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

17

Tendances de la cybercriminalité

Francis Fortin[1]
Benoit Gagnon[2]

Il est toujours risqué de parler de « tendances » quand vient le temps d'aborder la question de la cybercriminalité. En effet, jouer au jeu de la prédiction s'avère un exercice de haute voltige intellectuelle qui, la plupart du temps, se base sur une connaissance inconstante de la réalité. Dans le cas qui nous préoccupe, le jeu de la prédiction est d'autant plus risqué qu'il cible le croisement de deux phénomènes sociaux où l'innovation semble être la norme : l'informatique et la criminalité.

Tout d'abord, la vitesse à laquelle les nouvelles technologies de l'information et des communications se développent a pour conséquence qu'il devient très difficile de discerner les directions qu'elles emprunteront dans les années, voire les mois à venir. Par conséquent, il n'est pas facile de concevoir ce qui préoccupera les autorités de sécurité dans un avenir proche. Ensuite, le changement technologique est si imprévisible et sa diffusion si rapide qu'il engendre des transformations sociales tout à fait inattendues. Personne n'avait pu prédire le succès retentissant de Facebook. À cet égard, alors que Twitter demandait déjà aux internautes de mettre à jour leur statut quelques années auparavant, le réseau social

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

Facebook a réussi à obtenir la confiance des utilisateurs pour qu'ils partagent beaucoup plus que leur statut. Le géant des réseaux sociaux est parvenu à obtenir des niveaux encore inégalés d'informations personnelles pour un service sur le Web. Ce tour de force est d'autant plus remarquable que tous les services de Facebook existaient dans une forme non intégrée, et surtout avec des taux de pénétration beaucoup plus faibles. L'ironie du sort veut que le succès de Facebook ait donné, par synergie, un second souffle à Twitter. Or, bien que les réseaux sociaux soient l'exemple ultime de surprise technologique, l'exemple démontre qu'il est très complexe de connaître les innovations qui prendront le dessus, de distinguer la façon dont les criminels exploiteront les failles technologiques et, surtout, comment ils adopteront ces technologies et s'y adapteront.

Dans cette perspective, nous ne cherchons pas dans ce chapitre à effectuer une revue exhaustive des tendances pouvant être anticipées, mais plutôt à survoler les tendances lourdes que nous percevons dans le domaine de la cybercriminalité. D'abord, nous aborderons les nouveaux vecteurs de cybercriminalité. Nous traiterons ensuite de l'Internet des objets pour conclure avec la question des informations infonuagiques et de leur impact sur le crime.

17.1 Nouveaux vecteurs de cybercriminalité

Le développement des technologies associées à l'informatique et à Internet a amené des changements importants dans la façon de commettre certains crimes. Plusieurs exemples ont été cités dans le présent ouvrage. Dans cette partie, nous nous concentrerons sur les changements actuels et à venir qui constituent des vecteurs de cybercriminalité. Nous verrons les nouvelles façons de se brancher, les nouveaux lieux virtuels pour joindre des victimes, le développement de nouveaux univers virtuels et, finalement, les nouveaux modes de paiement.

17.1.1 Nouvelles façons de se brancher

Une des tendances que nous pouvons signaler est l'augmentation du temps passé en ligne. Sans représenter une action criminelle directe sur le réseau, de plus en plus d'appareils sont branchés presque en permanence

sur Internet. En effet, plusieurs innovations des dernières années ont fait augmenter radicalement le temps de connexion à Internet.

On peut distinguer deux types de transformations relatives à l'accès à Internet : la quantité des accès disponibles et la qualité des connexions et des fonctionnalités. En ce moment, on peut compter environ un milliard d'ordinateurs personnels dans le monde (Chapman, 2007). Il faut ajouter à ce bassin de dispositifs branchés à Internet les téléphones cellulaires, les baladeurs et tous les autres dispositifs encore à venir. On sait qu'il existe plus de quatre milliards d'utilisateurs de téléphonie cellulaire dans le monde (UNESCO, 2008).

Les progrès des réseaux cellulaires, avec la venue des réseaux de quatrième génération (4G) et les réseaux LTE, par exemple, augmentent sensiblement la capacité de transfert de données pour les utilisateurs à travers leurs téléphones cellulaires. Ces cellulaires, qui peuvent être bimodes et incorporer une connectivité sans fil réseau classique, représentent des plateformes d'échange idéales pour bon nombre d'utilisateurs qui sont en mouvement. Ainsi, cette augmentation de la capacité de transfert se conjugue à une augmentation de l'utilisation simple des réseaux 3G. Entre 2007 et 2008, l'utilisation du 3G a augmenté de 59 % aux États-Unis (RF Design, 2008). En somme, non seulement les réseaux cellulaires sont-ils plus puissants, mais ils sont aussi de plus en plus empruntés.

Le réseau cellulaire n'est pas le seul réseau sans fil permettant d'accéder à Internet qui est soumis à de fortes augmentations de puissance. Les réseaux sans fil classiques – réseaux Wi-Fi – s'améliorent et gagnent en popularité eux aussi. Entre 2007 et 2008, on estime à environ 46 % l'augmentation du nombre de réseaux sans fil (RF Design, 2008). Or, l'introduction récente des protocoles de connexion sans fil 802.11n dans les réseaux sans fil a eu pour effet d'augmenter la portée, la puissance et la rapidité des réseaux sans fil. Cela se poursuivra sous peu avec l'introduction du protocole 802.11ac. Toutefois, si on assiste à une augmentation inexorable de l'utilisation des réseaux sans fil et de la quête de vitesse, cela ne veut pas dire que la sécurité des nouveaux protocoles augmente au même rythme[3]. En outre, l'utilisation de plus en plus marquée d'Internet haute vitesse a eu pour conséquence que bon nombre

3. Ce thème est abordé dans le chapitre 2, « Réseaux sans fil et éléments criminogènes ».

d'utilisateurs laissent leur ordinateur allumé 24 heures par jour, sans être conscients des risques encourus (Lack, 2009).

