessé de gagner en popularité, car il est peu coûteux, il est puissant et il fonctionne bien (Anderson, 2003). Internet sans fil, aussi connu sous le nom de Wi-Fi, se retrouve souvent dans les foyers et est de plus en plus présent dans les endroits publics comme les commerces, les établissements scolaires, les hôpitaux et les parcs. Plusieurs projets ont été mis sur pied, surtout dans les grands centres urbains, afin d'offrir un accès à Internet sans fil dans des endroits publics. Par exemple, plusieurs villes québécoises ont vu apparaître des organismes ayant pour objectif de faciliter la mise en place de ces services. Parallèlement à cette augmentation de la couverture d'Internet, un grand nombre de dispositifs portatifs accèdent maintenant au Web. Il est dorénavant possible, avec les téléphones cellulaires, d'utiliser une connexion Internet en remplacement des ondes de téléphonie cellulaire. Les incitatifs des fournisseurs d'accès à la téléphonie sont importants : tout appel fait par

1. École de criminologie de l'Université de Montréal.
2. Chercheur associé, Centre international de criminologie comparée, et candidat au doctorat, École de criminologie de l'Université de Montréal.

l'intermédiaire d'Internet est sans frais[3]. De plus, les nouveaux téléphones « intelligents », comme le BlackBerry et l'iPhone, permettent de se brancher à Internet pour utiliser des applications Web spécifiquement conçues pour eux. Il y a aussi le nouveau baladeur d'Apple, l'iPod Touch, grâce auquel on peut se connecter sur Internet pour acheter de la musique, surfer, envoyer des courriels et utiliser la plupart des services offerts sur Internet. Enfin, les tablettes électroniques comme l'iPad peuvent également se connecter à Internet sans fil. L'augmentation des points d'accès dans les endroits publics ainsi que le nombre accru de dispositifs permettant de s'y brancher soulèvent une série de questions. On peut s'interroger sur l'ampleur de l'utilisation d'Internet sans fil dans le monde et plus particulièrement au Canada. Quelles sont les dispositions de la législation canadienne s'appliquant aux réseaux sans fil? Pour terminer, nous étudierons les raisons poussant à croire que ces réseaux peuvent être utilisés à des fins criminelles, en soulignant l'importance du sentiment d'anonymat dans la commission d'infractions.

2.1 Définition

Le Wi-Fi est une technologie de réseau informatique permettant d'avoir accès à Internet sans que l'appareil utilisé pour ce faire soit relié par câble au fournisseur Internet. Sur un plan plus technique, le fonctionnement du Wi-Fi est possible grâce à un protocole qui régit les communications à l'intérieur d'un réseau sans fil (PCMag, 2012). Le protocole le plus utilisé est le standard 802.11, notamment les variantes a, b, g (Boutin, 2003) et n. L'accès à Internet sans fil est possible grâce à des points d'accès qui communiquent par ondes radio ou par fil avec des fournisseurs d'accès Internet. Ces points d'accès peuvent émettre et recevoir des signaux dans un rayon pouvant habituellement atteindre de 20 à 50 mètres, parfois plus dans des conditions optimales. Les signaux reçus par un point d'accès peuvent être atténués par la distance, ils peuvent aussi souffrir

3. Le 6 mai 2008, un communiqué de presse annonçait : « Montréal, le 6 mai, CNW – Fido a lancé aujourd'hui son nouveau service Fido UNO(MC), une première dans l'industrie du sans-fil au Canada. Le fonctionnement du service Fido UNO est assuré par la liaison entre un appareil compatible et une connexion Internet haute vitesse à la maison ou au réseau sans fil de Fido, pendant les déplacements. Le client profite d'une mobilité simple, ininterrompue, et de la meilleure communication combinée qui soit (…) »

de distorsion en se reflétant sur des objets et ils peuvent connaître des problèmes d'interférence (Hills, 2005).

2.2 Utilisation des réseaux sans fil dans le monde et au Canada

Selon les informations de JiWire[4], on considère que la Grande-Bretagne est le pays ayant le plus de points d'accès à Internet dans des lieux publics, suivie des États-Unis. Dans ce pays, c'est dans l'État de New York que le Wi-Fi est le plus accessible, avec environ 14 581 points d'accès (JiWire, 2011). Plusieurs projets ont été mis sur pied un peu partout dans le pays, comme à San Francisco, où Google et EarthLink se sont unis en 2006 pour bâtir le réseau sans fil de la ville (Associated Press, 2006). Toutefois, plusieurs villes américaines ont suspendu leur projet de Wi-Fi en raison de différends avec les compagnies avec lesquelles elles font affaire (Leduc, 2007).

