Université de Montréal

Le capital virtuel
Entre compétition, survie et réputation

Par
David Décary-Hétu

École de criminologie
Faculté des Arts et des Sciences

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de Ph.D.
en criminologie

RÉSUMÉ

Les avancées technologiques liées à l'internet ont permis une démocratisation des outils de communication et une transformation des relations interpersonnelles. L'impact de ces changements s'est ressenti autant dans la sphère légitime que dans les marchés criminels. Ces derniers ont migré, au cours des dernières années, vers des plateformes en ligne qui leur permettent de mieux gérer les risques associés avec leurs activités illégales.

Cette thèse s'intéresse à l'impact de l'internet sur la criminalité et sur l'adaptation des criminels à cet environnement virtuel. Ces derniers forment maintenant des communautés en ligne et gardent le contact entre eux à l'aide de salles de clavardage et de forums de discussions. Nous nous intéresserons dans cette thèse à trois formes particulières de crime soit la fraude de propriété intellectuelle (*la scène des warez*), le piratage d'ordinateurs (*les botnets*) ainsi que la fraude de données personnelles et financières (*le carding*). Chacune de ces formes de crime sera analysée à l'aide d'un article publié ou présentement en évaluation.

L'article sur la scène des warez décrit l'organisation sociale ainsi que la distribution de la reconnaissance dans la communauté des pirates informatiques. Les systèmes de délinquance (Sutherland, 1947) et l'individualisme réseauté (Boase & Wellman, 2006) sont utilisés pour théoriser l'organisation sociale et la distribution de la reconnaissance dans la scène warez. L'article sur les botnets tente de comprendre la distribution de la réputation dans une communauté de criminels. En utilisant les données d'un forum de discussion où des botmasters louent et achètent des biens et services illégaux, cette recherche modélise les facteurs qui permettent d'augmenter le niveau de réputation de certains acteurs. Finalement l'article sur le carding mesure le lien entre la réputation telle que développée par Glückler & Armbrüster (2003) et la performance criminelle.

Notre thèse démontre que l'internet a eu un effet transformateur sur la criminalité à six niveaux : 1) l'augmentation de la facilité à trouver des co-criminels; 2) l'augmentation de la compétition entre les criminels; 3) l'augmentation du nombre de victimes; 4) la diminution des risques d'arrestation; 5) l'augmentation du taux de réussite des criminels et; 6) les changements dans l'équilibre entre criminels, victimes et protecteurs. Elle nous permet

également de démontrer l'importance de la réputation, le capital virtuel, dans les marchés criminels en ligne.

Mots clés : réputation, capital virtuel, réussite criminelle, réseaux sociaux, marchés criminels, Internet

ABSTRACT

Technological advances related to the Internet have led to a democratization of the tools of communication and transformation of interpersonal relationships. The impact of these changes is felt both in the legitimate sphere as well as in criminal markets. These markets have migrated in recent years to online platforms that allow them to better manage the risks associated with their illegal activities.

This thesis focuses on the impact of the Internet on crime and criminal adaptation in this virtual environment. These individuals now form online communities and keep in touch with each other using chat rooms and forums. We focus in this thesis on three specific forms of crime: intellectual property fraud (*the warez scene*), the hacking of computers (*botnets*) and fraud of personal and financial data (*carding*). Each of these forms of crime will be analyzed in an article that has either been published or is currently under review.

The article on the warez scene describes the social organization and the distribution of recognition in the hacker community. Crime behavior system (Sutherland, 1947) and networked individualism (Boase & Wellman, 2006) are used to theorize social organization and distribution of recognition in the warez scene. The article on botnets aims to understand the distribution of reputation in this community for offenders. Using data from a forum where botmasters rent and buy illegal goods and services, this research models the factors that increase the level of reputation of some actors. Finally the article on carding measures the link between reputation as developed by Glückler & Armbruster (2003) and criminal performance.

Our thesis demonstrates that the Internet has had a transformative effect on crime at six levels: 1) increase of the ease of finding co-offenders; 2) increased competition between offenders; 3) increase in the number of victims; 4) decrease in the risk of arrest; 5) increasing the success rate of criminals and; 6) changes in the balance between offenders, victims and protecteurs. It also allows us to demonstrate the importance of reputation, the virtual capital, on online market criminals.

Keywords : reputation, criminal achievement, social networks, criminal markets, Internet

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

What about being poor as a stand?
What about being proud of being phracked?
I don't like what's pretty, I like what's real.
What about finding beauty where it's not supposed to be?

Surprise me with stories and songs
I haven't heard a million times before…..

Confessions Of A Revolutionary Bourgeois, Part 3
THE SAINTE-CATHERINES

REMERCIEMENTS

Comme bien des décisions dans ma vie, celle de m'inscrire au doctorat a été prise assez rapidement et sans pleinement en évaluer les conséquences. Je suis encore étonné de constater la vitesse à laquelle ces trois années et quarts sont passées. Malgré quelques périodes plus intenses, mes études de doctorat ont été une suite ininterrompue de plaisir, de stimulation intellectuelle et de rencontres passionnantes. Pour tout cela, je me dois de remercier quelques personnes en particulier.

Carlo, ce projet n'aurait jamais commencé sans toi. Notre collaboration a commencé un peu frénétiquement avec une corrélation sur le coin de ton bureau qui t'avait mis en retard pour donner ton cours. Ta passion pour la vie et la criminologie est contagieuse et j'aspire un jour à être la moitié du mentor que tu as été pour moi. Merci pour ta patience sans borne et ta générosité. La compétition annuelle de pétanque perd maintenant ses *undefeated champions*...

Stéphane, le héros obscur de cette thèse et de mes études. Tu as été celui qui m'a donné ma première chance et qui m'a donné la piqûre pour les conférences. J'ai beaucoup appris de ta rigueur et de ta capacité à tout remettre en question. Maintenant que la thèse est terminée, j'espère qu'il n'est pas trop tard pour faire cette conférence à Québec!

Benoit, je ne me rappelle plus quelle mouche m'a piqué pour que j'aille m'asseoir dans ton bureau pour te proposer de travailler ensemble sur je ne sais plus quelle folie du moment. C'était le début d'une relation qui n'en est, je l'espère, qu'à ses débuts. Tes conseils ont été incroyablement précieux, surtout au cours des derniers mois. Tu m'as offert des opportunités qui m'ont permis de me réaliser en tant que chercheur et personne comme jamais je l'aurais imaginé. Je t'en serai éternellement reconnaissant.

Yanick, mon *partner in crime*. Nous aurons fait bien des folies *gigantico* ensemble au cours des dernières années. Tu as été celui qui a réussi à me ramener sur Terre. Tu occupes une place bien spéciale dans notre école et ce fut un honneur de partager ces années avec toi. Nos chemins semblent vouloir se séparer pour le moment, mais je suis convaincu que ce n'est que temporaire.

Chloé, je suis heureux d'avoir réussi à te convaincre que les premières impressions ne sont pas toujours les meilleures. Merci pour la plante porte-bonheur, ton écoute et la couleur que tu as mises entre nos quatre murs ternes. Tu es de celles qui ont tout pour réussir, peu importe l'entreprise dans laquelle ils se lancent.

Je ne serais sûrement pas en train d'écrire ces lignes si je n'avais pas eu les parents que j'ai. Ils m'ont appris ce qu'était la définition de l'amour inconditionnel et sont les meilleurs modèles qu'un fils puisse espérer. Maintenant que votre retraite est arrivée et que mes études sont derrière moi, j'espère vivement que nous pourrons rattraper tout le temps perdu.

Audrey, le calme dans ma tempête. J'ai toujours eu l'impression que mes rencontres arrivaient toujours au mauvais moment. Avec toi, cela a changé et j'ai finalement l'impression d'être au bon endroit au bon moment. Merci de m'aimer avec tous mes défauts et les folies qui me passent par la tête. Tu m'as démontré ton amour pour moi au cours des derniers mois. J'ai pris note de chacune de tes attentions et sache qu'elles te seront rendues au centuple maintenant que je suis un homme libre!

Catherine, nos vies ont pris des chemins divergents depuis les deux dernières années. Tu as acquis la maturité et le sens des responsabilités que je ne sais toujours pas si je serai en mesure d'avoir un jour. Tu m'as tout appris de la vie et sache que malgré la distance, tu n'es jamais loin dans mes pensées.

Finalement, j'aimerais terminer ces remerciements avec un mot pour Pierre Tremblay. Pierre, je ne sais si un jour ton intellect puissant, mais déstabilisant, sera reconnu à sa juste valeur. D'ici là, sache que je suis une autre de ces personnes dont on entend parler et qui a été transformée par ton contact. Tu nous as appris à ne jamais faire de compromis et à toujours foncer tête baissée. Pour le meilleur et pour le pire, j'entends bien poursuivre sur ta lancée et contribuer à ma façon à cette sociologie criminelle qui t'anime et te consume.

INTRODUCTION

À l'image de bien des thèses, celle que vous vous apprêtez à lire a connu un développement des plus sinueux. Tout a débuté avec un travail de session en méthodologie quantitative au niveau de la maîtrise. Comme nous devions nous-mêmes trouver une base de données pour le réaliser, nous nous sommes lancés à la recherche de données sur les pirates informatiques. Sans grandes connaissances sur le domaine, nous avons avancé à tâtons pour finalement découvrir ce qui allait être notre porte d'entrée sur le monde fascinant de la fraude de propriété intellectuelle en ligne, la scène des warez.

Plusieurs se sont montrés sceptiques quant à la pertinence d'étudier ce type de criminalité. Télécharger des fichiers contenant de la propriété intellectuelle sans payer n'était et n'est en effet toujours pas un crime au Canada. De plus, contourner les mesures de protection contre les copies illégales se situait et se situe aussi dans une zone grise juridique. L'utilité de cibler ce genre de comportement criminel était donc encore à démontrer. Plutôt que de réorienter nos recherches, nous sommes allés au devant d'experts en mesure de résoudre ces problèmes de pertinence et d'opérationnalisation. Cette persévérance nous a permis de non seulement remporter le premier prix du Colloque de méthodologie quantitative de l'École de criminologie de l'Université de Montréal, mais aussi de faire un passage accéléré au doctorat.

L'objectif de ce passage accéléré était de bâtir autour des données collectées sur la scène des warez une étude qui explorerait l'impact de l'internet sur une forme particulière de déviance. Le milieu des warez semblait particulièrement propice à ce genre d'étude étant donné qu'il s'agissait d'une déviance qui existait déjà avant la popularisation d'internet. Comme nous disposions déjà de près de quarante numéros de journaux rédigés par et pour les pirates informatiques de la scène des pirates durant les années 1990, nous aurions alors pu comparer ces journaux aux données plus récentes (2003-2009) afin de comprendre les transformations qui s'étaient opérées avec le temps.

Jusqu'à récemment, cette stratégie nous semblait être en mesure de tenir la route. C'était sans compter sur le hasard et les aléas de la recherche. Lors de nos premières

recherches sur la scène des warez, nous avons été marqués par l'importance de la réputation émanant des pairs chez les pirates. Cette dernière était en effet la source principale de motivation et les pirates étaient prêts à risquer leur liberté et prendre d'énormes risques simplement pour se faire un nom dans une communauté de criminels. L'aspect financier était donc ici totalement évacué de la scène où il est en effet très mal vu de recevoir toute rémunération en argent pour des raisons idéologiques qui remontent aux principes défendus par les premiers pirates qui tenaient à ce que toute information soit libre d'accès à tous. Parallèlement à nos recherches sur la scène des warez, nous avons aussi commencé, au cours des derniers mois, à nous intéresser à la transition des marchés illicites vers le monde virtuel, cet univers offrant une plateforme de plus en plus prisée pour la vente de biens et services illégaux. Un site de vente comme *SilkRoad* par exemple offre plusieurs milliers d'échantillons de drogue qui peuvent être envoyés par la poste dans la plupart des pays du monde. En étudiant ces marchés illicites en ligne, nos premières recherches sur la réputation nous sont revenues en tête et nous avons été frappés par l'importance de la réputation pour comprendre le phénomène de la déviance en ligne.