À ces données quantitatives s'ajoute une donnée qualitative indéniable : la popularité grandissante des téléphones et des appareils dits « intelligents ». Par exemple, les téléphones offrent à leurs utilisateurs des interfaces de plus en plus riches, capables d'effectuer des tâches de plus en plus complexes. En somme, les téléphones portables se transforment en mini-ordinateurs, comprenant caméra et dispositif de géolocalisation, et sur lesquels on exploite, traite et stocke de plus en plus de données, notamment des données personnelles.

Mentionnons également le marché de la tablette, qui a littéralement explosé au cours des dernières années, l'iPad étant une des innovations les plus percutantes à ce chapitre. Bien qu'elles constituent un nouveau type de dispositif, les tablettes sont en quelque sorte des hybrides, se situant entre les ordinateurs portables et les téléphones intelligents, supportent une somme non négligeable de données personnelles et utilisent bon nombre de logiciels. Compte tenu du fait que plusieurs modèles de tablettes utilisent des systèmes d'exploitation à la sécurité douteuse, cela risque d'engendrer des opportunités criminelles supplémentaires.

À la lumière de ces changements, comment envisager les transformations du crime? D'abord, il y aura fort probablement une augmentation des victimes potentielles. En effet, des dispositifs possédant de plus en plus de fonctionnalités risquent de faire croître les opportunités criminelles pour plusieurs types de crimes. La multiplicité des sources de branchement de même que le temps passé en ligne en mode actif ou passif (en étant, par exemple, simplement branché par l'intermédiaire de sa messagerie instantanée grâce à son cellulaire) contribuent à cet état de fait. De plus, il ne faut pas sous-estimer l'importance des nouvelles façons d'obtenir des données personnelles (vol de cellulaire, interception de données par réseau sans fil, protocole Bluetooth, etc.).

Ensuite, certains types de cybercrimes rapportent davantage à leurs auteurs en fonction du volume de victimes potentielles ou d'appareils potentiellement compromis. On peut aisément en déduire que les téléphones intelligents risquent fortement d'intéresser les fraudeurs et autres cybercriminels; un nombre aussi important d'appareils pouvant être exploités offre une opportunité à ces individus toujours à la recherche de « nouveaux marchés ». Cela veut donc dire que ces ordinateurs sont

des cibles offertes en permanence. Dans cette perspective, ces téléphones sont des cibles de choix pour les cybercriminels qui peuvent y voir un réservoir intéressant de données autant que des cibles potentielles de vol d'identité, par exemple. À ce chapitre, puisque les cibles potentielles augmentent, nul n'est besoin de spécifier que les experts prévoient déjà un maliciel aux impacts à grande échelle au cours des prochaines années (Gostev, 2012).

Ces transformations auront aussi un impact sur les méthodes d'enquête. L'utilisation de plus en plus mobile des connexions Internet, conjuguée au fait que cet accès est ouvert et permet de ne pas le lier à une adresse fixe, occasionnera des problèmes supplémentaires pour les enquêteurs. S'ils remontent grâce à des traces d'actes cybercriminels jusqu'à des ordinateurs se trouvant dans des cafés Internet ou à un téléphone mobile à la carte, il devient difficile de retrouver le malfaiteur. Pas étonnant d'ailleurs que les terroristes semblent particulièrement apprécier, depuis des lustres, les cafés Internet (Ribeiro, 2007), qui sont de plus en plus disponibles gratuitement, pour communiquer entre eux.

17.1.2 Nouvelles façons de joindre des victimes

Une autre évolution qu'on peut voir émerger est la diversification des supports utilisés pour fomenter des actes de cybercriminalité, comme la dissémination de maliciels, les fraudes nigérianes ou l'hameçonnage, par exemple. Auparavant, c'était surtout à travers les courriels que ces actes de cybercriminalité étaient perpétrés. Les tentatives étaient relativement simples, voire simplistes. Il s'agissait d'envoyer aux internautes des maliciels camouflés soit en pièce jointe légitime, soit en hyperlien. Les tentatives de fraude par ingénierie sociale étaient également courantes. Ensuite, le cybercriminel espérait que l'utilisateur ouvre le courriel, télécharge la pièce jointe, clique sur le lien proposé ou encore réponde positivement à la tentative de fraude. On affirme que les attaques ne se caractérisent plus par l'utilisation du courriel puisque son efficacité a diminué au cours des dernières années; c'est plutôt le navigateur qui est le nouveau vecteur d'attaque (Gostev, 2012).

Le domaine de l'hameçonnage est un bon exemple de cette tendance. Ce qu'on risque de voir dans un avenir rapproché, c'est un changement dans l'approche actuelle, qui est essentiellement une approche par le bas (*bottom up*), pour l'utilisation plus systématique de l'approche par

le haut (*top down*). Si la majorité des attaques classiques d'hameçonnage visaient de simples individus ou des employés d'organisations diverses (entreprises, gouvernements, etc.), les attaques d'hameçonnage à venir vont s'en prendre directement aux hauts gestionnaires et aux preneurs de décisions se trouvant dans différentes organisations (Martin, 2008).

Pour arriver à mener ce genre d'attaques plus sophistiquées – le terme *spear phishing* (harponnage) est souvent utilisé en anglais –, les cybercriminels raffinent présentement leurs méthodes en rendant leurs scénarios de plus en plus crédibles et de mieux en mieux construits. Une des méthodes utilisées pour arriver à un tel degré de crédibilité est l'utilisation des sources d'informations disponibles sur Internet, notamment les diverses informations laissées par les preneurs de décisions dans les réseaux sociaux, par exemple (McAfee, 2009).

