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

10

Piratage informatique

David Décary-Hétu[1]

Qu'ont en commun un journal britannique de nouvelles sensationnalistes et un réseau de jeux vidéo en ligne? Ce sont deux entités qui ont été associées, en 2011, au piratage informatique. Dans le premier cas, des employés sont accusés de s'être frauduleusement connectés à des boîtes vocales en devinant les mots de passe ou en se faisant passer pour leur propriétaire légitime. Dans le second cas, des pirates ont utilisé le réseau de Sony pour s'approprier des dizaines de millions de numéros de cartes de crédit.

Devant la diversité de tels comportements, il est permis de se demander si le terme « piratage informatique » n'a pas été surutilisé, dénaturé et vidé de son sens. Ce chapitre tentera de répondre à cette question et d'offrir une compréhension globale et stratégique de ce qu'est le piratage informatique.

Le point de vue abordé dans ce texte sera très restrictif et limitera notre étude aux connexions sans autorisation à des systèmes informatiques. Nous verrons qu'il existe plusieurs façons de classer les pirates informatiques, selon que l'on s'intéresse à leurs motivations ou encore à leurs connaissances techniques. Ils utilisent en effet trois techniques que nous définirons, soit le décryptage, le piratage et l'ingénierie sociale. Bien que

1. Candidat au doctorat, École de criminologie de l'Université de Montréal.

les statistiques officielles soient encore fragmentaires, nous démontrerons l'impact du piratage au Canada comme ailleurs dans le monde.

Afin de mieux illustrer les différentes facettes et la complexité du phénomène du piratage informatique, nous présenterons aussi trois cas pratiques de pirates informatiques impliqués autant dans le vol et le recel de numéros de cartes de crédit que de pirates cherchant à faire avancer leurs vues politiques. Bien que deux de ces cas soient basés sur les histoires de pirates accusés, nous verrons que les enquêtes les concernant font face à d'énormes obstacles, dont la détection même des attaques ainsi que celle de leur source et de l'identité des pirates. Nous terminerons ce chapitre avec une ouverture sur l'avenir des pirates informatiques.

10.1 Définitions

L'expression « piratage informatique » a été utilisée de bien des façons au cours des dernières années. Dans le milieu scolaire et dans les médias, une série de conduites, allant de l'accès sans autorisation à un ordinateur jusqu'au téléchargement illégal de contenu en passant par l'utilisation de mots de passe d'autrui, sont associées au piratage informatique. Pour les besoins de ce chapitre, nous utiliserons une définition plus simple et limitée de ce type de criminalité afin de restreindre notre champ d'études et ainsi d'arriver à une discussion plus en profondeur sur le sujet. Nous définissons donc le piratage informatique comme « le geste d'accéder à un système informatique sans autorisation » (Brenner, 2001).

10.2 Types de piratages informatiques

La définition du piratage informatique comme présenté par Brenner (2001) est volontairement restrictive puisqu'elle limite les comportements considérés comme des actes de piratage au fait de s'introduire sans autorisation dans un système informatique. Dans la littérature, nous avons identifié trois catégories d'attaques permettant de faciliter l'analyse du phénomène : le décryptage (Gold, 2011; Murakami et coll., 2010), le piratage (Estehghari et Desmedt, 2010; Razvan, 2009) et l'ingénierie sociale (Mann, 2010; Workman, 2008). Chacune d'entre elles sera présentée succinctement dans cette section.

La famille du décryptage inclut toutes les tentatives de deviner les mots de passe permettant d'accéder à un système informatique (Rowan, 2009). Pour ce faire, les pirates peuvent compter sur plusieurs outils de décryptage accessibles gratuitement et faciles d'utilisation (ex. : John The Ripper; L0phtcrack). Ceux-ci adoptent généralement deux approches : celle du dictionnaire ou celle de la force brute (Rowan, 2009).

Dans le cas du dictionnaire, le logiciel utilise une liste des mots de passe les plus courants et des mots communs du dictionnaire afin de deviner les mots de passe les plus vulnérables. Les utilisateurs ont en effet tendance à utiliser des mots de passe très simples du style « 1234 » ou encore « password » (Florencio et Herley, 2007). En se limitant à une liste de quelques milliers de mots, il est possible de deviner rapidement une bonne proportion des mots de passe. Dans le cas de la force brute, le criminel essaie tous les mots de passe possibles en commençant par « a », « b », […], « aa », « ab » et ainsi de suite jusqu'à ce qu'il découvre le mot de passe utilisé. Ce processus nécessite une grande dose de patience, car un jeu de caractères très large prendra des millénaires à décrypter.

Les attaques de type dictionnaire ou de force brute peuvent être réalisées en ligne ou hors ligne (Yazdi, 2011). Dans le premier cas, le pirate se connecte par un réseau à sa cible et essaie tour à tour des mots de passe en espérant arriver à se connecter. On pourrait penser ici à un pirate qui essaierait un à un tous les mots de passe possibles pour un compte de courriel Google. Dans la mesure où l'attaquant ne connaît habituellement ni la longueur ni le jeu de caractères utilisé (minuscule ou majuscule, chiffres, lettres, caractères spéciaux), ce travail doit se faire à l'aveugle et peut prendre de quelques secondes à quelques millénaires selon la complexité et la longueur du mot de passe visé[2]. Dans le cas d'une attaque hors ligne, l'attaquant possède une copie des mots de passe cryptés. Son travail consiste donc à tenter de deviner quelle série de caractères, une fois cryptée, se cache dans cette liste de mots de passe. Une attaque hors ligne sera toujours beaucoup plus rapide, car l'attaquant n'est pas limité par la connexion Internet qui le sépare de sa cible. Bien qu'un serveur ne prenne souvent que quelques millisecondes pour répondre à une requête, des millions de demandes engendreront

2. La Gibson Research Corporation offre un outil en ligne qui permet d'estimer le temps nécessaire pour deviner un mot de passe en tenant compte de sa complexité et de son jeu de caractères (www.grc.com/haystack.htm).

de longs délais dans le décryptage de mots de passe. Les attaques hors ligne peuvent aussi être accélérées par l'utilisation de *rainbow tables*, des bases de données qui contiennent une vaste quantité de mots de passe ainsi que leur équivalent crypté (Theocharoulis et coll., 2010). Il suffit d'y rechercher un mot de passe crypté pour avoir accès à son texte non crypté. Ce type d'outil est très utile, mais nécessite souvent des téraoctets de données, ce qui limite sa circulation.

N'importe quel mot de passe peut être décrypté; il s'agit simplement d'y consacrer le temps nécessaire. Afin d'éviter d'attendre interminablement le résultat de cette opération, les pirates peuvent plutôt tenter de pirater les systèmes informatiques pour y avoir accès. Ce processus est souvent illustré dans la culture populaire par un pirate qui tape frénétiquement sur un clavier pendant quelques secondes jusqu'à ce que la mention « accès autorisé » apparaisse à l'écran.

Dans la réalité, le piratage est un peu plus complexe et cherche à profiter des mauvaises configurations (Wood et Pereira, 2011) ou des erreurs des programmeurs (Abadeh et coll., 2007). Dans le premier cas, le pirate arrive à accéder aux ressources d'un système informatique qui sont mal protégées. Poulsen (2011) illustre ce type d'attaque en présentant le *modus operandi* de Max Vision, un pirate informatique arrêté et incarcéré dans les années 2000. Ce dernier avait en effet découvert que certains serveurs responsables du traitement des cartes de crédit de restaurants demandaient systématiquement aux personnes s'y connectant le niveau de sécurité qu'elles désiraient utiliser. Il n'avait alors qu'à répondre « aucune » pour avoir accès aux systèmes. La mauvaise configuration des serveurs exposait donc à tous les internautes certaines fonctionnalités qui auraient dû être privées.