Ces marchés sont en effet des milieux extrêmement risqués où la confiance est un luxe que peu d'individus peuvent se permettre. Une bonne réputation devient dans ce contexte une ressource qui peut être fort utile pour réduire les asymétries d'informations et augmenter les opportunités criminelles. Des systèmes automatisés de reconnaissance tels que ceux utilisés sur des sites marchands comme eBay ou Amazon ont été empruntés et adaptés par les marchés illicites et les criminels consacrent beaucoup d'énergie à maintenir et développer leur réputation en ligne.

Marqués par l'importance que les criminels portaient eux-mêmes au concept de réputation, nous avons décidé de recentrer cette thèse sur ce thème et de tenter d'en comprendre les sources et les impacts. Afin d'être aussi représentatifs que possible, nous avons analysé trois formes particulières de déviance en ligne qui seront présentées dans les prochaines sections. Les parallèles que nous tracerons dans le dernier chapitre de cette thèse nous permettront de dégager certaines tendances qui devront être explorées plus à fond dans les publications futures de notre programme de recherche.

Le premier chapitre se concentre sur les formes particulières de cybercrimes qui seront abordés dans cette thèse. Nous commencerons avec la scène des warez, la communauté de pirates informatiques qui se spécialisent dans la fraude de propriété intellectuelle en ligne. Alors qu'une telle fraude semble être commune à des millions de consommateurs peu scrupuleux, il s'agit dans la majorité des cas du résultat de la déviance de milliers d'individus qui sont en compétition pour obtenir le plus de reconnaissance possible de leurs pairs. Nous poursuivrons avec les botnets, ces réseaux de plusieurs milliers d'ordinateurs infectés, voire même de millions, qui sont contrôlés à distance par des criminels. Nous terminerons ce chapitre avec une revue des cardeurs, les individus impliqués dans la fraude de données personnelles et financières.

Le deuxième chapitre nous permettra de présenter aux lecteurs moins familiers avec les nouvelles technologies et la cybercriminalité une série de définitions sur les concepts au cœur de cette recherche. Cela inclut la notion même de cybercrime et leurs auteurs, les pirates informatiques. Nous passerons ensuite en revue l'environnement dans lequel ces derniers évoluent et les moyens qu'ils utilisent pour communiquer ensemble. Nous verrons aussi comment l'internet a transformé les relations entre les cybercriminels en raison de l'individualisme réseauté (Boase & Wellman, 2006).

Le troisième chapitre représente le cœur théorique de cette thèse et développera notre conception de la réputation. Nous verrons que ce concept peut et devrait être étudié comme une ressource. Celle-ci a des coûts et des bénéfices qui lui sont associés. Les personnes arrivant à manœuvrer le plus habilement seront le plus à même de récolter plus d'avantages que les autres. La majorité de la littérature passée en revue est tirée du domaine des affaires et du marketing. Nous terminerons quand même le chapitre avec une revue de la réputation dans le contexte criminel, un champ de recherche qui commence à peine à se développer suite à l'apparition de nombreux marchés illicites.

Le quatrième chapitre nous permettra d'expliquer en détail la méthodologie utilisée pour mieux comprendre et analyser la réputation dans le contexte de la cybercriminalité. Cette thèse par articles compte trois articles et la méthodologie de chacun de ces articles est passée en revue dans ce chapitre. Nous verrons qu'une méthodologie variée et pertinente (corrélation,

analyse multiniveaux, analyse de survie, analyse de réseaux sociaux) a été utilisée lorsque nécessaire.

Les chapitres cinq, six et sept sont les articles de notre thèse. Le premier a été publié en 2012 dans le *Journal Of Research On Crime & Delinquency*. Il décrit l'organisation sociale ainsi que la distribution de la reconnaissance dans la communauté des pirates informatiques responsables d'une bonne partie de la fraude de propriété intellectuelle sur internet. Les produits (films, jeux, livres, logiciels) qui y sont illégalement échangés portent le nom de *warez*, un diminutif du mot *software* (logiciel en anglais). Cette communauté est aussi connue sous le nom de *scène des warez*. Ses participants sont regroupés en clans qui s'affrontent dans un tournoi perpétuel afin d'obtenir le plus de reconnaissance possible de leurs pairs. Les données de l'étude ont été recueillies à partir d'un index en ligne qui conserve une liste du contenu illicite qui a été illégalement distribué entre 2003 et 2009. Les systèmes de délinquance (Sutherland, 1947) et l'individualisme réseauté (Boase & Wellman, 2006) sont utilisés pour théoriser l'organisation sociale et la distribution de la reconnaissance dans la scène warez. Dans cette thèse, la reconnaissance analysée sera le signal qu'une entité envoie à une autre afin de contribuer à son niveau de réputation. La réputation sera donc le total des signaux reçus et fait référence à l'image publique d'un individu sur la place publique.

Le deuxième article a été accepté dans un numéro spécial de la revue *Global Crime*. Celui-ci s'intéressait à la communauté des botnets et tentait de comprendre la distribution de la réputation dans une communauté de criminels. Les botnets sont des réseaux d'ordinateurs infectés par des virus et qui tombent sous le contrôle de criminels aussi connus sous le nom de *botmasters* ou *bot herders*. Toutes les fonctions d'un système informatique infecté deviennent accessibles au botmaster qui peut alors l'utiliser pour épier ses utilisateurs, envoyer du pourriel ou encore infecter d'autres machines. En utilisant les données d'un forum de discussion où des botmasters louent et achètent des biens et services illégaux, cette recherche modélise les facteurs qui permettent d'augmenter le niveau de réputation de certains acteurs.

Le troisième et dernier article a finalement comme objectif de mesurer le lien entre la réputation telle que développée par Glückler & Armbrüster (2003) et la performance criminelle. Des données issues d'un forum de discussion où des cardeurs achètent et vendent

des numéros de carte de crédit nous permettent de modéliser l'impact de la réputation publique, de l'expérience basée sur la réputation et de l'expérience réseautée sur la cadence des transactions illicites. Les cardeurs sont les criminels qui se spécialisent dans la fraude de données personnelles et financières, surtout les numéros de cartes de débit et de crédit. Il existe une forte division du travail parmi ces criminels et les individus qui arrivent à obtenir illégalement les informations sont rarement les mêmes qui les utilisent pour frauder. Des marchés virtuels sont plutôt utilisés pour que chaque spécialiste puisse vendre le fruit de ses crimes et se procurer les intrants nécessaires à leur commission. Ceci est donc une étude d'un marché noir où des individus vendent et achètent des informations personnelles et financières.

La thèse se termine avec une conclusion qui fera la synthèse des connaissances acquises dans les trois chapitres et qui situera nos résultats dans le contexte de la recherche sur l'internet, l'individualisme réseauté et la réputation criminelle.

L'étude du problème de la réputation criminelle s'inscrit dans un courant de recherche bien défini en criminologie, celui de la carrière criminelle. Au-delà de la simple relation âge/crime bien connue en criminologie (Farrington, 1986), plusieurs chercheurs se sont intéressés aux facteurs qui amènent certains individus à s'engager dans une carrière criminelle et aussi à s'y maintenir. Le problème du développement d'un mode de vie criminel a été étudié à l'aide l'association différentielle (Sutherland, 1947), de l'anomie (Merton, 1938) et de la théorie de l'étiquetage (Becker, 1963). Cette courte liste n'est évidemment qu'un fragment des explications possibles qui poussent certains individus à se tourner vers le crime. Elles font elles aussi néanmoins partie des études sur les carrières criminelles. Notre thèse s'intéresse davantage à la deuxième portion de ce type de recherche et rejoint plutôt une partie du projet de recherche de Sutherland et de la sociologie criminelle américaine (Sutherland, 1947). Notre premier article sur la scène des warez décrit plus en détail le concept de systèmes de délinquance et tend à démontrer les mécanismes que les criminels mettent en place pour maximiser leurs profits et diminuer au maximum leurs risques. Ce faisant, ils s'assurent d'une longévité accrue. Sutherland (1947) est d'avis que des facteurs systémiques sont responsables en partie de la création de marchés illicites qui perdurent dans le temps. Ce dernier mentionne que le sentiment d'appartenance, le réseautage et l'apprentissage de techniques sont essentiels au maintien d'une vie criminelle active.

Sutherland (1947) a été malheureusement quelque peu délaissé au cours des dernières. Les chercheurs se sont plutôt attelés à la création d'outils permettant de prédire la récidive (Tremblay, 2011). Ceux-ci s'intéressent autant aux facteurs dynamiques comme les problèmes de personnalité et les besoins criminogènes (Gendreau et al., 1996) qu'aux facteurs statiques comme les antécédents criminels et l'ethnicité (Gendreau et al., 1996). Étonnamment, les études portant sur le sujet ne se sont jamais intéressées à l'impact que pouvait avoir le succès d'un criminel sur la poursuite d'une carrière criminelle. Il serait pourtant tout à fait logique de poser l'hypothèse que les criminels qui possèdent une réputation supérieure et qui performent mieux dans le crime seraient plus enclins à continuer leur carrière que les autres. Ceux-ci seraient par ailleurs plus aptes à commettre davantage de crimes et aussi de servir de modèles pour des criminels débutants qui chercheraient un mentor pouvant leur enseigner les rudiments du métier ainsi que leur fournir une introduction auprès des personnes clés du milieu. La réputation criminelle semble donc être un autre morceau de l'explication du pourquoi de la poursuite d'une carrière criminelle. Nous espérons démontrer avec cette thèse qu'il est possible de pousser encore plus loin notre compréhension du phénomène et que la réputation est la clé du succès de cette quête.

Si nous avons choisi de nous intéresser à des cybercrimes pour démontrer cette thèse, c'est en raison des transformations dans la structure et dans l'actualisation de la criminalité qui sont survenues suite à l'adoption en masse de l'internet. Plusieurs formes de criminalité ne peuvent, aujourd'hui, être analysées sans tenir compte de leurs composantes virtuelles. C'est le cas entre autres de la fraude de propriété intellectuelle. Bien qu'il existe un vaste marché pour les films contrefaits notamment en Asie, l'accessibilité jour et nuit et partout dans le monde à des versions téléchargeables des derniers succès d'Hollywood est venue bouleverser ce type de fraude. Il en va de même pour la fraude des données financières qui peuvent aujourd'hui être vendues et achetées dans l'anonymat relatif des marchés virtuels. Dans ce contexte, le point sous-jacent à toutes nos discussions sera que l'internet est un développement technologique qui a davantage transformé la criminalité que créé de nouvelles formes particulières de crime. Ce faisant, les interactions entre criminels, victimes et l'environnement ont été profondément changées; cette thèse nous permettra d'en mesurer et d'en comprendre toute l'étendue.

CHAPITRE 1 – LA CYBERCRIMINALITÉ

L'idée voulant que la cybercriminalité soit une forme de crime ayant des caractéristique qui lui sont propres est encore contestée de nos jours (McGuire, 2007). Nous verrons dans ce chapitre comment les nouvelles technologies ont évolué au cours des quarante dernières années et l'impact que ces changements ont eu sur le développement de la criminalité en ligne. Nous choisirons donc et présenterons des définitions pour les concepts majeurs de cette thèse incluant le terme de pirate informatique. Nous nous intéresserons particulièrement aux moyens de communication et à l'organisation sociale des criminels virtuels. Ce chapitre portera par ailleurs sur la notion d'individualisme réseauté (Boase & Wellman, 2006). Ce cadre théorique nous permettra de comprendre comme les relations ont été transformées à l'ère de l'internet et l'impact que cela a pu avoir sur les criminels. Cette théorie, d'abord développée pour rendre compte d'activités légitimes, s'applique aussi parfaitement au monde illégitime. Ce chapitre nous permettra donc de faire le pont entre les formes particulières que nous avons vu dans le premier chapitre et le concept de réputation qui suivra dans le troisième chapitre.