Avec ces nouvelles techniques d'hameçonnage, on risque probablement de voir émerger de nouvelles techniques d'ingénierie sociale. Encore une fois tributaires du fait qu'il est désormais plus facile d'obtenir des informations sur les individus et des données personnelles, les ingénieurs sociaux seront désormais capables de mener des actions de piratage psychologique beaucoup plus efficaces et plus personnalisées.

Une technique de plus en plus exploitée porte le nom de « téléchargement furtif » (*drive-by-download*). Cette technique cherche à retirer l'utilisateur, et son assentiment, de la boucle permettant l'attaque informatique. Simplement en visitant une page Web utilisée par un cybercriminel, l'utilisateur peut être attaqué par un maliciel visant les failles de son ordinateur. Si la faille est présente, on infecte l'ordinateur en y implantant un « téléchargeur de cheval de Troie », c'est-à-dire un maliciel chargé d'aller chercher différents logiciels sur Internet et de les installer à l'insu de l'utilisateur. Cela permet ensuite de réutiliser la machine infectée à son propre usage.

On observe une autre technique particulièrement pernicieuse : le détournement d'onglets de navigation. En exploitant les failles issues du téléchargement furtif, le pirate change subtilement le site se trouvant dans un onglet non utilisé par un internaute. Ce nouveau site est, dans les faits, un site d'hameçonnage ressemblant à un site hautement fréquenté (Gmail, site bancaire, site de réseau social, etc.). L'utilisateur qui retourne à ses onglets cachés, n'ayant pas vu le changement s'opérer en arrière-plan, pourrait facilement être tenté de se connecter à ce site et d'y

entrer des informations confidentielles. Bref, cette méthode s'ajoute au lot grandissant de méthodes permettant de subtiliser des informations personnelles aux internautes.

Or, la problématique à laquelle les autorités de sécurité sont présentement confrontées est la multiplication des plateformes où peuvent se dérouler des tentatives de ce genre. Comme nous l'avons mentionné précédemment, les comptes de jeux en ligne deviennent des cibles intéressantes, ainsi que la panoplie de plateformes Web ou de nouvelles méthodes de communication. Pensons entre autres à Facebook, MySpace, YouTube, LinkedIn et à d'autres sites de réseautage social. Notons également l'éventail de sites de téléchargement poste-à-poste (P2P), incluant les sites de torrents qui peuvent facilement être des vecteurs de maliciels. Les sites de petites annonces ou d'encans virtuels sont aussi pris d'assaut par les fraudeurs.

Bref, ce que nous pouvons tirer comme conclusion par rapport à ces tendances, c'est que du moment que certaines applications attireront des individus, elles finiront tôt ou tard par attirer les cybercriminels qui y verront nécessairement un « marché » croissant de victimes. Pour l'heure, ce sont les entreprises qui font les règles du jeu. Elles développent de nouveaux outils qui permettent à des individus de manipuler Internet de manière créative, mais, d'un autre côté, ces outils permettent aussi d'innover en matière d'activités criminelles.

17.1.3 Nouveaux univers : les jeux en ligne et les univers virtuels

Parallèlement au développement des plateformes d'échange, des écosystèmes ayant leurs propres règles ont aussi vu le jour au cours des dernières années. Les jeux vidéo en ligne et les univers sociaux virtuels ont ouvert la porte à de nouvelles formes d'abus puisqu'ils constituent des lieux de rencontre et de criminalité financière impliquant les investissements des joueurs. On distingue deux grandes familles d'univers : les jeux vidéo se déroulant en partie en ligne et les jeux en ligne massivement multijoueurs (JELMM). Dans la première catégorie, les joueurs se réunissent dans un espace virtuel essentiellement pour jouer et échanger de manière plutôt succincte. Il s'agit de communautés tissées de manière plus ou moins serrée qui occupent cet espace le temps de jouer quelques parties.

Même s'il s'agit d'un espace relativement restreint sur le plan de la socialisation, certains criminels tentent de l'utiliser pour commettre des crimes; on pense entre autres à des tentatives de leurre d'enfant. D'ailleurs, on connaît déjà des cas de pédophiles exploitant les jeux en ligne pour tenter d'avoir des relations sexuelles avec des mineurs (Ellis, 2009; Salemi, 2009).

Les JELMM, pour leur part, sont des jeux vidéo se déroulant exclusivement en ligne. Pour y jouer, l'internaute doit se procurer un logiciel et payer un montant mensuel lui permettant d'accéder à ce monde en ligne. Ce genre de jeu est construit afin de faire vivre une expérience complète au joueur. Ainsi, non seulement le côté ludique est-il très important, mais il existe également une économie interne basée sur la rareté de certains éléments, sur la participation des joueurs dans la fabrication d'objets virtuels pouvant être revendus et sur le fait que la socialisation est un instrument efficace pour réaliser bon nombre des activités qu'offrent ces univers (Felder, 2012).

Les JELMM sont particulièrement propices à la cybercriminalité, et ce, pour deux raisons principales. La première vaut également pour les jeux vidéo standard dont une partie se déroule en ligne : ils offrent un espace de socialisation. Or, dans les JELMM, ces espaces sont beaucoup plus vastes, ce qui représente des occasions plus importantes pour d'éventuels cybercriminels. Encore ici, le leurre de mineur ira probablement en grandissant dans les années à venir. Les cas répertoriés s'accumulent déjà (Australian Associated Press, 2008).

La seconde raison pour laquelle les JELMM sont un vecteur criminel est qu'ils exploitent directement les données financières des joueurs. Étant donné que les joueurs doivent payer pour accéder au JELMM, ils fournissent bien souvent un numéro de carte de crédit. D'autres modes de paiement sont offerts, mais ils demeurent peu utilisés. Lier des données financières à des joueurs devient donc intéressant pour des cybercriminels. Ces derniers n'hésitent d'ailleurs pas à écrire des scripts malicieux s'attaquant aux JELMM populaires dans l'objectif de voler ces données; l'affaire du maliciel Mocmex est probablement un des cas les mieux connus de ce genre d'attaque (Nino, 2008).