Par ailleurs, les serveurs configurés selon les règles de l'art ne sont pas nécessairement à l'abri des actes de piratage. Les pirates peuvent en effet profiter des erreurs de programmation qui se glissent dans la production de logiciels pour obtenir illégalement un accès à des systèmes informatiques. Ces erreurs permettent aux pirates de profiter de systèmes en contournant ou en manipulant le processus d'authentification. Certains logiciels d'attaque « clé en main » (ex. : Metasploit) facilitent grandement ces attaques en prenant en charge le côté technique du piratage. Les vendeurs de logiciels ont relativement peu de raisons de s'inquiéter de la sécurité des logiciels qu'ils vendent. Il est vrai qu'une attaque contre

leurs produits peut ternir leur image, mais ce sont leurs clients et non eux qui subiront le gros de l'impact des attaques (Kim et coll., 2010). Par ailleurs, valider la sécurité des logiciels coûte très cher (Wright et Zia, 2010). Les compagnies préfèrent donc régler les vulnérabilités signalées par des tierces parties plutôt que de dépenser de vastes sommes d'argent pour rechercher de possibles menaces. Comme la sécurité n'est pas une priorité, en général, pour les producteurs de logiciels, il existe un nombre important de vulnérabilités que les pirates peuvent utiliser pour contourner l'authentification des systèmes informatiques (Symantec, 2011).

Alors que le décryptage et le piratage utilisent des moyens technologiques pour s'attaquer à leurs cibles, l'ingénierie sociale se concentre sur le facteur humain pour obtenir frauduleusement un accès à un système informatique. L'ingénierie sociale est ainsi considérée comme « l'utilisation d'une interaction sociale dans le but d'obtenir une information sur le système informatique de la victime » (Winkler et Dealy, 1995).

Kevin Mitnick a été l'un des premiers à mettre en évidence le pouvoir de l'ingénierie sociale et a écrit plusieurs ouvrages sur le sujet depuis sa sortie de prison (Mitnick et Simon, 2002, 2005; Mitnick, 2011). Au lieu de forcer son entrée sur un système, le pirate qui utilise l'ingénierie sociale tente de convaincre sa cible de lui ouvrir elle-même les portes des systèmes. Il s'agit ici de jouer sur les émotions et les sentiments des individus afin qu'ils coopèrent avec le pirate (Workman, 2008). Cela peut se faire en communiquant un sentiment d'urgence ou encore en jouant sur les peurs des gens, par exemple. Le succès de l'opération dépend en grande partie du prétexte, le scénario utilisé pour berner la cible. Souvent, les histoires les plus simples sont les plus efficaces. Pour s'introduire dans les bureaux d'une compagnie de télécommunications, Mitnick (2011) raconte qu'il s'est présenté tard dans la soirée à la guérite de sécurité et a simplement demandé au garde s'il pouvait faire visiter ses locaux de travail à un ami. Quelques minutes plus tard, Mitnick et ses complices se promenaient librement dans les locaux de la compagnie et mettaient la main sur une liste de mots de passe ainsi que sur des manuels techniques. Une ingénierie sociale réussie nécessite habituellement une bonne connaissance de la cible. Dans l'exemple ci-dessus, Mitnick connaissait déjà le numéro du local où se trouvait l'information recherchée, réduisant ainsi le temps nécessaire pour trouver les mots de passe et les risques de détection. Les possibilités qu'offre l'ingénierie

sociale sont illustrées dans le dernier rapport des organisateurs de la compétition d'ingénierie sociale qui a eu lieu à la conférence de pirates informatiques Defcon en 2010 (Hadnagy et coll., 2010). On y découvre que sur les 15 compagnies testées lors de l'exercice, 14 ont laissé filtrer de l'information, soit un taux de succès de plus de 93 %. Bien que l'information obtenue lors du concours ne soit pas nécessairement de nature confidentielle, cet exercice démontre l'efficacité de la technique dans cet environnement contrôlé.

10.3 Types de pirates informatiques

De par la nature même d'Internet, il est extrêmement difficile de déterminer les caractéristiques sociodémographiques des internautes et encore plus des pirates qui s'y cachent. Les recherches s'entendent cependant sur quelques caractéristiques communes à une grande proportion de pirates. Ceux-ci sont, dans une écrasante majorité, de sexe masculin (Goldman, 2005; Jordan et Taylor, 1998; Turgeman-Goldschmidt, 2011). Ils sont caucasiens (Turgeman-Goldschmidt, 2011) et plus jeunes que vieux (Yar, 2005; Goldman, 2005). Les autres caractéristiques sociodémographiques des pirates, telles que leur profil scolaire, professionnel ou social, varient grandement d'échantillon en échantillon (Goldman, 2005).

Pour différencier les pirates les uns des autres, la littérature définit deux axes : la motivation et les capacités techniques. Les typologies motivationnelles tentent de classifier les pirates informatiques en fonction des motivations qui les poussent à agir. Baillargeon-Audet (2010) présente une recension intéressante des typologies proposées où il est possible de cerner cinq motivations principales : la reconnaissance, l'argent, les défis techniques, l'idéologie et la curiosité. Nos propres recherches nous ont permis d'ajouter à cette liste une sixième motivation, l'altruisme.

Les pirates altruistes cherchent avant tout à aider les autres en testant leurs systèmes pour détecter des failles de sécurité et ensuite avertir plus ou moins discrètement les administrateurs de systèmes (Leeson et Coyne, 2005). Ceux-ci n'ont *a priori* pas la permission de commettre ces attaques et s'exposent donc à des représailles légales sérieuses. La soif de reconnaissance est aussi un besoin que les pirates cherchent à combler à travers leurs piratages (Rehn, 2003; Jordan et Taylor, 1998). Ceux-ci

ont tendance à former des alliances plus ou moins solides et tentent de s'impressionner mutuellement afin de se valoriser aux yeux de cette communauté (Rehn, 2003). Alors que la quête de reconnaissance est présente dans le monde des pirates depuis sa conception, la recherche de gains financiers est, quant à elle, beaucoup plus récente. Cette motivation prend de plus en plus d'importance et les recherches récentes ont permis de mettre en évidence l'envergure des sommes volées régulièrement par les pirates (Krebs, 2011; Leeson et Coyne, 2005; Kshetri, 2005). Tous les pirates ne sont pas uniquement motivés par l'argent cependant : Grabosky (2000) et Goode et Cruise (2006) démontrent en effet que les défis cognitifs sont assez stimulants pour occuper les pirates des heures durant. La reconnaissance est alors intrinsèque, car ceux-ci sont simplement satisfaits d'avoir déjoué les concepteurs de systèmes ou de logiciels.

Les pirates avares ne sont pas les seuls à avoir connu une vague de popularité au cours des dernières années. Les hacktivistes comme Anonymous ou LulzSec ont mené diverses campagnes de piratage récemment, réussissant même à mettre en déroute des compagnies de sécurité (Krebs, 2011).

La cinquième motivation, la curiosité, est plus rare. Le célèbre pirate Kevin Mitnick a toujours affirmé que sa motivation principale était la curiosité (Mitnick, 2011). Rojas (2010) rapporte aussi le cas de Gary McKinnon, qui a été accusé d'avoir piraté l'armée de l'air, l'armée de terre et le département de la Défense américain afin de faire la lumière sur le phénomène des extraterrestres.

D'autres chercheurs, comme Rogers (1999), se basent sur les capacités techniques des pirates plutôt que sur leurs motivations pour les distinguer. Rogers (1999) distingue quatre groupes :

1. les pirates aînés, non criminalisés, qui s'intéressent à la technologie avant tout et qui estiment que toute information devrait être gratuite;
2. les pirates adolescents (*script kiddies*), qui utilisent des logiciels automatisés pour mener à terme des attaques sans avoir les connaissances nécessaires pour comprendre ce qu'ils font ni créer d'autres outils;

3. les criminels professionnels, qui se consacrent à temps complet au piratage, en font un moyen de subsistance et sont embauchés par les gouvernements, les compagnies et le crime organisé;
4. les programmeurs qui produisent le code malicieux utilisé par les autres groupes pour pirater.