1.1 L'informatique, d'hier à aujourd'hui

L'informatique moderne a vécu trois phases distinctes au cours des cinquante dernières années (Campbell-Kelly, 2009). La première phase, que l'on pourrait qualifier de phase de l'unité centrale, s'étire du début du siècle et se termine au début des années 1980. À l'époque, les propriétaires d'ordinateurs se faisaient rares en raison des coûts d'achat, d'entretien et de main-d'œuvre ainsi que de la taille des machines. Il était presque impensable pour un individu ou même une entreprise de posséder un ordinateur. Ceux-ci envoyaient plutôt les données à analyser (ex. : des feuilles de temps de travail) par camion et recevaient par la suite les résultats des analyses (ex. : une liste des employés et le montant de paye dû). Avec l'arrivée des connexions par ligne téléphonique, les utilisateurs de tels services ont pu envoyer directement leurs données au serveur et recevoir les analyses de façon électronique. Bien qu'excessivement lente, cette façon de procéder permettait d'économiser en ne payant que pour le temps d'utilisation de l'ordinateur. Malgré ces économies, l'utilisation d'un ordinateur demeurait à cette époque un luxe que peu de personnes et d'entités morales pouvaient aisément se payer.

La deuxième phase, celle de l'ordinateur personnel, a débuté aux alentours de 1983-1984 avec l'apparition d'ordinateurs personnels puissants, abordables et relativement faciles d'utilisation. Ils permettaient de remplir les mêmes tâches que les unités centrales d'antan, mais sans avoir à attendre le retour des analyses par ligne téléphonique. Bien que toujours dispendieux, il devenait plus économique d'acheter un ordinateur que de louer du temps d'utilisation sur une unité centrale pendant une année. Les machines étaient donc des appareils qui ne remplissaient qu'un nombre limité de fonctions à l'image d'une télévision aujourd'hui qui ne réponde qu'à un seul besoin. Les vingt années qui ont suivis ont étonnement vu peu de changements à l'exception de l'arrivée de l'internet. Il a fallu plusieurs années avant qu'un accès haute vitesse devienne abordable et qu'une bonne partie de la population puisse s'en prévaloir. Ce changement était nécessaire pour réaliser la phase suivante.

La troisième et dernière phase en est encore à ses balbutiements, mais prend de plus en plus d'importance. Il s'agit de la phase de l'informatique dans les nuages. Il s'agit en quelque sorte d'un retour à la phase de l'unité centrale, mais dans une version revue et améliorée. Au cours des vingt dernières années, bien que le coût d'achat initial d'un ordinateur ait diminué, les frais d'exploitation ont nettement augmenté. Les utilisateurs désirent faire davantage avec leurs ordinateurs et doivent se procurer toute une série de logiciels pour répondre à leurs besoins. Même si certains d'entre eux sont gratuits, des incontournables comme les suites de bureautique coûtent encore dans les centaines de dollars. Cette évolution de la complexité des ordinateurs entraîne aussi une hausse du nombre d'heures dévouées à la gestion des appareils. La plupart des maisons possèdent plusieurs appareils branchés sur une même connexion et les utilisateurs doivent donc se transformer en experts en réseautage et en sécurité. La plupart des individus ne sont évidemment pas équipés pour remplir de telles tâches et embrassent maintenant l'informatique dans les nuages. Il s'agit en quelque sorte du même procédé que dans le temps de l'unité centrale. Une compagnie offre un logiciel et les utilisateurs s'y connectent à l'aide d'un fureteur web. Toutes les données, les copies de sauvegardes et les mises à jour du logiciel sont sous la responsabilité de la compagnie qui facture un montant chaque mois pour son travail. Les utilisateurs achètent en quelque sorte la tranquillité d'esprit. L'arrivée toute récente d'un ordinateur portable de Google (CR-48) vient montrer la force de

cette tendance (Google, 2010). Cette machine ne peut être utilisée que si elle est connectée à l'internet, ne disposant pas de disque dur pour enregistrer des données ou des logiciels.

Si l'informatique dans les nuages fait un retour en force dans une version revue et améliorée des systèmes centralisés de la première phase, c'est aussi en raison de la prévalence de l'internet. Les individus sont de plus en plus connectés tant à la maison que dans les cafés que sur leurs cellulaires (Google, 2011). L'application commerciale de l'internet date de la première moitié des années 1990, mais c'est avec la popularité de fournisseurs comme AOL qu'il a vraiment pris son envol (Mowery et al., 2002). L'internet s'est imposé très rapidement comme un moteur d'échange, de communication et d'informations très riches. Ne pouvant offrir que du texte sans possibilités d'interactions, la toile mondiale a régulièrement reçu des mises à jour qui lui ont permis de diffuser des images, du son, des vidéos et finalement d'interagir avec les utilisateurs à l'aide de formulaires. Aujourd'hui, l'internet est surtout utilisé pour faire des recherches d'informations, consulter des vidéos et participer à des réseaux sociaux. Avec le nombre de portes d'accès qui ne cesse d'augmenter (ordinateur, portable, cellulaire, console de jeux, lecteur MP3, télévision, automobile), l'internet ne peut que prendre que de plus en plus de place dans le quotidien de tous les individus.

La tendance actuelle est donc à l'intégration de l'internet dans nos activités de tous les jours. Cette démocratisation des technologies est en grande partie possible grâce à la facilité d'utilisation des services dans les nuages qui réduisent les coûts des ressources nécessaires à leur adoption. Nous verrons dans cette thèse que les criminels tirent eux aussi de plus en plus avantage des avancées technologiques et des plateformes en ligne pour commettre des crimes et optimiser leurs opérations. Des forums de discussions aux services de location de logiciels, les criminels sont maintenant très au fait des possibilités de l'informatique dans les nuages. Leur créativité et leur sens de l'innovation seront au cœur de nos analyses et nous serons à même de constater à quel point les sphères licites et illicites se rejoignent dans l'univers virtuel.

1.2 Pirate informatique : une définition

Les personnes qui commettent des cybercrimes aujourd'hui sont connues sous le nom de pirates informatiques. Traduite du terme anglais *hacker*, cette expression englobe une vaste

tranche d'internautes aux multiples comportements et motivations. Dans son sens original, le terme se rapporte aux ingénieurs universitaires des années 60 et 70 qui tentaient de repousser les limites des technologies informatiques de l'époque (Alleyne, 2010). Ceux-ci étaient encore à l'étape de l'exploration des sciences informatiques et ils n'hésitaient pas à briser certaines règles afin d'obtenir plus d'accès aux équipements ou encore afin d'augmenter les capacités des systèmes de l'époque. Ces ingénieurs étaient donc dénoués de toute malice et n'étaient motivés que par leur curiosité et leur amour de la technologie. Le développement de l'informatique personnel et surtout des ordinateurs en réseaux a ouvert un nouveau terrain de jeu aux enthousiastes dépassant ainsi le cadre limité des ingénieurs et étudiants d'université.

La génération suivante de pirates s'est davantage fait remarquer pour ses erreurs que pour ses réussites. Le résultat de leurs expériences ratées a eu des conséquences désastreuses comme le ver informatique rédigé par Robert Morris Jr qui, en quelques heures, a réussi à ralentir le trafic internet mondial (Chen & Robert, 2004). Ce projet avait pour objectif de tester la réplication de code informatique sur des réseaux et n'était pas destiné à nuire à qui que ce soit; son auteur cherchait plutôt à satisfaire sa curiosité juvénile. Les pirates en étaient donc encore à l'étape de l'expérimentation, mais leur laboratoire était maintenant l'internet plutôt que leur réseau universitaire.

Cette phase exploratoire n'a duré que quelques années entre le milieu des années 80 et le début des années 90. C'est à ce moment que les pirates se sont graduellement scindés en deux groupes divergents : les pirates blancs et les pirates noirs (Crandall et al., 2005). Les deux groupes sont très similaires; ils s'attaquent aux systèmes informatiques, créent des virus et des logiciels d'intrusion d'ordinateurs et manipulent les administrateurs de réseaux. La grande différence entre ces deux clans vient de la légitimité des pirates blancs (Kleinknecht, 2003). Ceux-ci sont embauchés par les compagnies pour tester les limites de leurs défenses ou pour étudier les nouveaux vecteurs d'attaques. Ils sont donc des pirates informatiques payés salariés. Les pirates noirs, pour leur part, n'ont pas l'autorisation de s'attaquer aux réseaux privés et le font pour une multitude de raisons : vengeance, profit personnel, reconnaissance (Saleem, 2006). Plusieurs pirates blancs affirment avoir été tentés par le côté noir du piratage pour ensuite traverser du côté légitime.

Il existe encore à ce jour beaucoup de confusion sur la définition du terme pirate informatique. Cette simple différence de légitimité peut sembler mince pour certains. En effet, si un pirate blanc crée un programme qui permet d'accéder à un réseau, il s'agira d'un logiciel de sécurité. Si un pirate noir produit l'équivalent, il s'agira alors d'un logiciel malveillant. Cette différence dans la légitimité nous semble par contre fondamentale, particulièrement en criminologie. Plusieurs recherches ne tiennent pas compte de cette séparation (Schell et al., 2002; Holt, 2008) et les impacts sur les résultats sont majeurs. Ils mélangent en effet des individus au code éthique et aux valeurs qui sont peu compatibles.

Pour les besoins de cette thèse, nous nous concentrerons uniquement sur les pirates noirs, communément appelés pirates informatiques ou cybercriminels. Il est de notre avis que ceux-ci, de par la nature de leur activité, se différencient significativement des pirates blancs et qu'il serait incompatible de tenter d'étudier le phénomène chez ces deux populations simultanément. Notre définition formelle d'un pirate noir sera celle de Wilhelm (2009) qui le présente comme un «individu qui s'attaque sans autorisation à un système d'information» (Wilhelm, 2009 : p15). Les pirates de la scène des warez semblent à première vue ne pas faire partie de cette catégorie. Ils doivent cependant régulièrement pirater des systèmes informatiques pour trouver de nouveaux produits à distribuer et doivent par ailleurs retirer les protections anticopie à l'aide de techniques de piratage. Ces actes les classent donc définitivement dans la catégorie des pirates noirs.

1.3 Les communautés de pirates informatiques

Les pirates informatiques ne peuvent, pour des raisons évidentes, discuter librement de leurs activités criminelles avec leur entourage. Bien que des termes comme *botnet*, *DDOS* ou encore *menaces avancées persistantes* fassent maintenant régulièrement leur apparition dans les bulletins de nouvelles, seule une frange marginale de la société comprend vraiment ce qu'elles signifient. Les criminels ne peuvent jamais être trop prudents lorsque vient le temps de se vanter de leurs exploits en personne. Un ami aujourd'hui peut très bien se transformer en ennemi le lendemain et un inconnu qui entend sans le vouloir une conversation peut rapporter ce qu'il sait à la police. L'être humain étant avant tout un être social, il lui est très difficile pour lui de garder à l'intérieur ce qu'il vit à travers ses activités de piratage.

C'est pour ces raisons que les pirates informatiques ont, dès le départ, cherché à trouver des points communs de socialisation avec des individus qui partagent leurs intérêts, leurs valeurs et leur mode de vie. Au début des années 80, ce point de rencontre était les Bulletin Board System (BBS), des serveurs auxquels les pirates pouvaient se connecter à travers les lignes téléphoniques afin d'échanger des messages et des fichiers. L'accès à ces serveurs était limité à un nombre restreint d'initiés et leurs opérateurs géraient jalousement les accès des usagers (Poulsen, 2011). Ces BBS sont rapidement devenus l'équivalent de ce que nous pourrions appeler des communautés en ligne. Les avancées technologiques ont permis aux pirates de diversifier leurs modes d'interactions et nous verrons dans les prochaines sections les différents vecteurs de communication qui ont existé et qui sont toujours utilisés aujourd'hui.

L'existence de telles communautés de pirates ne fait maintenant plus de doute. La littérature actuelle utilise plusieurs termes pour les décrire par exemple souterrain informatique (*computer underground*), communautés en ligne, communauté virtuelle et scène (Leeson & Coyne, 2005). Il existe plusieurs types de communautés. Certaines sont générales et attirent des pirates informatiques de tous acabits. On y retrouve autant des spécialistes du cryptage que des débutants qui en sont encore à l'apprentissage d'outils de piratage. Un excellent exemple de ce type de communauté est le forum en ligne Hack Forums (http://www.hackforums.com) qui contient des discussions aussi diversifiées que la suppression de journaux informatiques, l'exploitation des logiciels Flash et l'obscurcissement de logiciels malveillants. Le souterrain informatique contient aussi une foule de communautés ou scènes spécifiques à chaque type de pirate. De telles communautés permettent à leurs membres de rencontrer d'autres personnes aux intérêts et aux connaissances connexes. Plusieurs chercheurs se sont intéressés à ces communautés en ligne plus spécifiques comme celle des warez (Craig, 2005), des fraudeurs de carte de crédit (Hilley, 2006) ou encore celle de la production de virus informatique (Gordon, 1994).