Sans être considéré *stricto sensu* comme étant de la criminalité, ce que les JELMM suscitent de plus en plus est l'échange de biens virtuels contre

de l'argent sonnant. Par exemple, on voit un nombre croissant d'entreprises chinoises qui « vendent » de la monnaie virtuelle dans différents JELMM, un des plus populaires étant World of Warcraft. Le système est relativement simple : la compagnie engage un groupe d'individus qui jouent pendant de longues heures. Ils amassent des richesses virtuelles et les revendent au plus offrant. Or, en ce moment, on assiste au développement d'un marché pour les objets virtuels (Dibbell, 2003). Dès 2003, Dibbell soulignait d'ailleurs l'importance du phénomène en parlant d'un *unreal estate boom*, jeu de mots signifiant « boom de l'immobilier virtuel ». Ce genre de marché parallèle a de quoi faire sourciller, d'autant plus qu'il soulève des interrogations on ne peut plus légitimes sur la gestion des éventuels cas de fraudes. Comment gérer ceux qui ont non seulement une portée internationale, mais qui concernent également des objets virtuels dont l'échange n'est pas reconnu par la compagnie éditrice du JELMM?

À cela il faut aussi ajouter la montée en popularité des jeux sociaux. Ces jeux, fortement présents sur les réseaux sociaux, comme Facebook ou Google+, ont pour objectif de rendre les réseaux sociaux encore plus ludiques. De véritables empires naissent maintenant grâce aux jeux sociaux; mentionnons entre autres Zynga (company.zynga.com), qui a publié toute une série de jeux sociaux hautement populaires, comme Mafia Wars et Farmville.

Le fonctionnement de ces jeux est relativement simple : le joueur s'adonne à des activités au sein d'un univers ludique qui tend à croître et à se transformer – la ferme se développe, le réseau criminel grandit, la ville croît, etc. Or, le joueur peut accomplir un certain nombre d'actions dans un temps donné et il a le loisir de demander l'aide de personnes appartenant à son réseau.

À la base, ces jeux sont souvent gratuits, mais ils peuvent devenir payants selon ce que le joueur veut faire. En effet, les modèles les plus fréquents offrent aux joueurs d'augmenter le nombre d'actions auquel ils ont droit moyennant un montant d'argent. C'est à ce moment que les questions importantes se posent. En effet, les modes de financement de ces jeux sont pour la plupart légitimes. Néanmoins, certaines compagnies à l'éthique élastique pourraient être tentées d'exploiter les données recueillies par les réseaux sociaux pour les revendre à des entreprises plus ou moins légitimes. De même, le potentiel de fraude augmente

considérablement si la personne est invitée à insérer des données bancaires au sein d'un jeu exploitant les réseaux sociaux. Il ne faut pas être un génie du crime pour comprendre tout le potentiel que recèle ce modèle d'affaires, le tout allant de l'hameçonnage aux techniques plus évoluées.

Ce genre de situation sous-tend en fait une tendance lourde à laquelle devront faire face les corps policiers et le système de justice dans les prochaines années. En effet, la popularité croissante de ces espaces aura pour effet de multiplier les situations dans lesquelles la virtualité sera au cœur de l'acte criminel. Les biens virtuels auront de plus en plus de valeur aux yeux des individus qui les utilisent. Dans cette perspective, il faudra irrémédiablement se demander comment gérer les questions du « non-physique », des questions qui, pour l'instant, occupent quelques théoriciens universitaires, mais qui finiront tôt ou tard par glisser dans le monde de la pratique.

17.1.4 Nouveaux modes de paiement

Si on observe un croisement entre le virtuel et le réel pour les individus qui œuvrent dans ces nouveaux univers, il est aussi possible de constater qu'il y a de plus en plus de flou entre le milieu bancaire traditionnel et le milieu des nouvelles entreprises de paiement. En fait, il est possible de voir deux grandes transformations s'effectuer.

Tout d'abord, on observe une volonté de l'industrie de faire mousser l'utilisation des téléphones cellulaires comme portefeuilles, ce qu'il est convenu d'appeler les « portefeuilles mobiles ». Le projet sous-tendant cette vision est relativement simple : remplacer le portefeuille traditionnel, contenant de l'argent liquide et des cartes de paiement diverses, par le téléphone cellulaire. Il s'agit d'exploiter la technologie de communication en champ proche (*near field communication* ou NFC) pour effectuer une transaction entre le cellulaire et le point de vente. Le tout transforme donc littéralement le téléphone en plateforme complète de paiement et fait de lui un relais entre le consommateur et les institutions bancaires.

Actuellement, les grands constructeurs de systèmes d'exploitation pour cellulaires se penchent attentivement sur ces nouvelles technologies. Google y est d'ailleurs fortement impliquée avec son système

Android[4] puisqu'elle déploie bon nombre de ressources dans la mise en place de son système. Malgré cela, les avancées du portefeuille mobile sont encore timides. Toutefois, on peut penser que le mouvement ira en s'accélérant, d'autant plus que des géants du commerce de détail, comme Wal-Mart, 7-Eleven ou Sunoco, s'intéressent de plus en plus à ces technologies (Sidel, 2012).