Cette typologie rejoint celle de Ghernaouti-Hélie (2002), qui différencie les amateurs (pirates adolescents) des professionnels (pirates aînés, professionnels et programmeurs).

Rogers (2006) a récemment modifié cette typologie et a ainsi créé un modèle hybride qui tient compte des connaissances techniques et des motivations des pirates. Le résultat est une typologie qui comprend neuf catégories :

1. le novice, qui est le néophyte utilisant des outils automatiques et cherchant à se faire un nom;
2. le cyberpunk, légèrement supérieur au novice, qui programme minimalement et recherche la gloire et l'argent;
3. l'initié, qui attaque son employeur de l'intérieur pour se venger;
4. le simple voleur, qui passe du monde réel au virtuel afin de suivre ses cibles comme les banques et les compagnies de cartes de crédit et qui a pour principale motivation l'argent;
5. le programmeur de virus;
6. le pirate de vieille garde, qui a hérité de la mentalité des vieux pirates des années 1960 et qui recherche la stimulation intellectuelle;
7. le criminel professionnel spécialisé dans la criminalité informatique et recherchant les gains financiers;
8. le guerrier de l'information, qui a pour objectif de déstabiliser les centres de décision et qui est motivé par le patriotisme;
9. l'activiste politique.

Ces différentes typologies mettent en lumière la diversité des individus impliqués dans les actes de piratage. Ceux-ci ont des motivations et des connaissances techniques variant d'un profil à l'autre. Les données sociodémographiques portant sur ces individus sont très limitées de par la nature d'Internet. Une étude de Goldman (2005) portant sur

les pirates qui distribuent illégalement de la propriété intellectuelle a montré que les profils allaient de l'employé d'âge mûr travaillant pour une compagnie informatique à l'étudiant du niveau secondaire. Leur seul point en commun était qu'il s'agissait en grande partie d'hommes. Beaucoup de travail reste encore à faire avant d'arriver à dresser un portrait type du pirate informatique, mais tout porte à croire que ce profil sera aussi diversifié que celui des délinquants plus traditionnels.

10.4 Difficultés émanant de la question du piratage informatique

La question du piratage informatique pose deux problèmes de taille : l'identification des responsables (Wheeler et Larsen, 2003) et la détection des infractions (Axelsson, 2000). Autant la recherche que le contrôle de cette criminalité sont affectés par ces deux problèmes que nous décrirons en détail dans cette section.

L'identification des pirates informatiques est un processus en deux étapes qui implique d'une part de retracer l'ordinateur utilisé pour mener une attaque et, d'autre part, d'identifier la personne qui contrôlait l'ordinateur au moment de l'attaque. La configuration d'Internet est telle qu'il est aisé pour les délinquants d'utiliser plusieurs ordinateurs relais qui servent à camoufler l'origine réelle du piratage. Ainsi, même dans les cas où un enquêteur arriverait à reconnaître un ordinateur ayant servi dans une attaque, celui-ci pourrait n'être que le dernier d'une série de machines utilisées comme relais dans l'attaque. La seule solution à ce problème serait de réaliser des analyses techniques en profondeur de chacun des ordinateurs impliqués dans une attaque. Comme chaque pays possède des lois et procédures légales différentes, tenter de récupérer tous ces ordinateurs à des fins d'analyse s'annonce comme un cauchemar opérationnel et bureaucratique insurmontable. Bellia (2001) offre, à ce sujet, une analyse des difficultés qui peuvent se poser dans de telles enquêtes.

Retracer l'origine physique d'une attaque n'est cependant qu'une première étape; identifier la personne qui avait le contrôle du clavier lors de l'attaque est tout aussi critique. Pour ce faire, les enquêteurs peuvent utiliser le *modus operandi* du pirate. Il s'agit ici d'étudier les techniques de décryptage de mots de passe, les patrons d'attaque et les outils utilisés.

Jones et Romney (2004) avancent que les *honeypots*, des serveurs vulnérables placés sur Internet afin d'attirer les pirates, peuvent être des outils utiles pour réaliser ce type de profilage. Les enquêteurs peuvent aussi utiliser des preuves issues d'enquêtes plus traditionnelles comme les caméras de surveillance et la géolocalisation. Shaw (2006) propose une approche qui structure cette recherche de preuve et la découpe en trois temps, soit la détection du nombre d'attaquants, les caractéristiques des attaquants et l'évaluation de la dangerosité des attaquants.

Évidemment, l'identification des pirates et des outils utilisés dépend de la détection des actes de piratage. Comme nous l'avons mentionné précédemment, une nouvelle génération de pirates est maintenant surtout motivée par l'enrichissement personnel. Elle a donc tout intérêt à discrètement s'introduire dans les systèmes et à y rester aussi longtemps que possible. Une telle technique a été qualifiée de « menace avancée et persistante », et cette expression fait régulièrement les manchettes (Watchguard Technologies, 2011). Cette stratégie permet d'amasser une grande quantité d'informations confidentielles et de les exfiltrer lentement. Les systèmes de détection des intrusions ne sont en général pas configurés pour détecter de telles fuites et leur utilité en est donc significativement réduite. Devant l'ampleur des réseaux modernes et le nombre de connexions actives, il n'est guère surprenant de constater la difficulté qu'on a à déceler les comportements suspects.

Plusieurs groupes de pirates ont annoncé publiquement qu'ils avaient réussi à s'infiltrer dans des réseaux privés et à en extraire d'énormes quantités d'informations confidentielles sans que leurs propriétaires s'en rendent compte (Winder, 2011). L'exemple de la Japonaise Sony a démontré à quel point les conséquences de telles attaques peuvent être importantes. Prise à partie par des pirates pour sa mauvaise sécurité informatique (plusieurs dizaines de millions de numéros de cartes de crédit ont été volés sur son réseau; voir Schreier, 2011), la compagnie a dû fermer pendant plusieurs semaines son réseau de jeu en ligne en plus de devoir compenser des millions de clients.

10.5 Statistiques

Les statistiques sur le piratage informatique se font encore très rares malgré l'importance grandissante du problème. Plusieurs facteurs

viennent limiter la capacité des sondeurs à évaluer la problématique actuelle : le manque de consensus sur les définitions, la collecte hétérogène des données, la difficulté à détecter les activités criminelles, le manque de ressources policières ainsi que le manque de coopération des victimes (Mason, 2008). Le manque de ressources policières n'est pas propre au phénomène des cybercrimes, mais est exacerbé dans ce cas par un manque de formation, une incapacité à surveiller les comportements sur Internet, l'apathie du public et des lacunes au regard du partage de l'information (Davis, 2010). Nos recherches nous ont tout de même permis d'amasser quelques données sur le piratage informatique au Canada et dans le monde.

En Angleterre, une évaluation conservatrice de l'aveu des auteurs estime que 5 % des ordinateurs ont été infectés par un virus (Greenish et coll., 2011). Le tiers des vols de données en 2010 seraient le fait de pirates informatiques. Chaque dossier personnel volé dans ces attaques aurait une valeur de 106 $, ce qui représente une augmentation de plus de 10 % par année depuis les deux dernières années. Chaque acte de piratage causerait la perte d'entre 6 900 et 72 000 dossiers personnels. Un autre rapport anglais (Fafinski, 2006) affirme que 40 % des 92 000 cas de vol d'identité sont le résultat de piratage en ligne. Plus de 144 500 accès non autorisés à un ordinateur auraient eu lieu dans le pays en 2006 et 17 000 actes de pénétration illégale de réseau auraient été recensés. Environ 100 personnes auraient été accusées pour ces crimes.