Avec ses 5 417 points d'accès recensés, le Canada ne se classe pas parmi les 10 pays ayant le plus de points d'accès. Il est important de noter que les points d'accès sont principalement concentrés dans les grandes villes (JiWire, 2011). Plusieurs grandes villes canadiennes ont lancé des projets pour que leurs citoyens aient accès au Wi-Fi. Depuis le lancement de One Zone à Toronto, en septembre 2003, plus de 40 000 Torontois et visiteurs ont pu tester le réseau sans fil offert dans une zone de six kilomètres carrés (Guglielminetti, 2007). Hydro Toronto a lancé son service d'Internet sans fil dans le centre-ville le 24 avril 2007, permettant ainsi à un grand nombre de personnes d'y avoir accès. Le gouvernement de la Saskatchewan a également un projet de réseau sans fil pour ses quatre plus grandes villes. Ce projet consiste à bâtir le plus grand réseau Wi-Fi du pays, qui offrirait aux habitants et aux touristes un accès gratuit à Internet sans fil à partir d'émetteurs installés au centre-ville et dans les établissements postsecondaires (Smith, 2007).

4. JiWire est une compagnie ayant pour mission de recenser et de répertorier les points d'accès publics à travers le monde. Chaque semaine, elle recense les pays, les villes et les endroits où un service Wi-Fi gratuit est disponible. Il est possible que certains points d'accès n'aient pas été recensés, ce qui pourrait faire en sorte que les points d'accès soient en réalité plus nombreux.

Au Québec, 743 points d'accès ont été recensés en décembre 2011 (JiWire, 2011), dont la plupart se situent sur l'île de Montréal. En effet, il semble rentable pour les commerçants de Montréal d'offrir Internet sans fil dans la mesure où ce service attire les consommateurs (Ritoux, 2007). Plusieurs projets visant à augmenter le nombre de points d'accès à Internet sans fil au Québec sont en développement, notamment celui d'un groupe communautaire à but non lucratif, Île Sans Fil. Ce groupe a pour mission de fournir un accès gratuit à Internet à Montréal. En novembre 2011, Île Sans Fil englobait 210 points d'accès à travers la ville (Île Sans Fil, 2011). Plusieurs autres villes québécoises, comme Québec, manifestent l'intention d'emboîter le pas à cette initiative (Ville de Québec, 2011). Il semble que les points d'accès à Internet sans fil se multiplieront dans les espaces publics au cours des prochaines années.

En effet, dans une étude, la Wireless Broadband Alliance (WBA) estime que le nombre de points d'accès connaîtra une augmentation de 350 % d'ici à 2015. Cette augmentation s'expliquerait par le nombre croissant de téléphones intelligents et de tablettes électroniques en circulation. L'étude révèle également que le nombre de connexions à partir de téléphones intelligents devrait dépasser le nombre de connexions à partir d'ordinateurs portables (Wireless Broadband Alliance, 2011). Nous avons des raisons de croire que ces prédictions sont réalistes, et ce, pour plusieurs raisons. Tout d'abord, selon Negroponte (2002), un des fondateurs du MIT Media Lab, les télécommunications ont connu trois formes de changements majeurs au cours des dernières décennies. Premièrement, dans les années 1970, il y a eu la transformation numérique du multimédia. La deuxième évolution a été l'avènement de la communication orientée en paquets (*packet switching : always on connectivity*). La troisième a consisté en l'arrivée de la communication sans fil, qui est reliée à une meilleure fonctionnalité et à la mobilité des usagers. Nous serions donc toujours à cette étape. De plus, le développement dans le domaine des technologies d'Internet sans fil est toujours en effervescence. Par exemple, le Li-Fi est en développement et se caractérise par la transmission de données sans fil grâce aux DEL (diodes électroluminescentes). En faisant varier l'intensité de la lumière de façon tellement rapide que l'œil humain ne peut pas le voir, cette technologie transfère les données plus rapidement que le câble haute vitesse. Le Li-Fi est également sécuritaire dans les hôpitaux, là où les ondes radio sont bannies. La technologie est disponible depuis 2012 (Keats, 2011).