Ensuite, il faut mentionner la tendance à la décentralisation des modes de paiement. Les banques et les services de surveillance de transactions financières doivent de plus en plus faire face à des moyens permettant à des individus de devenir de véritables points de vente. Ainsi, les individus deviennent des acteurs supplémentaires à prendre en considération dans le spectre des acteurs financiers. Certes, ils étaient déjà impliqués dans une grande quantité de microtransactions au travers de services comme PayPal, mais cela s'est accéléré dans les derniers mois, notamment par le truchement de services exploitant les forces des téléphones intelligents. L'exemple de Square est probablement le plus éloquent de ce genre de système[5]. Il s'agit d'un module qui s'ajoute à un téléphone intelligent (Android ou iPhone) et qui permet d'effectuer une transaction par carte de paiement, et ce, moyennant un pourcentage sur chaque transaction. Cela remet donc entre les mains des individus la possibilité de devenir de véritables terminaux de points de vente et d'accepter les mêmes paiements que les commerçants traditionnels.

S'il y a décentralisation des modes de paiement, cela ne veut toutefois pas dire que le système bancaire en est mis en marge – l'argent finit généralement tôt ou tard par retourner dans un compte bancaire –; cela signifie plutôt qu'il y a un contrôle de moins en moins grand des moyens permettant d'effectuer les paiements. Or, c'est justement la diminution de ce contrôle qui soulève des questions.

En effet, la venue rapide et massive de ces technologies dans le spectre des transactions financières pose d'épineuses questions sur l'avenir de la protection contre la fraude bancaire. En effet, sachant qu'il y aura à peu près autant de formes de portefeuilles mobiles qu'il y aura de téléphones intelligents, on fera face à un énorme défi de sécurité. D'autant plus que des plateformes, la plateforme Android par exemple, sont ouvertes et

4. www.google.com/wallet
5. squareup.com

ne sont pas mises à jour de manière systématique (Newman, 2012); cela signifie donc que les failles potentielles seront nombreuses et qu'il sera difficile de les colmater par une approche par le haut. Ce seront donc les individus qui devront porter le fardeau de la sécurité de leurs transactions financières, ce qui impliquera de faire des choix difficiles pour les néophytes des technologies.

17.2 Tout connecter ensemble

Autre tendance importante à souligner : le fait que plusieurs objets du quotidien n'exploitant actuellement pas Internet deviennent tôt ou tard connectés à la Toile. Cette tendance s'est matérialisée autour du concept de l'Internet des objets.

Le concept n'est à vrai dire pas nouveau. Il est possible d'en déceler des traces depuis la fin des années 1990. La définition originale de l'Internet des objets voit les possibilités offertes par les technologies de radiofréquence et leur intégration dans des objets (Kranenburg, 2008). Par exemple, on peut mentionner toutes les technologies de traçabilité des aliments qui permettent de savoir où se trouve un aliment et d'où il vient.

La définition actuelle de l'Internet des objets tient essentiellement à deux aspects. Tout d'abord, il s'agit d'une série d'idées qui voient les technologies de l'information comme une série de couches pouvant être connectées à des infrastructures et des objets. Ensuite, il s'agit d'une série de concepts qui seront déstabilisateurs pour le paradigme de pensée actuel en ce qui concerne les outils contemporains (The Internet of Things Council, 2012).

De manière plus contemporaine, on constate qu'Internet s'est détaché des simples technologies de radiofréquence et s'est élargi. Dorénavant, il s'agit de pousser sur les fonctionnalités d'infrastructures ou d'objets par l'inclusion de nouvelles possibilités en exploitant les activités et les possibilités offertes par Internet; on inclut ainsi un bassin plus grand de technologies.

Un exemple actuellement très populaire permettant d'illustrer adéquatement les capacités de l'Internet des objets est le thermostat Nest (www.nest.com). Il s'agit d'un thermostat dit « intelligent » au sens où il est non seulement capable d'analyser et de comprendre son environnement,

puis de modifier la température en fonction de ce dernier, mais où il est aussi branché sur Internet. Ainsi, le propriétaire du thermostat peut le contrôler à distance en passant par des applications riches en fonctionnalités et en options.

Évidemment, à l'heure actuelle, les fonctionnalités offertes par l'Internet des objets demeurent relativement simples, voire quelque peu limitées. Néanmoins, l'avenir semble très prometteur à ce chapitre et bon nombre de géants des technologies de l'information se lancent dans des secteurs comme la domotique – l'exploitation d'outils électroniques et liés à la mécanique du bâtiment qui permet d'obtenir un contrôle poussé des activités se déroulant dans le bâtiment (chauffage, climatisation, détecteurs divers, etc.). Notons, entre autres, qu'Apple y voit un marché de plus en plus intéressant (Evans, 2011).

Il faut aussi mentionner que l'industrie automobile s'y intéresse de plus en plus avec des plateformes comme celles développées par Ford et Microsoft avec Ford Sync, par exemple[6]. Ford Sync permet pratiquement de transformer la voiture en une plateforme exploitant des outils technologiques existants, comme les téléphones intelligents. Ainsi, les voitures se voient connectées de manière indirecte à Internet. Toutefois, sachant que des véhicules prototypes complètement branchés au 4G commencent à émerger (Cheong, 2012), et que même des fournisseurs de réseaux cellulaires veulent faire payer pour des forfaits dans les voitures (Berman, 2012), cela ne prend pas beaucoup d'imagination pour voir poindre la production de masse de véhicules exploitant ce genre de technologie.

En ce qui concerne la criminalité, il faut bien se rendre à l'évidence que la situation sera particulièrement délicate dans les années à venir. En effet, au fur et à mesure que les infrastructures et les objets seront connectés à Internet, ils deviendront des cibles potentielles et supplémentaires pour des criminels. Or, cela posera des questions importantes en matière de sécurité : jusqu'où les criminels pourront-ils aller en matière d'actes criminels? Seront-ils capables de contrôler des éléments présents dans nos maisons? Auront-ils la possibilité de modifier les options des véhicules automobiles sans que le propriétaire donne sa permission? Ces questions demeurent à ce jour sans réponses.