Aux États-Unis, 23 % des entreprises ont été victimes de cybercrimes (PricewaterhouseCoopers, 2011a). Les menaces viennent surtout de l'extérieur (46 %) ou de l'intérieur et de l'extérieur (26 %). Les compagnies craignent que ces attaques ternissent leur réputation (40 %) et entraînent le vol de données personnelles (36 %) ou confidentielles (35 %). Dans le dernier rapport combiné du CSI/FBI (2006), il est noté par ailleurs que 21,6 % des attaques étaient dirigées contre des cibles précises alors qu'un tel constat n'était pas concluant dans 24 % des cas. Les entreprises sont surtout visées par des virus ou de l'hameçonnage. La pénétration de réseau sans fil ou le décryptage de mots de passe n'affectaient que 18,8 % des compagnies.

Une dernière étude américaine mérite d'être rapportée (Davis, 2010). Les policiers de Caroline du Nord sondés par l'analyste y indiquent qu'environ 6 % des enquêtes policières incluent un aspect cyber. La très grande majorité d'entre elles (79,3 %) visent des fraudes, de la

contrefaçon ou du vol. Seulement 1,9 % des enquêtes s'intéressent aux cyberattaques ou à la « cyberoccupation ».

À l'échelle canadienne, 8 % des entreprises ont été victimes de crimes informatiques en 2011 (PricewaterhouseCoopers, 2011b) et 26 % d'entre elles craignaient d'en être victimes dans l'année à venir. La majorité (53 %) des compagnies sont attaquées de l'intérieur et de l'extérieur. Les attaques externes viennent en particulier de Hong Kong (et de la Chine), de l'Inde, du Nigéria, de la Russie et des États-Unis. Les entreprises pensent avoir les effectifs nécessaires pour détecter 60 % des cybercrimes, enquêter sur 36 % d'entre eux, et ont accès facilement à des consultants externes dans 47 % des cas. La majorité (51 %) affirme informer les autorités lorsqu'elles sont victimes de cybercrimes. Dans 23 % des cas de crimes économiques, le vecteur d'attaque était le cybercrime.

Les citoyens canadiens sont aussi visés par les cybercriminels. Environ 4 % d'entre eux ont été victimes de fraude bancaire sur Internet (Perreault, 2011), un phénomène souvent relié au piratage informatique. Les personnes riches et habitant en ville sont beaucoup plus à risque d'être victimes que les personnes moins fortunées ou qui habitent en région. Perreault (2011) affirme aussi que 65 % de la population canadienne a été victime d'un virus au cours de l'année.

10.6 Cas pratiques

Ce chapitre met en évidence la diversité et l'étendue de la problématique du piratage informatique. Cette section présente trois cas concrets au cours desquels le piratage informatique a été utilisé pour amasser des millions de dollars illégalement. Le premier exemple est relié au vol de cartes de crédit, le deuxième s'intéresse à la fraude dans la vente de billets d'événements sportifs et culturels alors que le dernier se penche sur les incidents survenus entre le groupe Anonymous et la compagnie HBGary Federal.

10.6.1 Piratage de terminaux de vente

Le piratage informatique est un moyen très utile pour obtenir frauduleusement des numéros de cartes de crédit. En décembre 2011, des

procureurs américains ont accusé quatre individus roumains de piratage informatique dans le cadre d'une fraude impliquant le vol de ces numéros (Zetter, 2011). Les criminels avaient réussi à s'infiltrer dans les systèmes de paiement de 200 magasins et restaurants. La plupart des ordinateurs gérant les paiements par carte de crédit disposent d'un logiciel qui permet un accès à distance afin que des techniciens puissent régler les problèmes de traitement sans avoir à se déplacer. Les pirates accusés avaient deviné ou décrypté les mots de passe de ces logiciels de contrôle à distance afin de se connecter aux systèmes.

Une fois sur ces ordinateurs, les pirates avaient un accès total à toutes les fonctions ainsi qu'aux données des ordinateurs. Ils utilisaient des logiciels espions afin de sauvegarder une copie de tous les numéros de cartes de crédit qui transitaient par ces systèmes. Après quelques semaines ou quelques mois, les informations colligées étaient transférées vers des serveurs externes loués avec des cartes de crédit volées ou encore sur d'autres ordinateurs piratés. Afin de vendre l'information, les pirates demandaient de recevoir un virement bancaire par Western Union. Après réception du paiement, ils envoyaient les informations par courriel ou donnaient simplement un accès au serveur à l'acheteur. Dans certains cas, les pirates informatiques imprimaient eux-mêmes de fausses cartes de crédit afin de faire des paris sportifs ou des achats en ligne. Ce groupe criminalisé a été responsable à lui seul du vol de plus de 80 000 cartes et de millions de dollars en achats non autorisés. Dans ce cas pratique, les pirates n'avaient recours qu'au décryptage pour commettre leur piratage informatique. Leur façon de procéder était similaire à celle de plusieurs autres cybercriminels professionnels tel Max Butler, un célèbre pirate au centre du livre de Kevin Poulsen (2011). Leur motivation semble être uniquement d'ordre monétaire et, à en croire l'acte d'accusation, leur entreprise criminelle a été en mesure de les enrichir considérablement.

10.6.2 Achat de billets en ligne

Les promoteurs ont de plus en plus recours à Internet pour vendre les billets de leurs événements sportifs et culturels. Ce marché primaire de billets est contrôlé par un nombre très limité d'entreprises comme TicketMaster, LiveNation et Tickets.com. Cette concentration du pouvoir a permis l'instauration de règles d'utilisation très strictes de ces

services, notamment en ce qui a trait à l'accès aux billets. Les acheteurs sont habituellement limités dans le nombre de billets qu'ils peuvent se procurer pour chaque événement et les premiers arrivés ont priorité pour le choix des places. Ces façons de procéder créent une rareté et une intense compétition pour obtenir les meilleurs sièges aux plus grands événements. Pour les malchanceux qui n'ont pu obtenir les places désirées, un marché secondaire permet d'acheter et de vendre les billets à un prix souvent supérieur au prix d'achat initial. Un individu qui disposerait d'un nombre important de billets recherchés sur le marché secondaire pourrait aisément amasser une fortune très rapidement.

C'est avec cet objectif que quatre associés ont lancé l'entreprise Wiseguys Tickets Inc. en 2005. Accusés en 2010 de piratage informatique et de nombreux autres délits, ces quatre entrepreneurs ont su en quelques années monter une entreprise du crime organisé qui les a rendus maintes fois millionnaires (plus de 20 millions de dollars de profits selon les autorités; Zetter, 2010). Leur but était de parvenir à mettre la main sur un maximum de billets pour des événements culturels et sportifs dans le marché primaire afin de les revendre à profit sur le marché secondaire. Dans la mesure où les sites de vente de billets stipulent que toutes les ventes sont des ventes finales à des consommateurs, une telle pratique est illégale aux États-Unis. Plusieurs techniques ont été mises en place pour assurer un contrôle des ventes, soit la surveillance du comportement des utilisateurs sur le site de vente, la réussite d'un CAPCHA ainsi que l'analyse des transactions financières. Le CAPCHA est un test répandu sur Internet, qui consiste à présenter à l'utilisateur une image contenant des caractères déformés facilement reconnaissables à l'œil humain, mais difficilement interprétables par un logiciel automatisé. L'objectif d'un tel outil est de bloquer les robots et de s'assurer que la « personne » qui remplit un formulaire est bien un humain.