Qu'il soit question de communautés larges ou spécifiques, les pirates font une distinction très nette entre deux catégories d'individus : les pirates informatiques et les civils (Leeson & Coyne, 2005). Les pirates se considèrent comme faisant partie d'une classe à part des civils qu'ils voient même avec un certain mépris. Ceux-ci ne comprendraient pas la

richesse ni les possibilités qu'offre l'internet et l'informatique moderne et seraient donc à la remorque des pirates qui eux jouissent de toutes les avancées technologiques et en retirent un plus grand pouvoir. Avant d'entrer dans une communauté, les pirates doivent souvent prouver leur appartenance à la confrérie du souterrain informatique en répondant à des questions techniques ou en usant du bon vocabulaire. La connaissance de pirates reconnus est un autre moyen de prouver sa place dans la scène (Leeson & Coyne, 2005). Cet exercice a pour objectif de limiter l'accès aux communautés aux pirates en plus de rendre la vie plus difficile aux agences de police qui tentent d'infiltrer ces milieux clandestins. Les opérations policières des dernières années tendent à démontrer que ce deuxième objectif est loin d'être atteint cependant (Goldman, 2004).

Le monde des pirates n'est pas tout noir ou tout blanc. Il existe aussi plusieurs teintes de gris. À l'intérieur du groupe des pirates, les strates sociales sont aussi évidentes que dans la société générale. Le statut de chaque membre de la communauté est déterminé par plusieurs facteurs incluant sa persistance dans la communauté, ses réalisations, ses contacts et surtout ses compétences techniques (Leeson & Coyne, 2005). Les membres les plus juniors qui ne font qu'utiliser des programmes construits et distribués par d'autres pour tirer avantage d'ordinateurs sont catalogués comme des *noobs* ou encore des *script kiddies*. Ces termes à connotation péjorative rappellent qu'ils réfèrent à des individus qui ne contribuent en rien à la scène : ils ne font que prendre ses outils et ne contribuent en rien à l'accumulation des connaissances. Au-dessus de cette première catégorie se trouve la catégorie générique des pirates qui englobe la majorité des individus. Ceux-ci ont des capacités et des connaissances techniques au-dessus des script kiddies mais n'ont pas encore atteint l'échelon supérieur. Ils sont en mesure de comprendre et de modifier les programmes qu'ils trouvent en ligne et même d'en créer de nouveaux avec des fonctionnalités limitées. Le dernier groupe de pirates est qualifié d'élite ou encore de *leet* dans la communauté en ligne. Ce sont les plus doués de tous. Ils sont derrière les attaques les plus ingénieuses et les plus élaborées. Leur connaissance des systèmes et des réseaux rivalise avec celle de leurs créateurs. Il a souvent été dit que Kevin Mitnick, un pirate réputé des années 90, connaissait mieux les systèmes téléphoniques que les ingénieurs des compagnies eux-mêmes (Shimomura, 1996). Les membres élites ont d'habitude plus d'expérience et une façon de penser qui les sépare de la masse des pirates. Le nombre de

pirates faisant partie de cette catégorie est très faible lorsque comparé aux deux autres catégories.

Le désir de monter dans l'échelle sociale des pirates est une grande source de motivation (Rehn, 2003). Plusieurs pirates comme Mafiaboy[1] ont commis des délits seulement dans l'espoir d'impressionner les autres membres de leur communauté et ainsi d'obtenir le statut suivant (Calce & Silverman, 2008). Les pirates sont donc dans une classe bien particulière de criminels, car ils doivent publiciser leurs délits s'ils veulent recevoir la reconnaissance qu'ils recherchent. Ce besoin insatiable est amplifié par la sous-culture des pirates maintes fois décrite et présentée lors de recherches précédentes (Taylor, 1998). Comme toutes les sous-cultures, celle-ci possède sa langue (argot), ses comportements, ses valeurs et son sens de l'éthique. Devenir un pirate informatique est un processus qui nécessite l'intégration de ces différentes composantes. Ce n'est qu'une fois que cette sous-culture a été intégrée qu'un individu peut affirmer faire partit du sous-terrain informatique.

1.4 Les canaux de communication

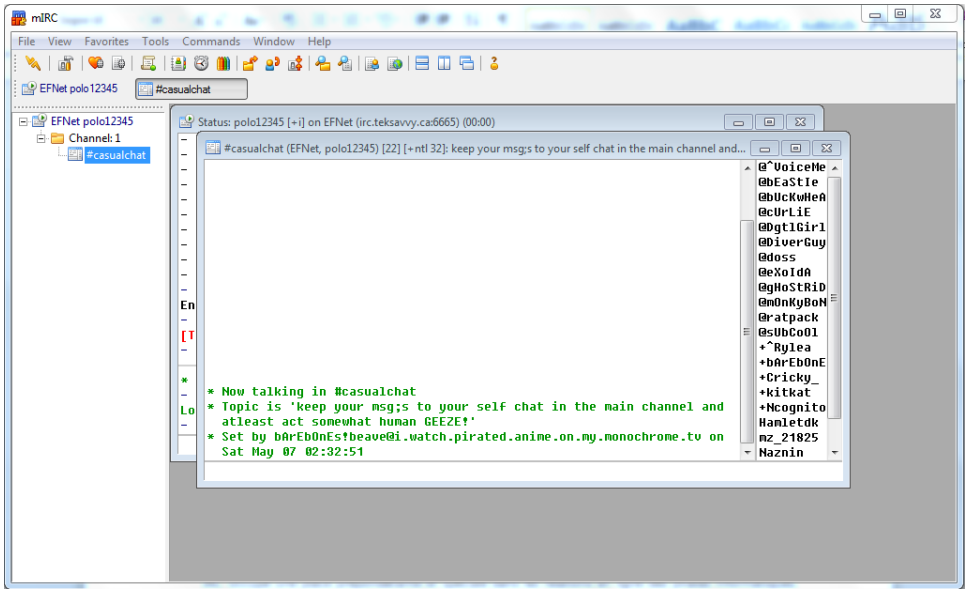
Les pirates informatiques repoussent les limites des technologies actuelles. Ce sont eux qui explorent les logiciels et les appareils les plus récents afin d'en comprendre le fonctionnement. Lorsque vient le temps de communiquer entre eux, les pirates adoptent étonnamment des comportements inverses et utilisent fréquemment des systèmes vieux de plusieurs décennies. Cette section présentera les quatre canaux de communication les plus utilisés par les pirates soit : 1) l'Internet Chat Relay (IRC); 2) les forums en ligne; 3) la messagerie instantanée et; 4) les courriels. L'étude de ces canaux de communication est particulièrement importante, car elle forme et circonscrit la nature des relations entre les pirates. Ceux-ci doivent en effet se limiter aux interactions permises par les systèmes en place. Nous verrons que certains canaux répondent davantage aux besoins des pirates que d'autres.

[1] Mafiaboy était un pirate informatique adolescent de Montréal responsable de la mise hors-service de plusieurs grands portails internet dont Yahoo!, eBay, Amazon et Dell. Son objectif était d'impressionner les pirates faisant partie de son groupe et les autres membres de la communauté. Les dommages estimés de ses attaques se chiffrent en millions de dollars (Wired, 2001).

1.4.1 L'Internet Relay Chat

L'Internet Relay Chat (IRC) occupe une place prépondérante et particulière dans les relations en ligne des pirates informatiques. Ce système de communication écrite synchrone a été créé dans les années 1980 afin de permettre des communications en temps réel.

Figure 1 : Salle de clavardage IRC



La structure d'IRC est hiérarchisée en deux niveaux soit les réseaux et les chambres. Il existe plusieurs centaines de réseaux IRC portant des noms comme EFnet, IRCnet et Freenode. Ceux-ci fonctionnent en silos hermétiques. Ainsi, bien que chaque utilisateur de ces réseaux doit avoir un identifiant unique qui le distingue des autres, il est possible pour plusieurs individus d'avoir le même identifiant tant qu'ils utilisent des réseaux distincts. Chacun de ces réseaux abrite aussi des chambres de clavardage où les utilisateurs peuvent discuter. Les messages peuvent soit être publics ou privés. Il est impossible de remonter dans le temps afin de lire les messages affichés dans le passé. Les serveurs IRC ne peuvent donc être utilisés pour repasser au travers des messages d'anciens utilisateurs, une caractéristique qui ne peut qu'être appréciée des pirates. L'accès aux chambres est libre par défaut. Il existe cependant plusieurs méthodes afin de limiter l'accès à ces chambres à un nombre restreint d'utilisateurs. De la même façon, les noms d'utilisateurs peuvent être utilisés par n'importe qui à moins qu'ils ne soient enregistrés auprès du réseau. Un mot de passe sera alors nécessaire afin de valider son identité.

En plus de son mode synchrone, des chambres privées et des noms d'utilisateurs privés, l'IRC offre plusieurs avantages aux pirates. Chaque serveur compte actuellement des dizaines voire des centaines de milliers de chambres de clavardage. Il est donc possible pour les pirates de se camoufler dans cet océan de chambres afin de passer inaperçu et d'éviter la détection par leurs ennemis et les forces de l'ordre. Par ailleurs, bien que le logiciel client d'IRC soit accessible à tous, il existe une certaine courbe d'apprentissage nécessaire à sa pleine utilisation. IRC possède ses propres commandes et un jargon spécifique qui doivent être intégrés. Cette barrière limite l'accès aux utilisateurs qui ne possèdent pas des compétences de bases et permet donc aux pirates de faire un premier tri entre les n00bs et les membres élites de la communauté. Finalement, les pirates peuvent utiliser des services d'anonymisation qui leur permettent de se connecter à IRC sans avoir à divulguer leur adresse IP. Sans cette information, il devient alors impossible de retracer l'individu qui se cache derrière un nom d'utilisateur. Ses activités peuvent être cataloguées, mais jamais son identité.