6. www.ford.com/technology/sync

17.3 Passages nuageux à prévoir

Comme nous l'avons évoqué dans le chapitre 3, « Crimes sur le Web 2.0 », l'évolution du Web l'a rendu plus social et plus ouvert. À la suite de ce changement de paradigme, il semble que les utilisateurs acceptent de plus en plus l'idée de déposer leurs données personnelles chez une tierce partie. Autrement stockées sur leur ordinateur personnel, les données des utilisateurs d'Internet se retrouvent plus fréquemment dans le nuage. Ainsi, on peut définir en termes simples que les services infonuagiques (*cloud services*) ont pour objectif d'offrir une interface en apparence unique pour que l'usager accède à ses informations. L'exemple le plus probant est sans doute iCloud, le service d'Apple, qui offre notamment aux utilisateurs de stocker les images sur leurs serveurs et de les redistribuer automatiquement vers les autres dispositifs branchés. En d'autres termes, l'utilisateur prend une photo avec son téléphone, puis l'image se rend sur le nuage (les serveurs d'Apple) et est ensuite redistribuée sur les autres dispositifs de l'utilisateur (ordinateur portable, ordinateur, etc.). Il s'agit aussi pour l'utilisateur d'avoir un lieu de stockage (généralement de grande capacité) lui permettant d'accéder à ses données, peu importe l'appareil utilisé.

Or, la centralisation des informations des utilisateurs dans le nuage a amené des considérations relatives au crime lui-même ainsi que des effets sur le déroulement des enquêtes. Dans la présente section, nous aborderons la question épineuse du stockage des informations dans le nuage et les considérations y étant associées. Nous examinerons ensuite la question de l'impact de son utilisation accrue sur les enquêtes et, finalement, nous verrons l'utilisation innovatrice des services infonuagiques à des fins de piratage.

L'idée de centraliser les données à un seul endroit pour les utilisateurs est loin d'être nouvelle. Aux balbutiements de l'ère informatique, le système UNIX offrait une architecture hautement centralisée. Des terminaux avec peu de puissance de calcul se connectaient à l'ordinateur central (*main frame*) qui, lui, possédait la puissance pour effectuer les opérations. Au besoin, l'utilisateur pouvait démarrer une tâche et revenir quelques minutes, voire quelques heures plus tard et obtenir le résultat. C'est d'ailleurs ce qui se passait lors d'une recherche sur Internet : les résultats étaient envoyés par courriel à l'utilisateur ayant préalablement fait la requête (Sohier, 1998). Or, l'idée de centraliser l'information

avait grandement perdu en popularité lors de l'apparition de l'ordinateur personnel (PC) dans les années 1980 et 1990. Cette période était caractérisée par le désir de l'utilisateur de conserver ses données sur son ordinateur personnel.

En 2004, l'idée du nuage allait commencer à germer avec, entre autres, des initiatives comme celle de Google et son service de courriel Gmail, qui se caractérisait par une capacité de stockage outrepassant largement celle de son plus proche concurrent, Hotmail. Les concepteurs de Gmail avaient même omis volontairement le bouton « Effacer » en alléguant que la gestion de l'espace disque n'était pas un problème et qu'il n'y avait donc nul besoin de faire de la gestion de l'espace. En contrepartie, Gmail se permettait d'analyser le contenu des courriels afin d'insérer des publicités pertinentes. Cette mesure a soulevé une controverse lors de son annonce (Battelle, 2006).

En dépit d'événements semblables qui auraient pu freiner la tendance à partager des informations sur le réseau, on a plutôt assisté au contraire. Les dernières années ont été marquées par la montée en popularité de Facebook, qui est devenu le plus grand observatoire social nouveau genre, alors que Gmail et les autres services de courriel semblent avoir gagné leur pari : les courriels ne sont plus transférés sur un ordinateur personnel, mais résident plutôt dans les nuages.

Comme mentionné précédemment, le nuage offre un moyen de se brancher qui permet d'offrir une expérience comparable selon tous les dispositifs utilisés. L'utilisateur se branche à une seule entité pour avoir accès à ses informations personnelles, ses photos, ses vidéos, etc. Cette nouvelle architecture nous amène à percevoir une nouvelle tendance dans la sphère criminelle. Quelle serait la valeur pour un individu malicieux d'avoir accès à des informations aussi abondantes qu'intéressantes? L'idée de l'importance des données personnelles a déjà été évoquée dans le chapitre 11, « Vol et usurpation d'identité : les contours imprécis d'un crime fourre-tout ». Or, quelques éléments nous poussent à croire que les données ont bel et bien une valeur marchande ou stratégique aux yeux de certains criminels. L'importance de cette tendance ne s'apprécie toutefois pas en termes de quantité d'événements, mais fort probablement en termes d'impact pour chaque événement recensé.

D'abord, le gouvernement chinois aurait lancé une attaque massive et sans précédent sur Google, Yahoo et des dizaines d'autres entreprises

de la Silicon Valley. Les pirates chinois auraient réussi, entre autres, à accéder au réseau interne de Google grâce à une douzaine de maliciels ainsi qu'à plusieurs niveaux de cryptage pour cacher leurs activités (Zetter, 2010). On a mentionné que l'objectif était de recueillir des informations sur des militants chinois pour les droits de l'homme, mais il semble que des éléments de propriété intellectuelle aient aussi été volés. Ces actions ont eu un impact important, au point de pousser Google à demander aux autorités politiques américaines d'intervenir (Zetter, 2010). Puis, des pirates se sont attaqués au réseau PlayStation, volant des quantités astronomiques de données personnelles. Bien que les motivations des auteurs de ces deux attaques soient différentes, le problème demeure de savoir comment les informations seront utilisées. Une chose est certaine : obtenir des quantités astronomiques d'informations en s'attaquant parfois aux centres de données constitue une tendance à prévoir au cours des prochaines années.