Pour contourner ces systèmes, les Wiseguys ont utilisé un stratagème complexe qui fait appel autant au piratage qu'à l'ingénierie sociale. Ils ont tout d'abord eu recours à des pirates informatiques embauchés sur contrat pour bâtir un logiciel capable de parcourir un site Web de vente de billets en imitant le comportement d'un humain et de réserver en une fraction de seconde les meilleures places d'un événement. Un opérateur était alors chargé de confirmer les billets qu'il fallait acheter et le logiciel

s'occupait de remplir le formulaire de vente. La compagnie Wiseguys s'est aussi abonnée au même service qui fournissait les CAPCHA aux sites de vente de billets. En ayant accès au même flux que les autres, il leur était possible de prendre en note le numéro de série de chacun et de demander aux employés de résoudre chacun d'entre eux. Le logiciel n'avait alors plus qu'à rechercher ce numéro de série dans une base de données pour trouver la bonne réponse. Étant donné le grand nombre de possibilités de CAPCHA, les Wiseguys ont aussi eu recours au piratage informatique pour obtenir le code source qui générait les CAPCHA sur les sites. Une fois ce fonctionnement compris, il était possible pour leur robot de trouver seul les réponses aux CAPCHA. Le logiciel ainsi créé était extrêmement complexe et arrivait à faire croire aux systèmes de protection qu'il était un utilisateur légitime du service de vente. Les compagnies chargées de vendre les billets détectaient malgré tout régulièrement les robots et les Wiseguys devaient utiliser constamment de nouvelles adresses IP et de nouveaux pseudonymes pour se créer de fausses identités acceptées par les sites de transaction.

Cet exemple illustre plusieurs phénomènes en lien avec le piratage informatique moderne. Tout d'abord, il existe un marché de pirates mercenaires disposés à créer des logiciels malveillants sur demande. Ceux-ci sont qualifiés et capables de livrer des systèmes intégrés extrêmement complexes. Par ailleurs, les meilleurs systèmes de détection ne feront jamais que ralentir les criminels. Ceux-ci pourront toujours se trouver de nouveaux serveurs et de nouvelles adresses IP pour camoufler leur réelle identité. Ils mèneront aussi des rondes de reconnaissance et trouveront un prétexte (ingénierie sociale) pour obtenir d'employés ou d'ex-employés des informations permettant de contourner les systèmes de détection des robots. Finalement, le piratage à grande échelle comme celui opéré dans le cas des Wiseguys a créé un quasi-monopole de la revente de billets dans un marché secondaire alors que la grande majorité des billets revendus étaient achetés des grossistes qui s'approvisionnaient chez les Wiseguys. Cette entreprise a accumulé des millions de dollars en profits et vendu des centaines de milliers de billets avant d'être perquisitionnée par la police. L'accès à de telles ressources génère une forte tentation chez des délinquants motivés et offre les outils nécessaires à la création d'entreprises criminelles bien organisées et capables de rivaliser technologiquement avec les grands de l'industrie.

10.6.3 Anonymous contre HBGary Federal

Comme nous l'avons mentionné précédemment, l'argent n'est pas la seule source de motivation des pirates informatiques. Au cours de l'année 2011, un groupe de pirates appelé Anonymous a fait les manchettes à plusieurs reprises. Motivé avant tout par un désir de justice et de liberté, ce groupe de pirates très informel s'est lancé à l'attaque de compagnies de cartes de crédit pour leur censure de Wikileaks (Watters, 2010), de services de police pour leur attitude envers les immigrants (Albanesius, 2011) et du service de transport public de San Francisco pour avoir bloqué l'usage de cellulaires lors d'une manifestation (Whittaker, 2011). Ce groupe d'individus n'est pas structuré et ne possède pas de leaders officiels. Il discute d'opérations futures sur des canaux IRC et publie des messages de relations publiques pour souligner ses prises de position. Étant donné le haut profil public d'Anonymous dans l'actualité, plusieurs experts en sécurité ont tenté de découvrir l'identité des individus qui se cachent derrière cette association de pirates criminels.

HBGary Federal était l'une de ces compagnies (Bright, 2011a). Elle offrait des produits et services de sécurité à de grandes sociétés ainsi qu'à des organismes publics américains comme la National Security Agency (NSA). Profitant de la vague d'attention portée à Anonymous, le directeur général de la société, Aaron Barr, a annoncé à l'avance qu'il allait dévoiler l'identité des membres d'Anonymous lors d'une prochaine conférence sur la sécurité. Face à cette menace, les membres d'Anonymous ont exploité une mauvaise configuration dans le serveur Web de la compagnie pour accéder à une liste cryptée des mots de passe de ses administrateurs. Une fois la liste téléchargée, une *rainbow table* a pu décrypter les mots de passe de Barr ainsi que ceux du directeur des opérations de la compagnie, Ted Vera. Cette information était suffisante pour obtenir le contrôle complet du site Web de la compagnie.

Non satisfaits, les pirates ont sondé plus intensément les systèmes informatiques de la compagnie et ont découvert un autre serveur qui contenait des copies de sûreté des courriels de l'entreprise ainsi que des rapports de recherche. Les mots de passe donnant accès au site Web donnaient aussi accès à ce deuxième serveur. Le directeur général de l'entreprise utilisait les mêmes mots de passe pour son compte de courriel hébergé par Google. De par sa position, il avait aussi accès au panneau

d'administration des courriels de tous les employés de l'entreprise; les pirates pouvaient donc changer n'importe quel mot de passe de courriel des employés. Barr était également responsable du site rootkit.com, un site d'échange et de discussion pour les experts en sécurité intéressés par les virus. Les pirates ont alors utilisé la messagerie du directeur général afin de le personnifier et de convaincre un de ses collègues de changer son mot de passe pour le serveur hébergeant le site rootkit.com afin qu'ils puissent le défigurer.

Une compagnie de sécurité qui se fait elle-même pirater démontre son incapacité à se défendre. Dans quelle mesure peut-elle alors défendre ses clients? À la suite de ces piratages, Anonymous a annoncé publiquement la compromission totale de l'entreprise. Pour le prouver, le groupe a publié toutes les communications de l'entreprise ainsi que plusieurs documents de recherche. Il a aussi modifié les pages Web de HBGary Federal ainsi que le site rootkit.com afin que tous soient au courant des actions d'Anonymous.

Les différents cas présentés dans cette section illustrent comment, dans la pratique, le décryptage, le piratage et l'ingénierie sociale peuvent être utilisés pour amasser de l'argent ou encore humilier son adversaire. Ces histoires ne devraient pas être interprétées comme une preuve de l'omnipuissance des pirates informatiques, mais bien comme un avertissement du fait qu'une mauvaise configuration de ressources en ligne peut mener à la chute rapide d'une entreprise. Les experts et responsables de la sécurité se doivent d'investir temps, énergie et ressources dans leurs systèmes de protection, à défaut de quoi des cas comme ceux de HBGary Federal pourraient se multiplier au cours des prochaines années.

10.7 Législation

Le Canada a été confronté dès les années 1980 aux difficultés qu'il y a à appliquer d'anciens articles du Code criminel au contexte informatique. C'est le cas par exemple de l'arrêt *R.* c. *Stewart* (1988) qui stipule que pour qu'il y ait un vol, une chose quelconque doit pouvoir faire l'objet d'un droit de propriété et doit être susceptible de priver la victime de son bien. Dans le cas de vol de données confidentielles ou de fichiers informatiques, la victime ne perd pas nécessairement la jouissance de son bien et le criminel ne peut donc être accusé en vertu du Code criminel.

Depuis ce jugement, le législateur a voté nombre de lois visant à interdire explicitement certains comportements dans le cyberespace. Les cinq principales infractions sont décrites ci-dessous.

10.7.1 Utilisation non autorisée d'un ordinateur (342.1 C.cr.)

Cet article, en vigueur depuis 1985, est le plus utilisé dans la lutte au piratage informatique. Son libellé stipule que ce crime est commis lorsque « quiconque, frauduleusement et sans apparence de droit, directement ou indirectement, obtient des services d'ordinateur ou […] intercepte une fonction d'un ordinateur ». Le législateur interdit donc ici tout accès à un ordinateur ou toute utilisation d'un ordinateur qui ne serait pas légitime. Un individu utilisant une faille de vulnérabilité pour avoir accès à une base de données contenant des informations confidentielles pourrait être poursuivi en vertu de cet article. La peine maximale est de 10 ans.