2.3 Protocoles de sécurité et réseaux sans fil : le jeu du chat et de la souris

Internet sans fil offre certains avantages aux pirates informatiques par rapport aux réseaux traditionnels. Si un pirate devait, dans un monde filaire, trouver un accès matériel pour être physiquement branché afin de se retrouver à l'intérieur du réseau, le Wi-Fi lui permet d'atteindre le même résultat sans contrainte physique. Comme la première étape pour réaliser une attaque importante demeure sans doute l'accès à une porte d'entrée sur le réseau, cette occasion s'avère intéressante à saisir. Cela est tout aussi valable dans un contexte de réseau d'entreprise que dans un contexte domestique, lorsqu'on désire obtenir l'accès aux ressources informatiques d'un voisin. Pour de nombreux utilisateurs, l'utilisation non autorisée d'un point d'accès sans fil constitue encore une banalité sans conséquence. Or, quels avantages au juste peut représenter la prise de contrôle d'un point d'accès résidentiel ou corporatif? D'abord, la prise de contrôle d'un point d'accès appartenant à quelqu'un d'autre peut augmenter le sentiment d'anonymat pour commettre d'éventuelles attaques : le pirate peut camoufler l'origine de ses attaques en empruntant une adresse IP qui agira comme un écran dans la chaîne des communications. Ensuite, en entrant subrepticement sur le réseau, le pirate a un accès plus direct aux ressources disponibles comme l'exploration et l'exploitation d'autres ordinateurs appartenant au même réseau. Avec ou sans fil, les réseaux sont habituellement configurés pour faire davantage confiance aux ordinateurs branchés sur un même réseau. Finalement, une fois sur le réseau, il est possible « d'écouter » ce qui se passe sur celui-ci. Dans certains cas, il peut s'agir de tenter d'intercepter des mots de passe échangés, alors que dans d'autres, il s'agira d'intercepter des informations personnelles ou confidentielles.

Tous ces cas de figure sont possibles à la condition que l'attaquant soit dans le rayon de couverture d'un réseau sans fil. Afin d'accéder illégalement à ces réseaux, les pirates ont pu compter sur des protocoles de communication de réseaux sans fil comportant certaines failles relevées par des chercheurs voulant améliorer le protocole ou encore par des pirates voulant les exploiter.

Si le passé est garant de l'avenir, ce jeu entre l'adoption de protocoles de sécurité, la découverte de leur vulnérabilité et leur remplacement par des protocoles moins vulnérables continuera encore longtemps.

Or, le premier protocole qui a été mis sur le marché est le WEP (*Wired Equivalent Privacy*). Ce protocole, lancé en 1999, était le premier destiné à sécuriser les échanges sur les réseaux sans fil. Il a rapidement reçu le sobriquet de « Weak Encryption Protocol » (faible protocole de cryptage), puisque la clé de chiffrement pouvait facilement être déduite grâce à l'analyse statistique des paquets échangés sur le réseau à l'aide d'un logiciel fourni gratuitement sur Internet (*Aircrack Wifi Password-Cracking*). En 2003, la Wi-Fi Alliance a annoncé que le protocole WPA (*Wi-Fi Protected Access*) allait devenir la nouvelle norme en matière de protection sans fil (Anderson, 2011). Encore une fois, on a décelé une faille dans ce protocole lors de la connexion du client au point d'accès grâce à des techniques de tests répétés de mots de passe. Cette même technique a aussi servi à pirater le protocole WPA2, qui constitue la version la plus sécuritaire actuellement disponible. Puisque ces techniques tentent de deviner les mots de passe, WPA2 constitue encore à ce jour un protocole avec un niveau acceptable de sécurité. Il revient donc à l'utilisateur de choisir un mot de passe long et complexe.

L'ensemble des opérations visant à pénétrer dans un système informatique protégé constitue des infractions dans plusieurs pays du monde. Voyons les détails de la loi au Canada.

2.4 Législation canadienne s'appliquant aux réseaux sans fil

Si, traditionnellement, la proximité physique avec un fil reliant l'internaute et Internet était nécessaire, la porte d'entrée sur le réseau ne comporte maintenant plus cette limite. Ainsi, il est difficile de contrôler la portée du signal que peut émettre un routeur domestique ou un routeur installé dans un environnement commercial. Notons qu'il ne s'agit pas ici de s'attarder sur les crimes qui peuvent se commettre sur Internet, puisqu'ils ne se distinguent pas des crimes commis sur un réseau classique, mais bien sur les crimes qui sont propres à l'utilisation des réseaux Wi-Fi. En raison de l'interprétation restrictive qui est de rigueur en droit criminel, notons également qu'il est périlleux de faire correspondre des crimes qui existent avec des actes problématiques sans précédents. Le tableau 2.1 montre les infractions possibles dans ce contexte où il existe de plus en plus de réseaux sans fil, lesquels peuvent représenter des cibles et des portes d'entrée pour des utilisateurs malveillants.