Or, si les données sont centralisées dans les nuages et que les dispositifs permettent l'accès sans nécessairement procéder au stockage des informations, le milieu des enquêtes doit forcément adapter ses méthodes. À quoi bon procéder à une perquisition sur l'ordinateur ou le téléphone cellulaire d'un suspect si aucune des informations ne se trouve sur ces derniers? Auparavant, les fournisseurs de services de courriel agissaient comme une boîte postale disponible pour les résidents d'une région, ils hébergeaient les courriels le temps que l'utilisateur se branche, les télécharge et les enlève du serveur de courriel. Il ne restait donc qu'une seule copie du courriel, soit celle sur l'ordinateur personnel du client. Maintenant, avec les services de courriel comme Gmail, Yahoo et Hotmail, pour ne nommer que ceux-là, beaucoup d'utilisateurs ont choisi d'accéder à leurs courriels directement au « bureau de poste » et d'y faire toutes les opérations. En d'autres termes, ce sont les fournisseurs de services Internet qui sont les hébergeurs principaux de ces données et ce sont eux qui gardent la seule copie des courriels des utilisateurs[7]. C'est donc avec ces fournisseurs que les organisations

7. Il est certainement possible que des traces restent sur l'ordinateur ou le dispositif s'étant branché au serveur, mais le succès de l'opération dépend d'une série de facteurs qui vont au-delà des objectifs du présent chapitre. Retenons que cette technique est certainement moins sûre que de consulter le contenu de la boîte de courriels.

d'application de la loi devront faire affaire afin d'obtenir des informations sur des utilisateurs Internet. Il y aura alors une adaptation du milieu des enquêtes, mais aussi des détenteurs de ces banques de données, d'une part, pour changer les pratiques légales et, d'autre part, pour agir comme gardiens de ces informations personnelles.

Finalement, les pirates peuvent aussi être clients des services infonuagiques disponibles sur Internet. Ainsi, plusieurs services de virtualisation sont apparus au cours des dernières années. Par exemple, la compagnie Amazon offre une multitude de services destinés aux entreprises afin d'héberger les applications, mais aussi pour offrir des capacités de calcul ultra-performantes. Le tout afin de simplifier la gestion d'application et des ressources pour les entreprises. Or, il semble que ces capacités puissent aussi être utilisées par des personnes ayant de mauvaises intentions. Selon certains analystes, des pirates ont recours à des ressources dans le nuage afin d'analyser des données, pour la découverte de mots de passe, par exemple. Cela constituerait une solution de rechange à l'utilisation des ordinateurs sous leur contrôle pour faire des opérations très exigeantes en capacité de calcul. Il sera intéressant de voir si ces observations deviendront une tendance. Il y aura minimalement un questionnement à faire quant aux crimes infonuagiques.

Bibliographie

AUSTRALIAN ASSOCIATED PRESS (2008). « World of Warcraft pedophile stole teen girl », *News.com.au* [En ligne] www.news.com.au/story/0,23599,23944622-421,00.html (consulté le 10 février 2009). [La page n'est plus disponible.]

BATTELLE, J. (2006). *The Search : How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*, New York, Portfolio Trade.

BERMAN, B. (2012). « Verizon Wants Your Car on a Data Plan », *ReadWriteWeb* [En ligne] www.readwriteweb.com/archives/verizon-wants-your-car-on-a-data-plan.php (consulté le 13 novembre 2012).

CHAPMAN, S. (2007). « PC numbers set to hit 1 billion », *Techworld* [En ligne] www.techworld.com/news/index.cfm?NewsID=9119 (consulté le 13 novembre 2012).

CHEONG, H. (2012). « Proton Inspira Yes 4G Internet Enabled Car », *Cars, Bikes, Trucks* [En ligne] www.cbt.com.my/2012/02/22/proton-inspira-yes-4g-internet-enabled-car (consulté le 13 novembre 2012).

DIBBELL, J. (2003). « The Unreal Estate Boom », *Wired* [En ligne] www. wired.com/wired/archive/11.01/gaming.html (consulté le 13 novembre 2012).

DUPONT, B., et GAGNON, B. (2008). *La sécurité précaire des données personnelles en Amérique du Nord* : *une analyse des statistiques disponibles*, Montréal, Chaire du Canada en sécurité, identité et technologie, note de recherche nº 1.

ELLIS, J. (2009). « Missouri man held in abuse of Sanger girl », *Fresnobee.com* [En ligne] www.fresnobee.com/local/story/1168587.html (consulté le 10 février 2009). [La page n'est plus disponible.]

EVANS, J. (2011). « Opinion : Apple's plan for the connected home », *Computerworld* [En ligne] blogs.computerworld.com/19012/why_an_internet_of_things_means_an_apple_in_every_home (consulté le 13 novembre 2012).

FELDER, A. (2012). « Making Real Money in Virtual Games : The Strange Economics of MMORPGs », *The Atlantic* [En ligne] www.theatlantic.com/business/archive/2012/04/making-real-money-in-virtual-games-the-strange-economics-of-mmorpgs/256192 (consulté le 13 novembre 2012).

FINJAN (2009). « Code Obfuscation », *Finjan Vital Security* [En ligne] www.finjan.com/Content.aspx?id=1456 (consulté le 9 mai 2009). [La page n'est plus disponible.]

GAGNON, B. (2004). *Are We Headed for a « Cyber-9/11 ? »* : *The Failure of American Cyberstrategy* [En ligne] www.benoitgagnon.net/biographie/biographie/publications_assets/cyberstrategy.pdf (consulté le 10 février 2009). [La page n'est plus disponible.]

GOSTEV, A. (2012). « Cyber-threat evolution : the year ahead », *Computer Fraud & Security Bulletin*, vol. 3, p. 9-12.