10.7.2 Possession de moyens permettant d'utiliser un service d'ordinateur (342.2 C.cr.)

En 1997, le législateur a voté cette loi qui stipule qu'une personne commet un crime lorsqu'elle fournit des instruments (ou des pièces de ceux-ci) permettant de commettre une utilisation non autorisée d'un ordinateur. Il est donc maintenant illégal au Canada de posséder des outils de pirates comme des logiciels de conception de virus. La peine maximale est de deux ans.

10.7.3 Méfait concernant des données [430(1.1) C.cr.]

Cette loi criminalise le fait de s'attaquer aux données en les détruisant, en les modifiant ou en gênant leur accès. Il est ici question de la libre jouissance des données. Les personnes qui inondent les serveurs de données illégitimes afin d'en empêcher l'accès (attaque par déni de service) commettent un méfait concernant des données. La peine maximale est de 10 ans.

10.7.4 Vol de télécommunication [326(1) C.cr.]

Ce crime vise à contrôler les individus qui « se servent d'installations ou obtiennent un service en matière de télécommunication » de manière « frauduleuse, malicieuse ou sans apparence de droit ». Dans ce cas, le terme « télécommunication » est extrêmement large; il inclut tout signal, qu'il soit envoyé par fil ou par des ondes.

10.7.5 Vol de télécommunication [327(1) C.cr.]

Ce deuxième article sanctionne les individus qui possèdent les outils (tant logiciels que matériels) pouvant servir à effectuer un vol de télécommunication. La portée de la loi est ici aussi très large et inclut même le fait d'entreposer pour autrui du matériel qui permettrait d'intercepter des télécommunications.

Le Canada s'est engagé à combattre la cybercriminalité à l'échelle internationale en signant la Convention européenne sur la cybercriminalité (Conseil de l'Europe, 2001). Ce traité propose un cadre législatif qui restreint encore plus que la législation actuelle les activités sur Internet. Parallèlement à cette dernière phase de changements législatifs, le gouvernement canadien s'est doté d'une stratégie nationale de la cybersécurité en 2010. Son objectif est d'aider les citoyens et le gouvernement à lutter contre les menaces virtuelles. Elle s'articule autour de trois axes :

1. La protection des systèmes gouvernementaux : le gouvernement dispense des services à tous les Canadiens en plus de détenir d'importantes quantités d'informations personnelles. Le gouvernement s'engage à investir les ressources nécessaires afin de sécuriser adéquatement les informations qu'il détient et de garantir un niveau de service satisfaisant.
2. La protection des infrastructures névralgiques : d'autres systèmes en dehors de ceux du gouvernement fédéral sont critiques pour le bon fonctionnement de la nation (gouvernements provinciaux, fournisseurs d'accès Internet, services de télécommunication). Le gouvernement s'engage à nouer des partenariats avec les différents acteurs impliqués pour s'assurer que ceux-ci sont protégés adéquatement.

3. La protection des citoyens : le gouvernement fournit l'information qui permettra à ses citoyens de se défendre contre les menaces venant d'Internet et aide les organismes de lutte au crime afin qu'ils puissent lutter contre les cybermenaces.

Cette politique souligne l'importance des systèmes informatiques pour le gouvernement fédéral et réaffirme que les mesures nécessaires seront prises pour sauvegarder les intérêts nationaux. Cette position ferme face au cybercrime peut être interprétée comme une annonce d'un durcissement prochain de la législation canadienne en ce qui a trait à la criminalité informatique.

10.8 Perspectives d'avenir

Le piratage informatique ne montre aucun signe d'essoufflement; au contraire, la tendance actuelle laisse présager une augmentation de la qualité et de la quantité des attaques. Plusieurs phénomènes expliquent l'expansion de cette forme de criminalité.

Tout d'abord, le profil des individus impliqués dans le piratage tend à changer. Les pirates motivés par la curiosité ou les émotions (vengeance, divergence d'opinions, réputation) sont de plus en plus noyés dans une mer de criminels qui recherchent avant tout des gains monétaires (Evers, 2005). Pour y arriver, ils ciblent les informations confidentielles monnayables comme des numéros de cartes de crédit, des codes d'accès, des secrets corporatifs et des informations personnelles. Comme de telles données se retrouvent autant sur les ordinateurs personnels que sur les serveurs d'entreprises et de gouvernements, les pirates s'attaquent maintenant sans distinction à tous les ordinateurs, peu importe leur localisation ou leur fonction. L'automatisation des outils leur permet de sonder Internet à la recherche de cibles potentielles sans devoir « cogner » activement à toutes les portes : les logiciels de piratage le font pour eux et leur retournent un message si une faille peut être exploitée.

Les dernières années ont aussi été marquées par la montée en puissance de marchés noirs du piratage, où des biens et des services de toutes sortes sont disponibles. Le cas des Wiseguys illustre bien comment des criminels aux capacités techniques limitées peuvent trouver aisément des pirates compétents prêts à bâtir n'importe quel programme sur demande. Ces mercenaires du clavier offrent leurs services de programmeurs, mais

aussi les informations confidentielles qu'ils obtiennent illégalement. Des identités complètes allant de numéros de cartes de crédit aux numéros d'assurance sociale sont vendues en lots, pour quelques dollars la plupart du temps (Richmond, 2010). Le piratage a donc entraîné une modification de l'information personnelle.

Les trois cas pratiques décrits dans la section 10.6 démontrent les gains potentiels que des délinquants professionnels peuvent engranger. Ces gains, bien que souvent financiers, ne sont pas toujours d'ordre matériel, comme dans le cas d'Anonymous. Il faudra s'attendre à ce que le niveau de détermination et de motivation des pirates soit à la hauteur de ces bénéfices. L'exemple d'Anonymous prouve d'ailleurs que l'idéologie est un moteur aussi ou parfois plus puissant que l'argent.

Les attaques seront de plus en plus ciblées et adaptées aux profils des victimes. Les compagnies qui offrent des services de sécurité à plusieurs gouvernements et sous-traitants gouvernementaux sont utilisées comme portes d'entrée dans les systèmes protégés. Le piratage de RSA[3], un fournisseur de clés de vérification d'identification, a permis à des cybercriminels de lancer des attaques de décryptage contre des serveurs du gouvernement américain ainsi que des sous-traitants de la Défense (Bright, 2011c). Ce type d'attaque démontre l'étendue de la patience des pirates et les ressources investies dans chacun des piratages (voir la discussion sur les menaces persistantes et avancées dans la section 10.4).

Les pirates informatiques ne sont pas uniquement embauchés par d'autres criminels désireux de se lancer dans une nouvelle forme de criminalité. De plus en plus de signes indiquent que certains pays cherchent à recruter des pirates pour faire de l'espionnage industriel ou militaire. Les ressources alors mises à la disposition des pirates sont encore plus importantes. L'exemple du ver « Stuxnet » est des plus révélateur du pouvoir du piratage informatique (Byres et coll., 2011). Ce virus informatique a été placé dans des ordinateurs de compagnies reliés au secteur nucléaire iranien. Il s'est propagé à travers des clés USB jusque dans les centrales, où il faisait surchauffer certaines pièces d'équipement afin de les rendre inopérantes. Le virus cachait simultanément les messages d'alerte qui auraient pu prévenir les opérateurs de centrale. Bien que les dégâts aient été limités dans ce cas, cette tendance vers le piratage

3. RSA a été fondé par les inventeurs de la cryptographie à clé publique : Ron Rivest, Adi Shamir et Leonard Adleman (RSA, 2012).

commandité par des États et le piratage d'infrastructures sont deux menaces qu'il ne faudra pas négliger dans les années à venir.