Tableau 2.1 Articles du Code criminel pouvant être utilisés en lien avec Internet sans fil

Articles du Code criminel	Exemples d'infractions
326(1) : Vol de service de télécommunication	Naviguer sur Internet sans autorisation
327 : Possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunication	Possession sans excuse légitime d'instruments particulièrement utiles et destinés à la commission de l'infraction d'obtenir un service en matière de télécommunication
342.1 : Utilisation non autorisée d'ordinateur	342.1 : Changer les paramètres d'accès du propriétaire
	342.1(1)a) : Naviguer dans Internet sans autorisation, car l'accès Internet est possible grâce à l'ordinateur du propriétaire du réseau sans fil qui est relié au Fournisseur de service Internet (FSI)
	342.1(1)b) : Entraver une communication sans fil en la bloquant, la brouillant ou l'altérant
	342.1(1)c) : • Il y a utilisation d'un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa 342.1(1)a). L'ordinateur du client utilisé pour solliciter le serveur du FSI et le portable qui est utilisé par le suspect sont visés au sens de cet alinéa • S'introduire dans un réseau local sans autorisation
	342.1(1)d) : Décrypter un mot de passe réseau
342.2 : Possession, sans justification ou excuse légitime, de moyens permettant d'utiliser un service d'ordinateur	342.2(1) : Quiconque, sans justification ou excuse légitime, fabrique, possède, vend, offre en vente ou écoule des instruments, ou des pièces de ceux-ci, particulièrement utiles à la commission d'une infraction prévue à l'article

Selon l'article 326(1) du Code criminel, commet un vol quiconque, frauduleusement, malicieusement ou sans apparence de droit, « se sert d'installations ou obtient un service en matière de télécommunication ». Le Code criminel définit le terme « télécommunication » comme toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par fil, radioélectricité, optique ou autres systèmes électromagnétiques. On peut constater qu'Internet sans fil correspond en tout point à cette définition d'un service de télécommunication. Par exemple, dans un café Internet, il est interdit de naviguer sur un réseau

payant sans permission ou encore d'utiliser la connexion d'un voisin sur un réseau non sécurisé. Afin d'obtenir un accès non légitime, il se pourrait qu'un individu ait utilisé des instruments conçus à cet effet. Selon l'article 327 du Code criminel, il est interdit de posséder sans excuse légitime des instruments ou des pièces particulièrement utiles pour utiliser des installations ou pour obtenir un service en matière de télécommunication.

L'alinéa 342.1(1)c) du Code criminel s'applique pour l'infraction qui correspond à s'introduire dans un réseau local sans autorisation. En effet, afin d'accéder au réseau sans fil, il faut passer par l'ordinateur du propriétaire. Un suspect pourrait vouloir obtenir l'accès à un réseau qui a été préalablement sécurisé par ses propriétaires. Il devrait donc « forcer l'entrée » du réseau en tentant de deviner le mot de passe. Or, décrypter un mot de passe constitue une infraction au Code criminel canadien.

Selon l'alinéa 342.1(1)d) du Code, il est interdit d'avoir en sa possession ou d'utiliser un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas a), b) ou c), d'en faire le trafic ou de permettre à une autre personne de l'utiliser. Après avoir obtenu un accès (légitime ou non), un individu pourrait vouloir capter des mots de passe des usagers branchés sur ce réseau. Entraver une communication sans fil en la bloquant, en la brouillant ou en l'altérant est également une infraction à l'alinéa 342.1(1)b) du Code criminel. Grâce à un brouilleur de signaux, il est possible d'empêcher toutes les communications sans fil sur un périmètre et un signal donnés.

L'alinéa 342.1(1)a) du Code criminel s'appliquerait également dans ce cas précis qui correspond à l'utilisation non autorisée d'un ordinateur. On pourrait également citer l'alinéa 342.1(1)c), car il y a utilisation d'un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa 342.1(1)a). Le portable qui est utilisé par le suspect est visé au sens de cet alinéa. Il n'est pas nécessaire qu'il soit démontré qu'il y a eu accès à Internet.

L'article 342.2 du Code criminel prohibe la possession, sans justification ou excuse légitime, de moyens permettant d'utiliser un service d'ordinateur. Toutefois, il pourrait être difficilement applicable, car les instruments sont souvent vendus de façon légitime, parfois par les fournisseurs de service Internet eux-mêmes.