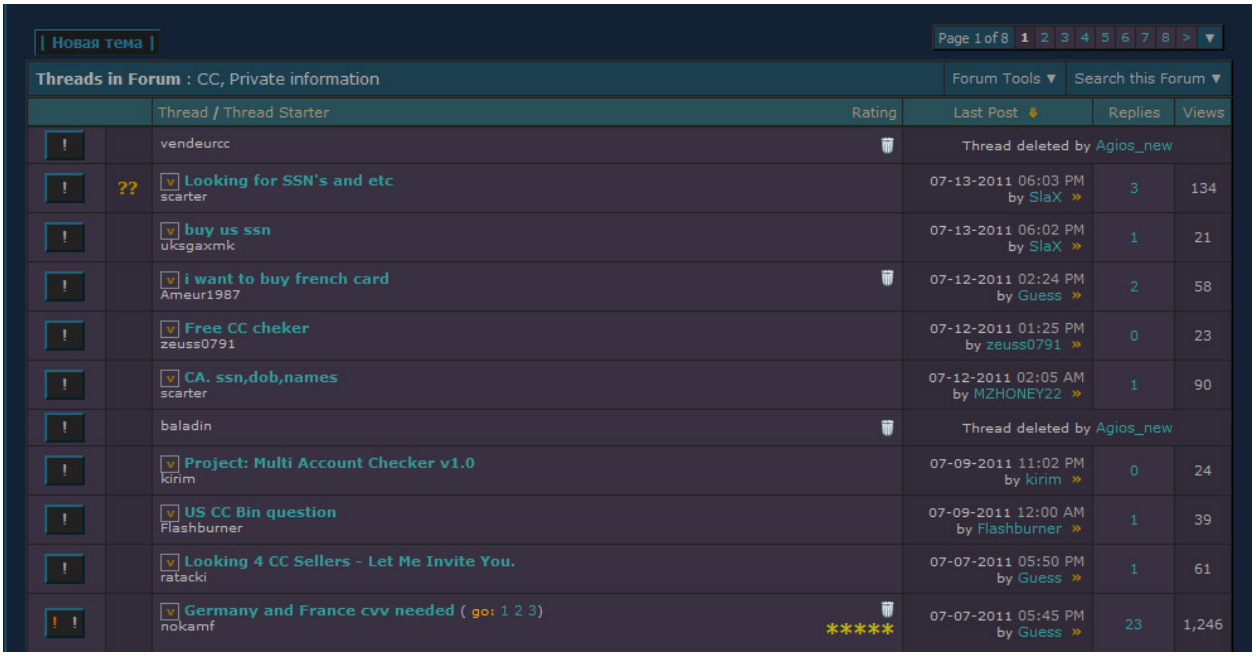
Tous ces facteurs conjugués ont assuré, au fil des ans, une présence importante de pirates sur IRC. Tous les utilisateurs d'IRC ne sont pas des pirates, mais une grande partie des pirates sont des utilisateurs d'IRC. Bien que l'utilisation de ce système de communication réponde à plusieurs de leurs besoins (socialiser, échanger de l'information, achat et vente de produits et services), l'attrait d'IRC vient avant tout de son axe communautaire. À travers ses chambres de discussion, de véritables communautés se sont formées. Les groupes de pirates qui distribuent illégalement de la propriété intellectuelle ont tous leur chambre attitrée. Les pirates qui s'intéresse au vol de télécommunication peuvent se retrouver sur les canaux #cellular et #hackphreak sur EFnet. Finalement, les pirates qui vendent et achètent des cartes de crédit volées trouveront des partenaires d'affaires et des trucs pratiques sur les chambres #carding des réseaux RusNet, Undernet et DALnet. Chacun des membres de cette communauté se créé une personnalité en ligne à travers son nom d'utilisateur qui illustre ses traits de caractère. Le fait que ces chambres soient accessibles en tout temps et partout dans le monde assure un afflux constant et important de membres à ces communautés. L'architecture d'IRC favorise les discussions de groupes tout en permettant, au besoin, à certains individus de discuter discrètement et en privé de sujets plus sensibles. Ces chambres sont donc en

quelque sorte l'équivalent des bars où les criminels se retrouvent pour discuter de leurs exploits et planifier leurs prochains délits.

1.4.2 Forums en ligne

Bien qu'elles occupent une place importante, les chambres IRC ne possèdent pas le monopole des relations en ligne des pirates informatiques. De plus en plus de pirates se tournent vers les forums en ligne pour socialiser avec leurs pairs. Ce type d'infrastructure est la source de plus en plus de recherches récentes sur les cybercriminels (Holt et al., 2010; Rush et al., 2009).

Figure 2 : Forum de discussion en ligne



Les forums en ligne sont des sites web qui permettent à leurs utilisateurs d'échanger des messages et parfois des fichiers. Les modalités d'accès sont différentes pour chacun des systèmes. Alors que certains sont ouverts à tous, d'autres requièrent que les utilisateurs soient enregistrés pour afficher et lire les messages. Les forums sont divisés en sous-sections qui comprennent chacune des discussions. Les messages s'affichent les uns en dessous des autres dans un ordre chronologique. Chaque fois qu'un individu affiche un message, le nom d'utilisateur de son auteur est affiché. Il existe plusieurs logiciels gratuits de forums en ligne comme vBulletin ou BBphp qui permettent d'installer un forum en quelques clics sur

n'importe quel serveur web. Cette facilité d'usage vient cependant avec des lacunes au niveau de la sécurité. Les pirates auront intérêt à découvrir des failles de sécurité dans de tels logiciels étant donné leur large bande d'installation et le passé nous indique qu'ils n'hésitent pas à s'attaquer aux forums d'autres pirates (voir Krebs, 2010c sur le pirate du forum Carding.cc). Les forums sont gérés par des individus qui portent le titre d'administrateurs. Ce sont eux qui policent les interactions en ligne et qui imposent au besoin des sanctions aux utilisateurs qui ne respectent pas les règles d'utilisation des forums. Ces administrateurs ne sont pas toujours des experts en sécurité informatique et en plus de devoir gérer les mises à jour régulières de leurs logiciels clés en main, ils doivent aussi tenter de les configurer du mieux qu'ils peuvent. Les attaques de pirates comme Max Butler (Poulsen, 2011) ont démontré que le succès était loin d'être garanti dans ce domaine.

Malgré ces lacunes du point de vue sécuritaire, les forums en ligne ont beaucoup à offrir aux pirates. Contrairement aux chambres IRC, les discussions sont asynchrones et il est donc possible d'effectuer des recherches dans les archives des forums. Les discussions sont aussi en général plus structurées, car elles sont divisées en catégories et en sujet de discussion. Au lieu d'abriter plusieurs discussions parallèles simultanément, les forums séparent les discussions. Le partage d'information et les discussions sont ainsi plus focalisés et permettent des échanges plus directs et enrichissants. Finalement, seuls les administrateurs du site ont accès aux journaux du site qui contient les adresses IP de ses visiteurs et de ses membres. Il revient alors aux membres d'utiliser des services d'obscurcissement d'adresses IP afin que même les administrateurs ne puissent les retracer.

Ces avantages viennent cependant avec certaines contraintes. En offrant des archives complètes, les forums en ligne sont de riches sources d'information pour les chercheurs et les forces de l'ordre qui peuvent alors amasser une quantité appréciable de preuves contre des individus. Alors qu'IRC oblige les observateurs à surveiller constamment les chambres de discussion, une seule visite sur un forum de discussion permet de télécharger l'ensemble des conversations pour les dernières années. La facilité avec laquelle de telles preuves peuvent être accumulées n'a rien pour rassurer les pirates. Par ailleurs, comme les forums en ligne sont hébergés sur des serveurs web, il est relativement aisé de retracer les adresses IP des utilisateurs. Il incombe donc aux pirates de ne pas oublier de toujours camoufler leurs adresses

IP. Une connexion non protégée peut faire toute la différence. Finalement, les forums de discussion ne peuvent exister sans des administrateurs pour les gérer. Ceux-ci sont encore plus à risque que leurs utilisateurs, car ils doivent trouver un serveur pour héberger le logiciel de forum en ligne. Bien qu'il soit possible de pirater des serveurs afin d'éviter toute trace de paiement, de tels systèmes n'ont pas une très longue durée de vie et ceux-ci doivent donc redoubler d'efforts pour camoufler leurs traces. Alors que n'importe qui peut lancer une chambre de discussion IRC, lancer un nouveau forum en ligne demande plus de préparation et limite ainsi l'arrivée de nouveaux joueurs.

Malgré ces contraintes, de véritables communautés de pirates se sont aussi formées sur les forums en ligne. Ceux-ci remplissent de multiples fonctions dont les deux principales sont le commerce de produits et services illicites ainsi que l'échange d'informations. Poulsen (2011) explique en détail comment les pirates en sont venus à créer des forums en ligne dédiés à la vente et l'achat de toutes sortes d'informations allant des cartes de crédit aux failles de sécurité. Dans de tels forums, des vendeurs affichent leurs marchandises alors que les acheteurs affichent leurs besoins. Les transactions se finalisent à l'aide de messages privés ou encore de la messagerie instantanée (voir ci-dessous). Les pirates recherchent avant tout des partenaires stables et les administrateurs accordent à chacun de leurs membres des cotes de fiabilité (Rush et al., 2009). Chaque pirate est donc encouragé à participer à un forum (ou une communauté) afin de maximiser sa réputation et ainsi réduire la méfiance inhérente à de tels marchés illicites.

Les forums en ligne sont aussi de grandes sources d'informations. Les questions des plus simples (ex : comment télécharger une chanson illégalement) aux plus complexes (ex : comment contourner le blocage de sites web sur un réseau) y sont posées. Les communautés de pirates sont des puits inépuisables de réponses. Au fil des échanges, les pirates en viennent à se bâtir une réputation en prouvant leur valeur à l'aide de leurs réponses. Cette infrastructure n'est pas sans rappeler celle des groupes d'envois de la fin des années 90 telles qu'étudiées par Mann & Sutton (1998).

1.4.3 Messagerie instantanée / courriels

Il n'existe pratiquement aucune étude sur l'utilisation de la messagerie instantanée ou des courriels par les pirates en lien avec leurs relations en ligne. L'information qui filtre de certaines études nous porte à croire que bien qu'utilisés, ces outils sont loin d'être les favoris des pirates. Dans les deux cas, il s'agit de méthodes de communication axées davantage sur des dyades plutôt que des communautés. Ce type d'interaction est de par sa nature privée et donc difficilement observable par les chercheurs. Les seules sources de données pourraient provenir de sources policières et les recherches basées sur des enquêtes de ce genre sont rarissimes. Plusieurs pirates actifs sur les forums en ligne diffusent leur contact de messagerie instantanée (surtout ICQ) afin que leurs partenaires commerciaux puissent les contacter en privé. Les adresses de courriel des pirates sont parfois aussi affichées comme dans les fichiers NFO des groupes de pirates de la scène des warez (Décary-Hétu et al., 2012). Ce type de communication pose par contre certains problèmes. Bien qu'il soit possible d'utiliser de tels outils de façon anonyme, il est techniquement plus compliqué de le faire. Alors que les forums et IRC offrent des systèmes de communication privés, la messagerie instantanée et les courriels offrent un canal de communication externe qui permet de segmenter l'information, mais à un coût humain plus élevé. Ce coût pourrait expliquer la faible utilisation de ces modes de communication par les pirates.

1.5 La communauté des pirates informatiques

Les pirates interagissent donc en ligne à travers deux médiums principaux soit IRC et les forums en ligne. Ils utilisent, au besoin, les systèmes de messagerie instantanée ainsi que le courriel. Leurs interactions en lignes à travers ces canaux de communication s'articulent autour de cinq axes principaux soit : 1) la socialisation; 2) l'échange d'information; 3) l'implication; 4) la reconnaissance et; 5) l'achat et la vente de services.

Tel que mentionné précédemment, les pirates forment des communautés virtuelles qui sont maintenant bien établies. Ce besoin naturel chez l'humain de socialiser fait d'ailleurs partie de l'échelle de Maslow (3^{e} palier; Stum, 2001). Encore plus que les attraits du piratage en lui-même, l'attrait des pirates est avant tout à la communauté (Craig, 2005). C'est en compagnie de ses pairs que le pirate a l'impression d'appartenir à un groupe. Pour plusieurs d'entre eux, c'est la première fois qu'ils se sentent inclus plutôt que rejetés et jugés

(Lunceford, 2009). Les pirates recherchent donc, à travers leur fréquentation des chambres IRC ainsi que les forums en ligne, à faire partie d'un groupe. Le piratage devient donc la clé d'accès qui permet de se joindre au groupe. Cela ne signifie pas pour autant que les actes de piratages n'occupent pas une certaine importance pour les pirates. En effet, une grande quantité de temps et d'énergie est nécessaire afin de maîtriser les bases du piratage et il est donc nécessaire que les pirates aient une certaine prédisposition envers le piratage. Ces actes sont cependant renforcés par la sous-culture du piratage et le besoin d'appartenance des pirates (Holt et al., 2010). Lorsque nous discuterons de l'évolution et de l'état actuel des relations interpersonnelles virtuelles des pirates dans la prochaine section, il sera important de garder en mémoire le cadre dans lequel ces dernières évoluent.

Afin de maintenir leur appartenance à la communauté des pirates, il est nécessaire que les membres restent à jour quant à leurs connaissances dans le domaine du piratage. Pour ce faire, ils se doivent de lire et de s'informer. Les pirates sont d'excellentes sources d'informations et la sous-culture du souterrain informatique encourage la dissémination de l'information entre les membres de la communauté (Holt, 2007). Les pirates se fient donc énormément à leurs pairs pour se garder à jour et comprendre les dernières failles de sécurité et comment les exploiter. Plusieurs recherches font état de cette transmission de l'information latérale chez les pirates informatiques (Holt, 2007). Un pirate qui voudra se joindre à une communauté devra d'ailleurs souvent faire preuve de son savoir en partageant ses connaissances et en répondant aux questions de ses pairs pour prouver son appartenance au souterrain informatique.