De telles techniques ne sont pas l'apanage d'un seul État. La paternité du ver « Stuxnet » a été attribuée aux Américains ainsi qu'aux Israéliens (Broad et coll., 2011). La Chine a aussi été accusée de mener de telles opérations. Dans un cas en particulier, des entreprises, des États et même le comité olympique ont été attaqués afin d'exfiltrer des informations confidentielles (Bright, 2011b). Devant de tels agissements, Google a décidé de se retirer complètement de la Chine (Anderson, 2010). En raison des incertitudes inhérentes à l'attribution de la responsabilité des attaques informatiques, les jeux politiques et diplomatiques ne manqueront certainement pas d'action au cours des prochaines années.

Les experts en sécurité aiment rappeler qu'ils se doivent de repousser 100 % des attaques pour accomplir leur travail alors que les pirates n'ont qu'à réussir une seule fois pour accomplir le leur. Avec une telle disparité des chances, le piratage informatique se doit d'être une priorité pour les administrateurs d'ordinateurs de milieux tant résidentiels que corporatifs. Aussi désagréable que soit cette réalité, elle ne semble pas près de changer.

Bibliographie

ABADEH, S., HABIBI, J., et LUCAS, C. (2007). « Intrusion Detection Using a Fuzzy Genetics-Based Learning Algorithm », *Journal of Network and Computer Applications*, vol. 30, nº 1, p. 414-428.

ALBANESIUS, C. (2011). « Anonymous Hits Arizona Police A Third Time », *PCMag.com* [En ligne] www.pcmag.com/article2/0,2817,2387980,00.asp (consulté le 3 janvier 2012).

ANDERSON, N. (2010). « Furious Google Throws Down Gauntlet To China Over Censorship », *ars technica* [En ligne] arstechnica.com/tech-policy/news/2010/01/furious-google-throws-down-gauntlet-to-china-over-censorship.ars (consulté le 3 janvier 2012).

AXELSSON, S. (2000). « The Base-Rate Fallacy and the Difficulty of Intrusion Detection », *ACM Transactions on Information and System Security*, vol. 3, nº 3, p. 186-205.

BAILLARGEON-AUDET, K. (2010). *Le piratage informatique : étude de cas d'un réseau de pirates informatiques au Québec*, mémoire de maitrise présenté à l'École de criminologie de l'Université de Montréal.

BELLIA, P. L. (2001). « Chasing Bits Across Borders », *University of Chicago Legal Forum*, p. 35-101.

BRENNER, S. W. (2001). « Cybercrime Investigation and Prosecution : The Role of Penal and Procedural Law », *Murdoch University Electronic Journal of Law*, vol. 8, nº 2.

BRIGHT, P. (2011a). « Anonymous Speaks : The Inside Story of the HBGary Hack », *ars technica* [En ligne] arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/ (consulté le 3 janvier 2012).

BRIGHT, P. (2011b). « Operation Shady RAT : Five-Year Hack Attack Hit 14 Countries », *ars technica* [En ligne] arstechnica.com/security/news/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries.ars (consulté le 3 janvier 2012).

BRIGHT, P. (2011c). « RSA Finally Comes Clean : SecurID Is Compromised », *ars technica* [En ligne] arstechnica.com/security/news/2011/06/rsa-finally-comes-clean-securid-is-compromised.ars (consulté le 14 novembre 2011).

BROAD, W. J., MARKOFF, J., et SANGER, D. E. (2011). « Israeli Test On Worm Called Crucial In Iran Nuclear Delay », *The New York Times* [En ligne] www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3etpagewanted=1ethp (consulté le 3 janvier 2012).

BYRES, E., GINTER, A., et LANGILL, J. (2011). « Stuxnet Report : A System Attack », *Industrial Safety and Security Source* [En ligne] www.isssource.com/stuxnet-report-a-system-attack/ (consulté le 14 novembre 2011).

CONSEIL DE L'EUROPE (2001). « Convention on Cybercrime », *Convention Committee on Cybercrime*, Actes de la convention (Budapest, 23 novembre 2001) [En ligne] conventions.coe.int/Treaty/en/Treaties/html/185.htm (consulté le 14 novembre 2011).

DAVIS, J. T. (2010). *Computer Crime In North Carolina : Assessing The Needs Of Local Law Enforcement*, North Carolina Governor's Crime Commission.

ESTEHGHARI, S., et DESMEDT, Y. (2010). « Exploiting The Client Vulnerabilities In Internet E-Voting Systems : Hacking Helios 2.0 As An Example », *Helios*, sect. 4, p. 0-27.

EVERS, J. (2005). « Hacking For Dollars », *Cnet news.com* [En ligne] broadbandbutler.com/media/filer_public/2011/05/29/hacking_for_dollar.pdf (consulté le 14 novembre 2011).

FAFINSKI, S. (2006). « UK Cybercrime Report », *Garlick* [En ligne] www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf (consulté le 14 novembre 2011).

FLORENCIO, D., et HERLEY, C. (2007). « A Large-Scale Study of Web Password Habits », *Proceedings of the 16th International Conference On World Wide Web* (Banff, Canada).

GHERNAOUTI-HÉLIE, S. (2002). *Internet et sécurité*, Paris, France, Presses universitaires de France.

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

GOLDMAN, E. (2005). « The Challenges of Regulating Warez Trading », *Social Science Computer Review*, vol. 23, nº 1, p. 24-28.

GOODE, S., et CRUISE, S. (2006). « What Motivates Software Crackers? », *Journal Of Business Ethics*, vol. 65, nº 2, p. 173-201.

GORDON, L. A., LOEB, M. P., LUCYSHYN, W., et RICHARDSON, R. (2006). *CSI/FBI Computer Crime And Security Survey* [En ligne] pdf.textfiles.com/security/fbi2006.pdf (consulté le 14 novembre 2011).

GRABOSKY, P. (2000). « Computer Crime : A Criminological Overview », *Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Vienne, 15 avril 2000 [En ligne] pandora.nla.gov.au/nph-wb/20010320130000/www.aic.gov.au/conferences/other/compcrime/computercrime.pdf (consulté le 3 janvier 2012).

GREENISH, P., et RYDER, I. (2011). « Malware And Cyber Crime », Lettre de réponse au House of Commons Science and Technology Select Committee Inquiry on Malware and Cyber Crime.

HADNAGY, C. J., AHARONI, M., et O'GORMAN, J. (2010). « Social Engineering Capture The Flag Results », *Social-Engineer.org* [En ligne] www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf (consulté le 3 janvier 2012).

JONES, J. K., et ROMNEY, G. W. (2004). « Honeynets : An Educational Resource for IT Security », *Proceedings of ACM SIGITE 2004* (Salt Lake City, É.-U.).

JORDAN, T., et TAYLOR, P. (1998). « A Sociology of Hackers », *Sociological Review*, vol. 46, nº 4, p. 757-780.

KIM, B., CHEN, P.-Y. et MUKHOPADHYAY, T. (2009). « An Economic Analysis of the Software Market With a Risk-sharing Mechanism », *International Journal of Electronic Commerce*, vol. 14, nº 2, p. 7-40.

KREBS, B. (2011). « HBGary Federal Hacked By Anonymous », *Krebson Security* [En ligne] krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous (consulté le 3 janvier 2012).

KSHETRI, N. (2005). « Hacking the Odds », *Foreign Policy*, vol. 93 (mai-juin 2005), p. 93.

LEESON, P. T., et COYNE, C. J. (2005). « The Economics of Computer Hacking », *Journal of Law, Economics and Policy*, vol. 1, p. 511-532.

MANN, I. (2010). *Hacking the Human*, Aldershot, R.-U., Gower Publishing Ltd.

MASON, D. (2008). « The Dimensions of Cyber Crime », dans National Center For Justice And The Rule Of Law, *Combating Cyber Crime : Essential Tools And Effective Organizational Structures, A Guide For Policy Makers And Managers*, NCJRL.

MITNICK, K. (2011). *Ghost In The Wires : My Adventures As The World's Most Wanted Hacker*, Londres, R.-U., Little, Brown and Company.

MITNICK, K. D., et SIMON, W. L. (2002). *The Art of Deception*, New York, NY, Wiley.