2.5 Impact criminogène des réseaux sans fil : étude sur les points d'accès montréalais[5]

Afin d'examiner les stratégies, les techniques et les outils qui pourraient être employés par les personnes utilisant Internet sans fil à des fins criminelles, des observations ont été effectuées à l'automne 2007 dans des lieux publics où un accès à Internet sans fil était disponible. Ces observations ont permis de constater les problèmes inhérents à la diffusion élargie des accès à Internet sans fil (cafés Internet, réseaux corporatifs non protégés, universités, points d'accès, résidences, etc.). Ainsi, la méthodologie de l'étude Baillargeon-Audet (2007) a consisté à choisir aléatoirement 25 lieux publics dans lesquels Internet sans fil était disponible, afin d'identifier les caractéristiques physiques et criminologiques de chacun de ces points d'accès[6]. L'échantillon était composé de treize commerces, de deux établissements scolaires, de deux lieux de transport, de six parcs, d'une bibliothèque et d'un centre communautaire. Parmi les données recensées pour ces points d'accès figuraient des renseignements généraux sur le lieu, des détails sur les éléments de prévention situationnelle (surveillance et contrôle d'accès) ainsi que des informations techniques sur les caractéristiques d'Internet sans fil. Voici les conclusions de l'étude.

- Fort pourcentage d'occupation : Le nombre de personnes présentes peut influencer le sentiment d'anonymat de la personne qui utilise Internet sans fil. Les gens autour peuvent jouer le rôle de gardiens, ce qui peut diminuer le sentiment d'anonymat de l'utilisateur, car ces « gardiens » peuvent voir ce qu'il y a sur l'écran du portable utilisé. Dans les endroits restreints comme les commerces où beaucoup de gens sont présents, il est plus facile d'effectuer de la surveillance.
- Présence d'employés : Cela signifie la présence de gardiens. En effet, les employés pourraient voir ce qui s'affiche sur l'écran d'un utilisateur.

5. Cette section est issue d'un stage au module de cybersurveillance et de vigie de la Sûreté du Québec dans le cadre du baccalauréat en criminologie.
6. La recension de ces lieux publics s'est faite à l'aide des sites Internet qui servent à localiser des points d'accès.

- Présence de caméras : Il devient possible d'identifier une personne qui aurait utilisé Internet sans fil à des fins criminelles. La caméra peut également agir à titre de gardienne.
- Absence de recoins et de cachettes : Un endroit où il est impossible de voir ce qu'il y a sur l'écran de l'internaute est considéré comme un recoin ou une cachette. Il s'agit d'un élément important, car même s'il y a beaucoup de gens, il devient possible de dissimuler ce qui s'affiche sur l'écran de l'ordinateur.
- Inaccessibilité à partir d'une voiture : Il s'agit également d'un élément important, car tous les éléments de prévention situationnelle qui se trouvent dans le lieu public où Internet sans fil est disponible n'ont plus d'importance si Internet sans fil est accessible à partir d'un autre endroit. Par exemple, s'il y a des caméras dans un commerce, mais qu'Internet sans fil est accessible à partir du stationnement de ce commerce, il devient impossible d'identifier un utilisateur.
- Paiement : Le fait qu'un paiement soit exigé signifie souvent qu'une identification est nécessaire pour se connecter au réseau sans fil.
- Connaissances des employés : Si les employés possèdent des connaissances sur ce qu'est Internet sans fil, ils seront plus portés à surveiller et à déconnecter Internet après les heures d'ouverture du commenrce.

Ainsi, la thèse avancée est que certains éléments de prévention situationnelle sont plus susceptibles de diminuer le sentiment d'anonymat des utilisateurs d'Internet sans fil ayant des intentions criminelles. Il y a donc lieu de prendre davantage ces éléments en considération lorsqu'il est question d'élaborer des programmes de prévention.

Grâce à un système de pointage, un palmarès des « meilleurs endroits » pour commettre des crimes (ceux qui offrent le niveau d'anonymat le plus élevé) à l'aide d'Internet sans fil a été dressé. La connaissance de ces « meilleurs endroits » permet d'envisager des solutions au problème. Voici un résumé des résultats.

- Les parcs se classent généralement en haut de la liste. Cela s'explique par l'absence d'éléments de prévention situationnelle. En effet, il n'y a souvent aucun employé ni aucune caméra de surveillance sur

les lieux, et le pourcentage d'occupation est généralement faible. De plus, les cachettes et recoins sont nombreux.

- Les commerces se répartissent à tous les niveaux du palmarès. Les résultats dépendent des éléments de prévention situationnelle qui se trouvent dans le commerce. Un commerce avec peu de surveillance, l'absence de caméras et un faible pourcentage d'occupation risque de se retrouver en haut de la liste. À l'inverse, un commerce présentant plusieurs éléments de prévention situationnelle risque de se retrouver en bas de la liste.
- Les transports se retrouvent en bas de la liste. Premièrement, il y a beaucoup d'achalandage et, deuxièmement, le contrôle d'accès est assez dissuasif : il faut absolument payer par carte de crédit.