HENDRY, A. (2008). « Non-tech criminals can now rent-a-bot », *Network World* [En ligne] www.networkworld.com/news/2008/051508-non-tech-criminals-can-now.html (consulté le 13 novembre 2012).

KRANENBURG, R. Van (2008). « The Internet of Things. A critique of ambient technology and the all-seeing network of RFID », *Network Notebooks* [En ligne] www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf (consulté le 13 novembre 2012).

KRAVETS, D. (2008). « Hackers Launches Botnet Attack via P2P Software », *Wired* [En ligne] www.wired.com/threatlevel/2008/06/hacker-launches (consulté le 13 novembre 2012).

KREBS, B. (2006). « Hacking Made Easy », *The Washington Post* [En ligne] www.washingtonpost.com/wp-dyn/content/article/2006/03/16/AR2006031600916.html (consulté le 13 novembre 2012).

LACK, A. (2009). « Cybercrime Grows Up », *The National Clearing House for Science, Technology and the Law* [En ligne] www.ncstl.org/news/Lack October07 (consulté le 13 novembre 2012).

MARTIN, D. (2008). « Cybercriminalité : l'importance du facteur humain », *Les cahiers de la sécurité*, nº 6, p. 130-139.

MCAFEE (2008). *McAfee Virtual Criminology Report : Cybercrime Versus Cyberlaw* [En ligne] www.ifap.ru/pr/2008/n081212b.pdf (consulté le 13 novembre 2012).

MCAFEE (2009). *Économies non sécurisées. Protection des informations stratégiques* [En ligne] www.3dcommunication.fr/pdf/Unsecured_economies.pdf (consulté le 11 février 2009). [La page n'est plus disponible.]

NEWMAN, J. (2012). « The Android Update Trap », *PC World* [En ligne] www.pcworld.com/article/254304/the_android_update_trap.html (consulté le 13 novembre 2012).

NINO, T. (2008). « Did you give the gift of a hacked account this Christmas? », *Massively* [En ligne] www.massively.com/2008/02/17/did-you-give-the-gift-of-a-hacked-account (consulté le 13 novembre 2012).

PAPPALARDO, D. (2007). « What you need to know about 4G », *NetworkWorld* [En ligne] www.networkworld.com/news/2007/052107-special-focus-4g.html (consulté le 13 novembre 2012).

RF DESIGN (2008). « Worldwide business use of Wi-Fi hotspots increases by 46 %; US 3G data use grows 59 % », *RF Design* [En ligne] rfdesign.com/next_generation_wireless/news/wifi_hotspot_use_1014 (consulté le 13 novembre 2012).

RIBEIRO, J. (2007). « Indian Police Urged to Tap Cybercafes to Fight Terrorism », *PCWorld* [En ligne] www.pcworld.com/article/137107/indian_police_urged_to_tap_cybercafes_to_fight_terrorism.html (consulté le 13 novembre 2012).

RIGUIDEL, M. (2008). « Les technologies numériques du futur : nouvelles menaces, nouvelles vulnérabilités », *Les cahiers de la sécurité*, nº 6, p. 66-77.

ROIG-FRANZIA, M. (2007). « Mexican Drug Cartels Leave a Bloody Trail on YouTube », *The Washington Post* [En ligne] www.washingtonpost.com/wp-dyn/content/article/2007/04/08/AR2007040801005.html (consulté le 13 novembre 2012).

SALEMI, P. (2009). « Parma : Police arrest Michigan man for raping 12-years-old boy he met through online video game network », *Cleveland.com* [En ligne] blog.cleveland.com/parmasunpost/2009/01/parma_police_arrest_michigan_m.html (consulté le 13 novembre 2012).

SCHOOF, R., et KONING, R. (2007). *Detecting peer-to-peer botnets* [En ligne] staff.science.uva.nl/~delaat/sne-2006-2007/p17/report.pdf (consulté le 8 mai 2009). [La page n'est plus disponible.]

SHAH, A. (2008). « Samsung Shipped Infected Digital Picture Frames », *PCWorld* [En ligne] www.pcworld.com/businesscenter/article/156050/samsung_shipped_infected_digital_picture_frames.html (consulté le 13 novembre 2012).

SIDEL, R. (2012). « Big Retailers Join Forces to Develop Mobile Wallet », *The Wall Street Journal* [En ligne] online.wsj.com/article/SB10000872396390444375104577590954176856154.html (consulté le 13 novembre 2012).

SOHIER, D. J. (1998). *Internet* : *le guide de l'internaute 1998*, Montréal, Éditions Logiques.

SWARTZ, J. (2004). « Crooks slither into Net's shady nooks and crannies », *USA Today* [En ligne] www.usatoday.com/tech/news/2004-10-20-cyber-crime_x.htm (consulté le 13 novembre 2012).

SYLVERS, E. (2008). « Social networking benefits from financial crisis », *The New York Times*, 2 novembre [En ligne] www.nytimes.com/2008/11/02/business/worldbusiness/02iht-boss03.1.1743619.html (consulté le 13 novembre 2012).

THE INTERNET OF THINGS COUNCIL (2012). « Internet of Things : what is it? », *The Internet of Things Council* [En ligne] www.theinternetofthings.eu/internet-of-things-what-is-it%3F (consulté le 13 novembre 2012).

UNESCO (2008). « Number of cell phone subscribers to hit 4 billion this year, UN says », *UNESCO* [En ligne] portal.unesco.org/ci/en/ev.php-URL_ID=27530&URL_DO=DO_TOPIC&URL_SECTION=201.html (consulté le 13 novembre 2008).

ZETTER, K. (2010). « Google Hack Attack Was Ultra Sophisticated, New Details Show », *wired.com* [En ligne] www.wired.com/threatlevel/2010/01/operation-aurora (consulté le 13 novembre 2008).