Ce partage d'information permettra donc aux pirates de montrer en quelque sorte son implication dans la communauté. La sous-culture du piratage indique que les vrais pirates se doivent de consacrer un nombre important d'heures chaque semaine à leurs activités de piratage (Craig, 2005). Les pirates actifs dans la vente de numéros de carte de crédit affichent d'ailleurs leurs vacances afin de ne pas faire attendre leurs clients. La réputation d'un vendeur dépend en partie de son accessibilité et de la vitesse avec laquelle il est en mesure de répondre aux commandes. Le même phénomène se produit chez les pirates de la scène des warez. Lorsqu'un produit doit être distribué sur internet, le groupe s'attend à ce que ses membres

chargés de la distribution soient disponibles immédiatement et qu'ils se chargent du transfert sans attendre.

Ces échanges d'information ainsi que cette implication dans la communauté des pirates sont en lien intime avec le besoin de se vanter et de recevoir de la reconnaissance de la part des pirates. Ceux-ci forment le seul groupe criminel qui laisse des cartes de visite ou qui annonce publiquement ses crimes (Craig, 2005). Quelques études s'intéressent de près au phénomène de la réputation chez les pirates (Jordan & Taylor, 1998; Sharma, 2007). Elles démontrent que ce besoin incontrôlable d'être reconnu (qui est en lien avec la socialisation) est une des motivations principales derrière les relations interpersonnelles des pirates. Ceux-ci voudront ainsi faire du réseautage avec des pirates reconnus afin d'augmenter leur valeur auprès des autres pirates. Dans plusieurs cas, ce besoin de réputation aura raison des pirates. L'exemple de Mafiaboy est ici frappant. C'est à la suite de ses vantardises dans des chambres IRC publiques que le jeune pirate montréalais a été arrêté (Calce & Silverman, 2008).

Cette réputation n'est pas seulement une source de vanité. Comme mentionnée ci-dessus, celle-ci permet aussi de mesurer la fiabilité des acheteurs et des vendeurs de produits et services illégaux en ligne. Dans tout marché illégal, les sources de conflits et de problèmes sont nombreuses. Comme il n'existe aucun mécanisme officiel de règlement des différends et que les participants sont souvent anonymes, l'établissement d'une cote d'efficacité permet des échanges plus fluides et moins coûteux. Au cours des dernières années, les pirates motivés par l'argent ont pris de plus en plus de place dans les communautés. Les phases d'expérimentation sont maintenant terminées et les pirates sont pleinement conscients du potentiel monétaire de leurs activités. Bien que l'aspect social soit toujours très important pour les pirates, de plus en plus d'entre eux adoptent une attitude d'affaires et le côté social passe ici au second plan.

1.6 Les relations interpersonnelles à l'ère de l'internet

Notre recension des écrits nous a permis jusqu'à maintenant de situer ce qu'est un cybercrime, qui sont les individus qui en commettent et l'organisation sociale, les outils de communication ainsi que le contenu des interactions des cybercriminels. Il est indéniable que le contexte dans lequel ces individus évoluent a eu un impact marquant sur leurs activités et sur leur façon d'entrer en relation les uns avec les autres. Pour comprendre l'impact que

l'internet a eu sur les criminels, particulièrement au niveau de leurs interactions sociales, nous nous tournerons maintenant vers la théorie de l'individualisme réseauté tel que développé par Boase & Wellman (2006).

Ceux-ci se sont intéressés dans un chapitre paru en 2006 à la notion de relation en ligne et ont tenté de comprendre comment les relations interpersonnelles avaient évolué depuis l'arrivée massive des technologies de communication. Ceux-ci (Boase & Wellman, 2006) affirment que depuis plusieurs décennies, la société a vu un changement dans les relations sociales. Cette transformation est issue du développement des transports (avion, automobile, train, autobus) ainsi que des réseaux de télécommunication. Cette transformation qui se veut encore plus marquée dans les centres urbains, s'intitule l'individualisme réseauté (*network individualism*) et comporte cinq caractéristiques soit que :

1) Les gens entretiennent des relations autant avec des personnes proches qu'éloignées géographiquement.

2) Les individus évoluent dans plusieurs réseaux à la fois; ces réseaux sont peu connectés entre eux, mais sont très denses en eux-mêmes.

3) Les relations sont de plus en plus éphémères.

4) Bien que les gens aient toujours tendance à s'associer à des gens qui leur ressemblent, ils entrent en relation de plus en plus avec des personnes aux origines et aux profils différents du leur.

5) Bien que certaines relations soient basées sur des liens forts, la plupart reposent sur des liens faibles.

À eux cinq, ces caractéristiques forment le cœur de la théorie de l'individualisme réseauté. Nous les reprendrons ici individuellement afin d'en extirper toute l'essence.

Relations autant avec des personnes proches qu'éloignées géographiquement

Alors que les possibilités d'échanger avec des gens dans d'autres villes étaient limitées avant les années 1950, il est maintenant possible d'entretenir des relations sérieuses à distance.

Cette affirmation n'est pas nouvelle et remonte aux travaux de Wellman qui avait déjà découvert, en 1979, que la plupart des relations des résidents de Toronto résidaient dans un autre quartier. Les visites en personne et le téléphone étaient alors utilisés pour maintenir des contacts avec ces individus. Les résidents du quartier ne formaient donc qu'une petite partie du réseau social de chaque individu. L'arrivée de l'internet a permis de multiplier les possibilités de communication, et ce, à peu de frais. Bien qu'il soit possible de communiquer avec quiconque dans le monde grâce à l'internet, les internautes préfèrent encore communiquer avec des personnes qui leur sont familières soit leurs amis et leur famille. La simplicité et la rapidité des communications par internet sont les deux facettes qui ont assurées sont adoption par les masses. Boase & Wellman (2006) espèrent pouvoir un jour confirmer l'hypothèse de Shklovski et al. (2006) qui affirment que l'internet est une des sources de la multiplication des contacts des individus avec leurs réseaux sociaux. Cette caractéristique était déjà manifeste dans l'étude de Netville[2] (Wellman & al., 2002) et devra cependant être validée lors d'études futures.

Évolution dans plusieurs réseaux à la fois

Alors qu'auparavant les individus avaient tendance à s'investir dans un seul groupe homogène et très dense, la tendance des dernières années est plutôt à l'investissement dans plusieurs petits groupes. Ces petits groupes ont peu de liens entre eux et c'est en ce sens que chaque personne forge une communauté qui lui est propre. Il n'existe donc plus (ou du moins beaucoup moins) de communautés fermées et exclusives. Conséquemment, il sera difficile de trouver deux personnes qui possèdent exactement le même réseau de liens. Boase & Wellman (2006) amènent l'exemple des couples qui ont des activités séparées de par les rencontres que chacun des époux fait au travail et dans ses loisirs. L'internet est un excellent outil pour maintenir une telle configuration de relations. Il permet de garder le contact avec plusieurs individus à la fois de façon rapide, efficace et sans être intrusif. L'internet est aussi un lieu qui favorise les échanges de un à un ce qui est idéal pour communiquer avec des personnes qui ne se connaissent pas nécessairement entre elles. D'ailleurs, il sera rare qu'une personne

[2] Netville était un nouveau quartier de la région de Toronto au Canada où 109 familles se sont installées. Environ les deux-tiers d'entre elles ont pu avoir accès à un accès internet haute vitesse alors que les autres servaient de groupe de comparaison. Cette étude a démontré que les personnes connectées avaient plus de contact tant au niveau local que régional et international.

connaisse intimement tout le réseau social d'une autre personne, même dans le cas d'un couple. Cela ne veut pas dire pour autant que l'internet empêche le fonctionnement des groupes. Bien au contraire, les forums de discussion ou encore les listes d'envoi sont des outils formidables pour coordonner des projets ou encore des évènements. Cela permet de faire de nouvelles rencontres avec des personnes qui ne viennent pas nécessairement du même milieu que nous sans pour autant avoir à négocier avec les préjugés de son groupe d'appartenance. Alors que certaines sociétés interdisent des liens entre des personnes sur les bases du sexe, de l'origine ou encore de la religion, il devient très difficile pour cette régulation sociale de s'exprimer dans le contexte de l'internet. Une personne peut donc sembler adhérer totalement à un groupe ou une classe sociale et entretenir en secret des liens avec d'autres groupes sociaux sans pour autant avoir à subir les conséquences sociales de ses actes.

Relations de plus en plus éphémères

Les relations modernes sont plus éphémères que jamais. Boase & Wellman (2006) soulèvent à ce sujet le cas des divorces qui sont à un niveau très élevé : même deux personnes qui se sont juré fidélité et amour jusqu'à la mort en viennent à se séparer. Pourquoi en serait-il autrement dans le cas des autres relations sociales? Les changements majeurs dans la vie de tous les jours sont aussi plus marqués depuis les dernières décennies. Cela est dû à une plus grande mobilité des individus tant au niveau professionnel que géographique. Dans ce contexte, la vie moderne amène à faire de nouvelles rencontres et forcément à devoir mettre de côté certaines autres. L'internet devient alors un précieux atout pour maintenir des liens ou encore rencontrer des personnes dans un nouveau milieu. Les réseaux en ligne permettent par ailleurs aux personnes qui ont des phobies sociales ou encore des déficiences au niveau de la socialisation à rencontrer des individus d'une manière douce et graduelle. Il peut parfois être difficile de se parler au téléphone avec le rythme de vie qui accélère toujours plus dans les sociétés industrielles. Le courriel permet alors de s'entendre sur un lieu de rendez-vous plus facilement. Ce même courriel, alors si utile, peut par contre aussi se retourner contre l'expéditeur. Il est plus facile d'ignorer les messages électroniques d'un individu que d'ignorer sa personne lors d'une rencontre en personne. C'est dans ce sens que ceux qui utilisent l'internet strictement pour garder le contact avec les autres peuvent ainsi perdre une partie de leur réseau social s'ils ne s'investissent pas aussi dans des rencontres en personne.

Relation avec des personnes aux origines et aux profils différents

Boase & Wellman (2006) qualifient les échanges par courriels de maigres. Ils entendent par ce terme que le contenu émotif d'une communication électronique est par définition plus faible qu'une communication directement en personne. Bien que cela puisse être une limite dans certaines conditions, c'est une aussi une force lorsque vient le temps de communiquer avec des personnes qui ont des profils sociodémographiques différents. Afin de démontrer son appartenance à un groupe, un individu doit adopter la manière d'être, de parler et d'agir du groupe. Cela demande un grand effort de la part d'un étranger qui veut s'intégrer à un groupe. Les communications digitales permettent de camoufler certaines lacunes dans nos savoir-être et savoir-faire et ainsi de communiquer avec plus de personnes aux profils différents.

Liens forts et liens faibles

Les courriels permettent de renforcer les relations en nous permettant de prendre des rendez-vous plus facilement. Cela permet aussi de coordonner certaines activités tout en n'envahissant pas l'horaire des autres par des appels téléphoniques ou des messages textes qui requièrent l'attention immédiate des personnes avec qui nous communiquons. Les courriels permettent aussi de garder un contact superficiel avec des connaissances et eux de nous répondre au moment qui leur convient le mieux. Cela évite à avoir à rencontrer certaines personnes à des intervalles fréquents et donc de rester en contact avec un plus grand nombre de personnes à la fois. Comme le disent Boase & Wellman (2006), chaque message est un rappel qu'un individu existe pour un autre.