Plusieurs éléments sont à considérer lorsqu'il est question d'Internet sans fil et de son utilisation à des fins criminelles. Parmi ceux-ci se retrouvent des éléments de prévention situationnelle. L'absence de « gardiens » accentue de façon considérable le sentiment d'anonymat. Le processus d'identification à Internet sans fil peut également avoir un rôle important à jouer dans le sentiment d'anonymat. Le manque de connaissances des employés d'un commerce où se trouve un accès à Internet sans fil doit aussi être considéré. Il reste certainement de la sensibilisation à faire, auprès des fabricants de dispositifs sans fil d'abord. Étant donné que le processus d'identification pour les réseaux sans fil est souvent un élément problématique, on pourrait obliger les utilisateurs à fournir un mot de passe, ce qui les identifierait automatiquement. Nous avons observé que cette tendance est déjà en amélioration. Ensuite, on pourrait confier un rôle de prévention accru aux fournisseurs de service Internet sans fil. Des groupes comme Île Sans Fil ont déjà commencé à le faire.

2.6 Exemples

Nous avons vu que l'utilisation d'Internet sans fil est désormais répandue au Canada et au Québec. Malgré le nombre de lois qui pourraient s'appliquer aux infractions reliées à Internet sans fil et l'impact criminogène de certains points d'accès sans fil, il semble encore que très peu de crimes de ce type soient judiciarisés au Canada. Soulignons toutefois un cas survenu aux États-Unis et un autre qui s'est produit au Canada.

En 2009, Barry Ardolf, un Américain de 46 ans, a fait de la vie de ses voisins un enfer en piratant à répétition leur connexion Wi-Fi. Il a utilisé illégalement leur connexion dans le but de commettre différents types de crimes pour qu'ils en soient accusés, et ce, afin de détruire leur réputation professionnelle et leur mariage. Motivé par la vengeance à la suite d'une plainte faite à la police par ses voisins qui l'accusaient d'avoir embrassé leur fils de quatre ans sur la bouche, Barry Ardolf a utilisé leur connexion Internet pour commettre des crimes reliés à la pornographie juvénile, faire du harcèlement criminel, tenir plusieurs types d'inconduites professionnelles et envoyer des courriels de menaces à des politiciens. Pour ce faire, il a téléchargé un logiciel de piratage et a passé deux semaines à décrypter la protection WEP de ses voisins.

Comme l'une des victimes travaillait pour une firme d'avocats et clamait son innocence, son patron a engagé un détective privé pour aller au bout de cette affaire. En installant un renifleur de paquets (*packet snifer*) sur son ordinateur, un logiciel qui permet de voir les données non chiffrées qui transitent, le détective a pu constater du contenu au nom du suspect. Le FBI a donc obtenu un mandat pour fouiller la maison et l'ordinateur de ce dernier, ce qui leur a permis de mettre la main sur plusieurs preuves accablantes et de procéder à son arrestation. Il a été condamné à 18 ans de prison, une longue sentence selon son avocat, étant donné qu'il s'agissait d'une première offense.

Au Canada, il semble qu'un seul crime perpétré à l'aide d'Internet sans fil ait été répertorié dans les médias jusqu'à maintenant (Shim, 2003). En 2003, Walter Nowakowski, un Torontois de 36 ans, s'est fait intercepter par la police de Toronto pour une infraction au Code de la sécurité routière. Les policiers ont surpris le conducteur sans vêtements sous la ceinture, avec sur le siège avant un ordinateur portable sur lequel jouait une vidéo de pornographie juvénile. L'homme utilisait la connexion Internet sans fil non protégée d'une résidence qui se trouvait non loin de là. Un mandat a été obtenu et une grande quantité de matériel de pornographie juvénile a été trouvée sur le disque dur de son ordinateur. Walter Nowakowski a été accusé de possession, de distribution et de production de pornographie juvénile, et également de vol de service de télécommunication. Comme il s'agissait d'une première au Canada selon les autorités, cet incident a permis d'éveiller les consciences quant à la possibilité qu'un réseau non sécurisé soit piraté (CTV.news.ca, 2003).

2.7 Perspectives d'avenir

Internet sans fil étant de plus en plus accessible, il devient important de s'attarder à la problématique du Wi-Fi et de son utilisation à des fins criminelles. En l'absence de contrainte physique, les pirates savent reconnaître l'opportunité criminelle. Ils sont conscients qu'ils ont la possibilité d'augmenter leur sentiment d'anonymat, ce qui leur permet d'explorer et d'exploiter d'autres ordinateurs dans le but d'intercepter des informations personnelles tout en ayant une certaine tranquillité d'esprit. L'exploitation des failles des protocoles de communication a eu comme conséquence la création de nouveaux protocoles. Bien qu'on en soit arrivé à un niveau acceptable de sécurité, il est très probable que d'autres personnes chercheront à repousser les limites de la technologie afin de mieux comprendre son fonctionnement et, par le fait même, trouveront de nouvelles failles à exploiter.