MITNICK, K. D., et SIMON, W. L. (2005). *The Art of Intrusion*, New York, NY, Wiley.

MOORES, R., et DHILLON, G. (2000). « Software Piracy : A View From Hong Kong », *Communications of the ACM*, vol. 43, nº 12, p. 88.

MURAKAMI, T., KASAHARA, R., et SAITO, T. (2010). « An Implementation And Its Evaluation Of Password Cracking Tool Parallelized On GPGPU », *2010 International Symposium on Communications and Information Technologies*, 26 au 29 octobre, p. 534-538.

NARAYANAN, A., et SHMATIKOV, V. (2005). « Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff », *Proceedings of the 13th ACM Conference on Computer and Communications Security*, p. 364-372.

PERREAULT, S. (2011). « Self-Reported Internet Victimization in Canada, 2009 », *Component of Statistics Canada Catalogue no. 85-002-X*, Statistique Canada.

POULSEN, K. (2011). *Kingpin : How One Hacker Took Over The Billion-Dollar Cybercrime Underground*, New York, NY, Crown Publishings.

PRICEWATERHOUSECOOPERS (2011a). « Cybercrime : Protecting Against the Growing Threat », *www.pwc.com* [En ligne] www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf (consulté le 18 janvier 2013).

PRICEWATERHOUSECOOPERS (2011b). « The Global Economic Crime Survey – Canadian Supplement », *www.pwc.com* [En ligne] www.pwc.com/en_CA/ca/risk/forensic-services/publications/economic-crime-survey-canadian-supplement-2011-en.pdf (consulté le 18 janvier 2013).

RAZVAN, R. (2009). « Over The SQL Injection Hacking Method », *Proceedings of the 3rd International Conference On Communications And Information Technology*, Stevens Point, WI, World Scientific and Engineering Academy and Society, p. 116-118.

REHN, A. (2003). « The Politics Of Contraband : The Honor Economies Of The Warez Scene », *Journal of Socio-Economics*, vol. 33, p. 359-374.

RICHMOND, R. (2010). *Stolen Facebook Accounts For Sale* [En ligne] www.rbhs208.org/IntSafety/Identity%20Theft%20Stories.pdf (consulté le 14 novembre 2011).

RILEY, M., et WALCOTT, J. (2011). « China-Based Hacking of 760 Companies Shows Cyber Cold War », *Bloomberg* [En ligne] www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html (consulté le 14 décembre 2011).

ROGERS, M. K. (1999). « Psychology of Hackers : Steps Toward a New Taxonomy » [En ligne] homes.cerias.purdue.edu/~mkr/hacker.doc (consulté le 14 novembre 2011).

ROGERS, M. K. (2006). « A Two-Dimensional Circumplex Approach To The Development of a Hacker Taxonomy », *Digital Investigation*, vol. 3, nº 2, p. 97-102.

ROJAS, A. (2010). « What Did UFO Hacker Really Find? », *OpenMinds* [En ligne] www.openminds.tv/what-did-ufo-hacker-really-find/ (consulté le 3 janvier 2012).

ROWAN, T. (2009). « Password Protection : The Next Generation », *Network Security*, vol. 2, p. 4-7.

RSA (2012). « RSA History », *RSA Laboratories* [En ligne] www.rsa.com/rsalabs/node.asp?id=2760 (consulté le 2 janvier 2012).

SCHREIER, J. (2011). « PlayStation Network Hack Leaves Credit Card Info at Risk », *Wired* [En ligne] www.wired.com/gamelife/2011/04/playstation-network-hacked (consulté le 14 novembre 2011).

SECURITYFOCUS (2010). « Vulnerabilities », *Symantec Connect* [En ligne] www.securityfocus.com/bid (consulté le 3 janvier 2012).

SHAW, E. D. (2006). « The Role Of Behavioral Research And Profiling In Malicious Cyber Insider Investigations », *Digital Investigation*, vol. 3, p. 20-31.

SOCIAL-ENGINEER (2011). *Social Engineering Framework* [En ligne] www.social-engineer.org/framework/Social_Engineering_Framework (consulté le 14 novembre 2011).

SYMANTEC (2011). « Internet Security Threat Report », *www.symantec.com* [En ligne] www4.symantec.com/mktginfo/ownloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf (consulté le 7 janvier 2013).

THEOCHAROULIS, K., PAPAEFSTATHIOU, I., et MANIFAVAS, C. (2010). « Implementing Rainbow Tables In High-End FPGAs For Super-Fast Password Cracking », *International Conference on Field Programmable Logic and Applications* (Milan, Italie, 31 août au 2 septembre), p. 145-150.

TURGEMAN-GOLDSCHMIDT, O. (2011). « Identity Construction Among Hackers », dans K. Jaishankar, *Cyber Criminology : Exploring Internet Crimes And Criminal Behavior*, Boca Raton, FL, CRC Press.

WATCHGUARD TECHNOLOGIES (2011). « WatchGuard Unveils Top 10 Security Predictions for 2012 », *WatchGuard Technologies* [En ligne] www.watchguard.com/news/press-releases/watchguard-unveils-top-10-security-predictions-for-2012.asp (consulté le 1er octobre 2012).

WATTERS, A. (2010). « DDoS Attacks Take Down Mastercard and Visa Websites, "Payback" For Their Stance on Wikileaks », *ReadWriteWeb* [En ligne] www.readwriteweb.com/archives/ddos_attacks_take_down_mastercard_and_visa_website.php (consulté le 3 janvier 2012).

WHEELER, D. A., et LARSEN, G. N. (2003). *Techniques for Cyber Attack Attribution*, Alexandria, VA, Institute for Defense Analyses, 82 p.

WHITTAKER, Z. (2011). « Anonymous Hack San Francisco Subway Website; Mass User Data Leaked », *ZDNet* [En ligne] www.zdnet.com/blog/btl/anonymous-hack-san-francisco-subway-website-mass-user-data-leaked/54944 (consulté le 3 janvier 2012).

WINDER, D. (2011). « Who Are TeamPoison And What Is Operation Robin Hood? », *Daniweb* [En ligne] www.daniweb.com/community-center/geeks-lounge/news/398497 (consulté le 14 décembre 2011).

WINKLER, I. S., et DEALY, B. (1995). « Information Security Technology? Don't Rely On It – A Case Study in Social Engineering », *Proceedings of the Fifth USENIX UNIX Security Symposium* (Salt Lake City, É.-U.).

WOOD, K., et PEREIRA, E. (2011). « Impact of Misconfiguration in Cloud – Investigation Into Security Challenges », *International Journal Multimedia and Image Processing*, vol. 1, nº 1, p. 17-25.

WORKMAN, M. (2008). « Wisecrackers : A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Theats to Information Security », *Journal of the American Society For Information Science And Technology*, vol. 59, nº 4, p. 662-674.

WRIGHT, C. S., et ZIA, T. A. (2010). « The Economics Of Developing Security Embedded Software », *Proceedings of the 8th Australian Information Security Management Conference* (Perth, Australie, 30 novembre au 2 décembre).

YAR, M. (2005). « Computer Hacking : Just Another Case Of Juvenile delinquency? «, *Howard Journal of Criminal Justice*, vol. 44, nº 4, p. 387-399.

YAZDI, S. H. (2011). *Analyzing Password Strength and Efficient Password Cracking*, Mémoire de maîtrise, College of Arts and Sciences, Florida State University.

ZETTER, K. (2010). « Wiseguys Indicted In $25 Million Online Ticket Ring », *Wired* [En ligne] www.wired.com/threatlevel/2010/03/wiseguys-indicted (consulté le 14 novembre 2011).

ZETTER, K. (2011). « Four Romanians Indicted For Hacking Subway, Other Retailers », *Wired* [En ligne] www.wired.com/threatlevel/2011/12/romanians-subway-hack (consulté le 14 décembre 2011).