L'intérêt principal de la théorie de l'individualisme réseauté est de présenter un cadre dans lequel nous pouvons situer les relations interpersonnelles dans le contexte d'internet. Celui-ci nous permet de comprendre comment les nouveaux modes de communication ont affecté la façon dont nous entrons en communication et en relation les uns avec les autres. Les cinq points qui forment les caractéristiques de l'individualisme réseauté apparaissent de manière informelle dans plusieurs articles de Wellman et/ou Boase entre 1999 et 2003 (Wellman, 1999; Wellman et al., 2002; Wellman, 2002; Wellman et al., 2003). Chacun de ces articles présente plus ou moins superficiellement les aspects qui forment l'individualisme

réseauté et se chevauchent passablement. Il est étonnant à ce titre de voir le nombre de publications sur le sujet qui n'apportent, dans les faits, que très peu de faits nouveaux. Le chapitre de livre de Boase & Wellman (2006) est à ce titre plus rafraîchissant. Bien qu'il reprenne les mêmes points qu'auparavant, il a le mérite de structurer et encadrer en cinq points tout le rationnel derrière la théorie. Ce n'est donc que dans cet article que l'individualisme réseauté est ainsi présenté. Les articles précédents sur le sujet ont par contre l'avantage de situer la théorie dans un contexte plus historique. Wellman affirme ainsi que l'individualisme réseauté n'est pas apparu avec l'internet. Le processus qui mène à ce type de structure sociale est en fait né au 20^{e} siècle, mais a été grandement accéléré par l'arrivée des communications informatiques. Le téléphone, les automobiles et les avions ont chacun joué leur rôle dans ce mouvement d'une société des groupes vers une société individualisée.

Plusieurs des caractéristiques de l'individualisme réseauté ont aussi été reprises par d'autres chercheurs. Ceux-ci confirment que la distance n'est plus un facteur déterminant lorsque vient le temps d'entrer en relation avec les autres (Shklovski et al., 2008). Les associations se forment autour de communautés en ligne ou encore autour d'activités en commun (jeux en ligne, intérêts particuliers). Alors qu'à une certaine époque les phreakers (pirates des téléphones) avaient le monopole des télécommunications à bas prix, il est maintenant donné à tous de pouvoir échanger avec des individus à des prix plus qu'abordables. La compétition est à ce point vive qu'une compagnie comme Google offre même à ses utilisateurs la possibilité d'appeler n'importe quel téléphone en Amérique du Nord gratuitement (Google, 2011). Les communications informatiques sont l'outil qui permet de contourner les contraintes liées à la distance (Shklovski et al., 2008).

L'internet a aussi permis à un nombre incalculable de communautés de se former. Qu'il s'agisse de forums en ligne, de groupes de discussion ou encore de chambres de clavardage, les internautes ont maintenant entre leurs mains un puissant outil de réseautage (Di Gennaro & Dutton, 2007) qui leur permet de participer dans différents groupes auxquels ils s'identifient. Ces communautés sont plus ou moins ouvertes et encouragent l'investissement chez leurs membres. Ces groupes sont la plupart du temps isolés en ce sens que leur contenu n'est partagé qu'avec les membres. Les internautes peuvent ainsi puiser dans plusieurs de ces groupes afin de répondre à leurs besoins (Di Gennaro & Dutton, 2007). Comme ces besoins

sont différents d'individu en individu, il serait surprenant de constater que deux personnes ont exactement le même cercle social en ligne.

L'appartenance à de tels groupes n'est que très rarement maintenue dans le temps. Des changements dans le mode de vie, des conflits interpersonnels ou encore des problèmes techniques peuvent venir nuire au maintien dans le temps des relations. Comme l'identité d'une personne n'est basée, la plupart du temps, que sur son surnom, il devient difficile de maintenir des liens à l'extérieur de la communauté ou encore de retracer un individu en ligne. Tous ces facteurs nous amènent à constater que les liens en ligne ne peuvent qu'être éphémères. Plusieurs recherches sur les cybercriminels supportent cet argumentaire et soulignent le manque de constance dans les communications (Décary-Hétu et al., 2012). Les pirates informatiques ont l'habitude de disparaître de façon inexpliquée pendant de longues périodes de temps pour ensuite réapparaître. Dans un tel contexte, entretenir une relation est des plus problématique.

Qu'ils soient criminels ou non, les internautes ne montrent pas toujours leur vrai visage aux autres. L'anonymat que procure l'internet leur permet de camoufler leurs traits et caractéristiques personnelles. Ceci peut être bénéfique pour les personnes souffrant d'anxiété ou négatif pour les criminels qui tentent d'abuser de victimes potentielles. Comme les points de rencontre sur internet sont organisés par intérêt particulier, il est normal de voir dans une même chambre de clavardage des personnes aux profils très différents qui ne voient chez les autres que le point commun qui les rassemble à ce moment.

Ce type de relation à distance, éphémère et sans fondement vérifié a un impact négatif sur la qualité des liens. Plusieurs chercheurs soulignent en effet le caractère superficiel des communications en ligne ainsi que la faible implication psychologique des personnes impliquées (Shklovski et al., 2008; Utz, 2007). Les courriels sont le médium favori pour entretenir des relations à distance (Utz, 2007). Il existe encore certains préjugés face aux relations en ligne et à leur qualité médiocre comme en témoigne cette citation : «the internet is a place where individuals are separated from the natural world, isolated from the offline reality and from their real and more genuine relationships» (Standlee, 2009). Bien qu'il soit possible d'entretenir des relations fortes à distance (Shklovski et al. 2008), il semble que la majorité des

chercheurs concèdent que le maintien de relations en ligne soit difficile et pour la plupart relativement superficiel (Nasi et al., 2004).

1.7 Pirates informatiques et individualisme réseauté

La dernière section nous a permis de comprendre comment l'internet avait modifié les relations interpersonnelles des internautes. Cette section tentera maintenant de comprendre si les théories générales des relations interpersonnelles peuvent aussi s'appliquer aux pirates informatiques. Pour ce faire, nous reprendrons point par point la théorie de l'individualisme réseauté et nous examinerons comment elle peut s'appliquer aux pirates informatiques.

Relations autant avec des personnes proches qu'éloignées géographiquement

Ce premier point sur la répartition géographique des relations ne pourrait être plus vrai que pour les pirates. Au plus fort de l'époque des BBS, les contacts entre pirates étaient fortement limités par les coûts des appels interurbains (il fallait se connecter au BBS par ligne téléphonique et donc payer ces frais). Avec l'arrivée de l'internet, les communications entre les pirates se sont accélérées et ont permis au niveau de prendre une ampleur mondiale. Cela ne veut pas dire que les pirates ont renié leurs racines pour autant. Plusieurs groupes de pirates affichent dans leur nom l'indicatif régional d'origine de leur membre (ex : The 414s; Lin, 1995) démontrant ainsi qu'il existe toujours un lien qui unit les pirates sur un niveau régional. Plus récemment, l'arrivée des Hackerspaces a démontré l'attachement des pirates pour leur région géographique. Ces salles communautaires ouvertes à tous offrent la possibilité aux pirates de côtoyer d'autres individus aux intérêts similaires et de travailler sur leurs projets dans un environnement stimulant (Hackerspaces, 2011). Bien qu'officiellement à vocation légale, ces endroits ne discriminent pas leurs membres selon qu'ils soient des pirates blancs ou noirs et les deux clans s'y rencontrent.

Parallèlement à ces regroupements locaux, les pirates se sont aussi connecté les uns aux autres au niveau international. Les études sur les fraudes par cartes bancaires en sont un excellent exemple. Les forums de discussion où se négocient les informations bancaires volées offrent des numéros de carte européens, asiatiques et nord-américains. Les services connexes (impression de fausses cartes, matériel nécessaire à la contrefaçon, mules pour détourner des fonds) proviennent autant d'Europe de l'Est que des États-Unis. À la lecture des messages

affichés sur ces forums, il est raisonnable de supposer que bien des participants à ce type de fraudes ne proviennent pas de pays anglophones (voir par exemple http://www.carding.cc). Certains forums ont d'ailleurs des sous-sections dédiées à des langues ou des régions spécifiques. Avec l'arrivée de services de paiement comme eGold, il est maintenant possible de transférer des fonds de façon anonyme et rapide partout sur la planète pour payer les services des fraudeurs.

La scène des warez est elle aussi fortement décentralisée et repartie sur plusieurs continents. Les chercheurs s'entendent pour dire que les pirates proviennent autant de Russie, des États-Unis que d'Europe (Symantec, 2008). Plusieurs groupes importants se sont fait arrêter au cours des 15 dernières années et à chaque fois ces arrestations ont nécessité la coopération de plusieurs corps de police nationaux afin de mener à bien les opérations confirmant ainsi la nature internationale des groupes de warez.

Évolution dans plusieurs réseaux à la fois

Comme mentionné dans le chapitre précédent, les pirates utilisent surtout les chambres IRC ainsi que les forums de discussion pour communiquer entre eux. Ces médiums sont excessivement bien adaptés à la nature des réseaux tels que décrits par Boase & Wellman (2006). Chaque chambre ou chaque section de forum compte sur ses propres membres qui forment chacun une communauté. Les pirates peuvent ainsi rester en contact avec plusieurs groupes simultanément. Ainsi, un opérateur de botnet désirant vendre ses services pourra utiliser plusieurs chambres IRC et forums afin de placer ses annonces et ainsi trouver dans chacune de ces communautés une source différente de clients potentiels. Les liens à l'intérieur de ces communautés sont d'ordinaire très nombreux. Ainsi, les clients s'attendent à ce que les opérateurs de botnet puissent fournir dans un délai très bref des réponses à leurs questions. Cela implique une participation active et un nombre élevé de messages échangés quotidiennement. Le même phénomène se retrouve aussi dans la scène des warez. Les membres d'un même groupe de pirates passent plusieurs heures à se parler en ligne chaque semaine et chaque groupe exige de ses membres une implication au plus haut niveau (Craig, 2005). Chaque pirate est libre de faire partie de plusieurs groupes comme l'indique la théorie

de Boase & Wellman (2006). Des recherches passées ont démontré que les liens entre les différents groupes sont assez restreints (Décary-Hétu et al., 2012).

Relations de plus en plus éphémères

Cette caractéristique des relations interpersonnelles à l'ère d'internet s'applique aussi parfaitement aux pirates. Ces derniers utilisent des surnoms afin de maintenir un certain anonymat. Rien n'est plus aisé que de changer de surnom sur un site ou dans le souterrain informatique. Aux premiers signes de problème ou encore de conflit, un pirate peut changer de surnom et ainsi repartir avec une réputation vierge (Craig, 2005). Ce changement est une arme à double tranchant. En changeant de nom, les pirates perdent aussi leurs réseaux de contacts plus distants (à qui ils ne veulent pas dévoiler leur double identité) ainsi que la réputation qu'ils avaient jusqu'alors accumulée. Ces changements de surnoms arrivent fréquemment dans la scène et les pirates se questionnent continuellement sur la véritable identité des nouveaux pirates qui font leur entrée dans le souterrain informatique (Craig, 2005). Certains novices semblent en connaître beaucoup pour des non-initiés.

Relation avec des personnes aux origines et aux profils différents

Les pirates informatiques font partie d'une frange marginalisée d'internautes. Ils sont de façon routinière démonisés par les médias de masse – par exemple de Kevin Mitnick était accusé de pouvoir lancer des frappes nucléaires à partir du téléphone de sa prison en sifflant des commandes aux ordinateurs de l'armée américaine. Comme nous l'avons vu, les pirates se considèrent eux-mêmes comme différents des autres et ont en quelque sorte intériorisé cette image. Ce trait de caractère est une des rares caractéristiques qui lie les pirates entre eux. Les recherches passées, bien que relativement superficielles, font état du manque de cohésion entre les profils sociodémographiques des pirates (Jordan & Taylor, 1998). Ceux-ci sont d'origine variée, de tous âges et occupent des postes allant du chômeur à l'ingénieur (Goldman, 2004). Les sections précédentes de ce papier nous ont permis de prouver le fort degré de socialisation des pirates. Il nous est donc permis de supposer que ces différences au niveau de leur profil n'empêchent pas les pirates de se regrouper. Tel que le proposent Boase & Wellman (2006), les modalités des communications par ordinateur réduisent les barrières à la socialisation entre différents groupes culturels et permet ainsi des échanges et des relations, peu importe l'origine

et le statut. L'important pour les pirates semble davantage d'atteindre ses objectifs que de juger les autres.