De plus en plus, les utilisateurs d'Internet sans fil sont conscients qu'il y a des risques liés à la sécurité des données qu'ils transmettent au moyen de cette technologie. Pour pirater, il n'est pas nécessaire d'avoir des connaissances particulières; il est possible d'utiliser des scripts ou programmes mis au point par d'autres. Par exemple, Firesheep est un plugiciel qui permet d'accéder à des données de connexion requises pour pirater les sessions Web d'autres utilisateurs sur des réseaux Wi-Fi non sécurisés. Un utilisateur malveillant peut donc avoir accès à des informations personnelles contenues dans des réseaux sociaux requérant un identifiant tels que Facebook, Twitter et Google[7] (Boivin Filion, 2010).

Puisqu'il y a une multiplication des appareils qui utilisent le Wi-Fi et une utilisation grandissante de réseaux Wi-Fi publics, les opportunités criminelles augmentent également. La mobilité qu'assurent aux utilisateurs les nouveaux petits appareils tels que les cellulaires intelligents et les tablettes électroniques pourrait avoir un effet sur le sentiment d'anonymat, puisqu'il est plus facile d'être discret lorsqu'on navigue sur Internet avec ces appareils.

L'étude de Baillargeon-Audet ouvre la voie à d'autres études qui pourront être plus précises quant à leur objet d'étude. Par exemple, elles pourraient cibler un type de cybercrime en particulier, un endroit bien

7. Il est toutefois possible de configurer Google pour qu'il utilise le protocole https afin d'éviter la capture d'informations.

précis où le Wi-Fi est utilisé ou encore les nouveaux types d'appareils permettant d'avoir accès à Internet sans fil.

Bibliographie

ANDERSON, C. (2003). « The Wi-Fi Revolution », *Wired*, mai [En ligne] www.wired.com/wired/archive/11.05/unwired/wifirevolution.html (consulté le 17 janvier 2012).

ANDERSON, C. (2011). « WEP Vs. WPA Wireless Security », *eHow*, 3 juin [En ligne] www.ehow.com/info_8537450_wep-vs-wpa-wireless-security.html (consulté le 4 février 2011).

ASSOCIATED PRESS (2006). « Look Homeward, Google », *Wired*, 16 août [En ligne] www.wired.com/science/discoveries/news/2006/08/71603 (consulté le 22 mai 2007).

BAILLARGEON-AUDET, K. (2007). *Le Wi-Fi et les opportunités criminelles*, Projet de stage non publié, Université de Montréal, Canada.

BOIVIN FILION, A. (2010). « Firesheep : L'extension de Firefox dévoile les identifiants de Facebook et de Twitter », *Branchez-vous techno*, 25 octobre [En ligne] www.branchez-vous.com/techno/actualite/2010/10/firesheep-extension-firefox-devoile-identifiant-site-web.html (consulté le 8 février 2011).

BOUTIN, P. (2003). « How to Hook Up, A step-by-step-guide to building your own network », *Wired*, mai [En ligne] www.wired.com/wired/archive/11.05/unwired/network.html (consulté le 9 janvier 2012).

BRADBURY, D. (2011). « Hacking wifi the easy way », *Network Security*, vol. 2011, nº 2, février, p. 9-12, ISSN 1353-4858, 10.1016/S1353-4858(11)70014-9.

CENTRE CANADIEN DE LA STATISTIQUE JURIDIQUE (2002). *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Ottawa, Centre canadien de la statistique juridique.

CTV.NEWS (2003). « Police warn of Wi-Fi theft by porn downloaders », *ctv.ca*, 23 novembre [En ligne] www.ctv.ca/servlet/ArticleNews/story/CTVNews/1069439746264_64848946/?hub=CTVNewsAt11 (consulté le 24 septembre 2007).

FARELL, N. (2007). « Teen wi-fi network thief get probation », *The Inquirer*, 17 janvier [En ligne] www.theinquirer.net/inquirer/news/1028456/teen-wi-network-thief-probation (consulté le 12 septembre 2007).

FLUHRER, S., et MANTIN, I. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4* [En ligne] aboba.drizzlehosting.com/IEEE/rc4_ksaproc.pdf (consulté le 4 février 2011).

GOLD, S. (2011). « Cracking wireless networks », *Network Security*, vol. 2011, nº 11, p. 14-18.

GUGLIELMINETTI, B. (2007). « Toronto, une ville sans fil », *Le carnet techno* [En ligne] www.radio-canada.ca/radio/techno/commentaires-86235.shtml (consulté le 25 avril 2007).

HILLS, A. (2005). « Smart Wi-Fi. Wireless access to the Internet via Wi-Fi is increasingly popular, so the technology is being upgraded to ensure that user get prompt, reliable service », *Scientificamerican* [En ligne] www.sciam.com/article.cfm?articleID=00036961-D024-1332-902483414B7F0000etsc=I100322 (consulté le 17 janvier 2012).

ÎLE SANS FIL (2011). Île Sans Fil [En ligne] www.ilesansfil.org/tiki-index.php (consulté le 22 mai 2007).

INTERPOL (2007). « IT Crime, Wireless technology », *Interpol* [En ligne] www.interpol.int/Public/TechnologyCrime/CrimePrev/WirelessTechnology.asp (consulté le 9 mai 2007). [La page n'est plus disponible.]

JIWIRE (2011). « WiFi HotStats », *JiWire* [En ligne] www.jiwire.com/search-hotspot-locations.htm (consulté le 17 novembre 2011). [La page n'est plus disponible.]

KEATS, J. (2011). « Jargon Watch : Pitstops, War-Texting, Data Furnace », *Wired*, 1er novembre [En ligne] www.wired.com/magazine/tag/li-fi/ (consulté le 4 décembre 2011).

LEDUC, C. (2007). « Le Wi-Fi en difficulté dans les villes américaines? », *Branchez-vous techno*, 20 septembre [En ligne] techno.branchez-vous.com/actualite/2007/09/eu_le_wifi_en_difficulte_dans.html (consulté le 24 septembre 2007).

LE NOUVELLISTE (2007). « Shawinigan WiFi », *Le Nouvelliste* [En ligne] technaute.lapresseaffaires.com/nouvelles/texte_complet.php?id=81,12399,0,052007,1354009.htmletref=rss_technaute (consulté le 22 mai 2007). [La page n'est plus disponible.]

NEGROPONTE, N. (2002). « Being Wireless », *Wired* [En ligne] www.wired.com/wired/archive/10.10/wireless.html (consulté le 10 décembre 2011).

PCMAG (2012). « Definition of : Wi-Fi », *PCMAG* [En ligne] www.pcmag.com/encyclopedia_term/0,2542,t=WiFieti=54444,00.asp (consulté le 17 janvier 2012).

POULSEN, K. (2006). « Crazy-Long Hacker Sentence Upheld », *Wired*, 11 juillet [En ligne] www.wired.com/science/discoveries/news/2006/07/71358 (consulté le 25 avril 2007).

PRESSE CANADIENNE (2007). « Montréal veut 400 points Wi-Fi », *Branchez-vous techno*, 22 novembre [En ligne] techno.branchez-vous.com/actualite/2007/11/montreal_veut_400_nouveaux_poi.html (consulté le 26 novembre 2007).

RITOUX, N. (2007). « Les meilleurs cafés "Wi-Fi" de Montréal », *La Presse*, 25 mai [En ligne] technaute.cyberpresse.ca/nouvelles/texte_complet.php?id=81,12399,0,052007,1355861.htmletref=rss_technaute (consulté le 5 septembre 2007).

SHIM, R. (2003). « Wi-Fi arrest highlights security dangers », *CNET*, 28 novembre [En ligne] www.cnetnews.com/2100-1039_5112000.html (consulté le 12 septembre 2007).

SHORE, R. (2007). « WiFi could pose threat during Vancouver Olympics : police expert », *Vancouver Sun* [En ligne] www.canada.com/topics/news/national/story.html?id=207f6d54-68fc-40da-8ae3-dc9f057c-2f54etk=25065 (consulté le 25 avril 2007).

SMITH, B. (2007). « Saskatchewan plans wireless network for four cities », *Itbussiness.ca*, 11 mai [En ligne] www.itbusiness.ca/it/client/en/Home/News.asp?id=43274 (consulté le 14 mai 2007).

VILLE DE QUÉBEC (2011). *Québec, ville branchée* [En ligne] ville.quebec.qc.ca/actualites/zapquebec.aspx (consulté le 20 novembre 2011). [La page n'est plus disponible.]

WIRELESS BROADBAND ALLIANCE (2011). « Global Developments in Public Wi-Fi WBA Industry Report, 2011 », *Wireless Broadband Alliance* [En ligne] www.wballiance.com/resource-centre/global-developments-wifi-report.html (consulté le 30 novembre 2011).