Liens forts et liens faibles

Le souterrain informatique n'a pas toujours été aussi populeux qu'aujourd'hui. Au départ, le haut coût des pièces et des logiciels limitaient grandement le nombre d'adaptes et de pirates informatiques. Les études actuelles sur les différents réseaux de pirates démontrent que ceux-ci sont maintenant très développés et comptent des milliers de membres (Symantec, 2008). Ce nombre important de contacts potentiels ne peut qu'avoir un effet à la baisse sur la qualité des liens que les pirates entretiennent. Des études ont déjà démontré que n'importe quel individu ne peut entretenir qu'un nombre très restreint de relations fortes. Lorsque nous déduisons de ce nombre les relations dans le monde réel des pirates, leurs relations sérieuses en ligne ne peuvent qu'être restreintes. Par ailleurs, la nature des activités des pirates noirs ne peut qu'être un frein à la création de liens forts. Afin de maintenir un certain anonymat, les pirates se doivent de garder jalousement le plus de détails possible sur leur vie. Établir une relation forte basée sur la confiance est alors on ne peut plus difficile. Bon nombre de pirates amis ne sont jamais rencontrés en personne (Craig, 2005) et bien qu'ils se disent amis, il serait intéressant de voir à quel point ils se connaissent vraiment. Dans un tel contexte, les liens entre les pirates ne peuvent qu'être faibles dans la grande majorité des cas.

Ces quelques paragraphes viennent confirmer que les pirates informatiques ne se différencient que très peu des internautes lorsque vient le temps d'étudier leurs relations interpersonnelles. Même s'ils évoluent dans un contexte plus particulier, les mêmes dynamiques s'appliquent aussi dans leur cas. Avant d'être des criminels, les pirates sont donc des internautes et leurs relations sociales ne sont pas si différentes des autres individus. Il est clair de par les nombreuses études citées dans cette section que les activités des pirates sont très différentes de l'internaute moyen. Peu d'entre eux pourraient, en effet, prendre le contrôle de serveurs web ou encore trouver des numéros de carte de crédit à vendre. La nature humaine l'emporte cependant lorsque vient le temps d'entrer en relation et autant les internautes que les pirates ont migré vers l'individualisme réseauté.

1.8 Conclusion

Ce premier chapitre nous a permis de développer une compréhension commune du contexte de cette thèse, l'internet. Les récents développements des services dans les nuages ont permis une démocratisation des outils technologiques. Cet accès élargi a eu pour impact de fournir de nouvelles armes à une catégorie de criminels mieux connus sous le pseudonyme de pirates informatiques. Ceux-ci ont vu autant leur capacité d'attaque que leur surface d'attaque s'agrandir avec le nombre d'internautes et de systèmes branchés sur la toile mondiale. Un accent particulier a ici été placé sur les relations et les interactions entre criminels. Nous avons ainsi pu passer en revue plusieurs des moyens de communication utilisés par ces cybercriminels comme IRC, les forums de discussion et la messagerie instantanée. Nous avons aussi été en mesure d'analyser la formation de communautés en ligne de criminels ainsi que la dynamique des relations interpersonnelles à l'ère de l'internet.

Un tel centre d'intérêt n'a pas été choisi au hasard. En effet, la tendance actuelle est à la création de marchés criminels en ligne où des biens et services sont vendus illégalement. La prochaine section qui porte sur certaines formes particulières de cybercrime nous présentera plus en détail ces marchés illicites. Dans ce contexte d'économie souterraine, les relations interpersonnelles promettent d'être des plus importantes. Comme les études le démontrent (Snijders & Zijdeman, 2004), il est pratiquement impossible de déterminer la qualité d'un produit ou d'un service à l'avance. Étant donné l'anonymat relatif des plateformes en ligne, il est aussi excessivement difficile d'évaluer la fiabilité des partenaires d'affaires. Les signaux utilisés habituellement pour juger de la qualité de possibles associés (Gambetta, 2009) ne trouvent évidemment pas d'équivalent dans le monde virtuel. Pour comprendre le fonctionnement des marchés criminels en ligne, il est donc éminemment important de comprendre les relations interpersonnelles des acteurs, car celles-ci seront au cœur des transactions illicites. La vision de Boase & Wellman (2006) que nous embrassons dans cette thèse est que les relations sont maintenant beaucoup plus nombreuses, diversifiées et personnelles. Cela nous permet de penser que les réseaux criminels seront beaucoup plus résilients à l'ère de l'internet en raison de la redondance des liens et des nombreux contacts. Identifier et retirer le pivot d'un réseau sera une tâche beaucoup plus compliquée en raison de

l'individualisme réseauté. Une bonne compréhension des réseaux criminels passera donc immanquablement par une analyse fine des relations interpersonnelles des pirates.

Ceci dit, la nature même des réseaux criminels est et sera du moins à court terme un frein à l'établissement des relations interpersonnelles. Passer outre à l'asymétrie d'informations qu'entretiennent les cybercriminels est une difficulté difficilement surmontable. Cette thèse aura pour objet de démontrer pourquoi et comment la réputation criminelle est utilisée pour réduire les frictions inhérentes aux marchés illicites. Qu'elle soit de première ou de seconde main, la réputation criminelle permet de faire un premier tri des partenaires potentiels et de mieux guider les choix stratégiques. Le Chapitre III nous permettra de développer ce thème plus à fond en passant en revue une littérature large et variée issue des champs de la criminologie, du marketing et de la gestion des affaires. Avant d'y arriver cependant, nous continuerons à bâtir les fondements de cette thèse en passant en revue les connaissances actuelles sur trois types de criminalité qui ont aujourd'hui une forte présence en ligne soit le vol de propriété intellectuelle, les réseaux d'ordinateurs infectés et le vol d'informations financières.

CHAPITRE 2 – FORMES PARTICULIÈRES DE CYBERCRIMES

L'ingéniosité des cybercriminels n'est plus à prouver aujourd'hui. Au cours des dernières années, leur capacité à abuser de systèmes informatiques a explosé, tel que le démontre un article de Krebs (2012 b) expliquant pourquoi des criminels mettaient tant d'efforts à infecter tous les ordinateurs connectés à l'internet, aussi vieux et lents soient-ils. Ceux-ci seraient en effet en mesure de tirer d'important profits en utilisant ces machines pour héberger du contenu illicite, pour attaquer d'autres systèmes ou encore dérober les données financières et personnelles de ses utilisateur. Il est difficile de se maintenir à jour devant toutes les nouvelles formes que peut prendre la cybercriminalité. De nouvelles formes apparaissent chaque année et les techniques évoluent au rythme de l'internet. Ce chapitre nous permettra de mettre à jour les connaissances de tous en lien avec les formes particulières de cybercrimes sur lesquelles nous centrerons notre attention tout au long de cette thèse.

Nous commencerons tout d'abord par une présentation de la scène des warez, la communauté de pirates responsables de la fraude de propriété intellectuelle en ligne. Nous verrons qu'elle est très décentralisée et efficace en raison d'une division du travail très perfectionnée. Nous continuerons avec les botmasters, ces individus qui prennent le contrôle de systèmes informatiques. Ceux-ci sont d'excellents courtiers qui mettent leur expertise au service du criminel le plus offrant. Nous terminerons cette revue par les cardeurs. Ces criminels dérobent et utilisent les informations financières personnelles d'individus et de compagnies pour s'enrichir personnellement. À eux trois, ces cybercriminels représentent les plus grandes menaces actuelles et nous permettront d'avoir une vue d'ensemble du genre de criminels actifs sur l'internet.

2.1 Les warez

Le fait qu'internet permet de télécharger illégalement de la propriété intellectuelle (livres, jeux, musique, films, logiciels) n'est plus un secret pour personne. Les médias de masse ont en effet commenté extensivement les déboires de réseaux comme Napster, qui facilitaient comme jamais auparavant l'échange de fichiers protégés par le droit d'auteur (Ku, 2002). Ce que peu de gens savent, par contre, c'est qu'il existe une communauté de pirates informatique qui se spécialisent dans la diffusion de ce type de produits sur internet (Craig,

2005). Ces individus forment des groupes (ou clans) qui tentent d'obtenir le plus de reconnaissance de la part de leurs pairs en distribuant le plus grand nombre de fichiers aussi connus sous le nom de warez (Rehn, 2003). La communauté dans laquelle évoluent ces groupes de pirates se nomme la scène des warez (déformation techno-enthousiaste du mot "software"). La littérature sur le sujet se concentre sur trois aspects de la scène: la régulation (la réponse sociale), l'offre (les groupes de pirates) et la demande (les consommateurs qui téléchargent les fichiers distribués par les pirates). Nous aborderons chacun de ces aspects individuellement.

2.1.1 La régulation de la scène des warez

La Business Software Alliance (BSA), la Recording Industry Association of America (RIAA) et la Motion Picture Association of America (MPAA) ont tous déclaré que le piratage en ligne leur coûte à eux et la société en général des milliards de dollars (Marshall, 2006) sans pour autant être en mesure de démontrer que c'est bien le cas (Leman-Langlois, 2004). Afin d'arrêter cette supposée hémorragie de fonds, ces groupes de pression ont utilisé une variété de méthodes. Ils ont tout d'abord fait pression sur les gouvernements pour qu'ils adoptent de nouveaux règlements plus agressifs au niveau des infractions du droit d'auteur. Cet objectif a largement été atteint avec l'adoption d'une série de nouvelles lois et de traités comme le NET (No Electronic Theft Act), le DMCA (Digital Millennium Copyright Act), le FECA (Family Entertainment And Copyright Act), le WCT (World Intellectual Property Organization Copyright Treaty) et l'EUCD (Directive sur le droit d'auteur de l'UE) (Goldman, 2004; Ponte, 2008; Marshall, 2006). D'un point de vue pénal, certaines de ces législations se sont avérées très efficaces pour condamner les personnes accusées. Le No Electronic Theft Act, par exemple, criminalise les infractions au droit d'auteur en échange d'un gain financier ou autre[3] (Goldman, 2004). À elle seule, cette loi a été utilisée pour accuser et condamner plus de 80 pirates, y compris des employés de grandes sociétés comme Intel et Microsoft ainsi que des membres des plus grands groupes de pirates comme PWA et DoD (Goldman, 2004). Chaque personne qui a été accusée en vertu du NET Act a été condamnée ou a plaidé coupable (Goldman, 2004).

[3] La jurisprudence a tranché que les pirates qui obtenaient, en échange de leur travail, un accès à des serveurs contenant des warez obtenaient ainsi un gain similaire à un gain financier étant donné qu'ils pouvaient bénéficier de produits commerciaux sans pour autant avoir à payer pour.

Les sociétés détentrices de droit d'auteur ont aussi misé sur des solutions techniques au problème des warez en appliquant divers stratagèmes de gestion des droits numériques (*digital rights management*, DRM) comme l'indicatif régional appliqué aux DVD commerciaux (Ponte, 2008; Bridy, 2009, Marshall, 2006). Ces outils visent à limiter la façon dont un individu peut consommer le matériel produit par ces entreprises. Ils permettent aussi de contrôler les plates-formes et les délais sur lesquels le contenu est disponible. Puisque ces solutions techniques sont vulnérables à des contre-solution, des lois comme le DMCA ont criminalisé le fait de distribuer des outils permettant de contourner les limites imposées par les DRM (Marshall, 2006). Cette interdiction légale n'a en rien empêché l'accès à de tels outils sur internet (Goode, 2006).

Les détenteurs de droits ont également pris les choses en main à l'aide des tribunaux civils, en poursuivant les consommateurs de warez (Bridy, 2009). Ils ont embauché des sociétés privées pour épier les réseaux P2P et faire une liste des individus y accédant. Ils se sont également attaqués aux grands opérateurs de réseaux P2P tels que KaZaA et Limewire, qui fournissaient un moyen d'échanger du matériel protégé par le droit d'auteur (Bridy, 2009). Bien que ces réseaux aient été déclarés illégaux dans plusieurs juridictions, la technologie derrière leurs infrastructures ne l'a pas été, ce qui a permis à d'autres services de prendre la relève dans de très brefs délais en raffinant à chaque itération les fonctionnalités proposées (et l'anonymat des utilisateurs). Les détenteurs de droits ont également conclu des accords avec les fournisseurs d'accès à l'internet afin de surveiller activement les individus qui utilisent des protocoles P2P, une pratique qui a depuis été mise hors la loi par les autorités américaines (Bridy, 2009).

Les chercheurs sont jusqu'à présent parvenus à la conclusion que les stratégies énumérées ci-dessus n'ont pas été des plus efficaces. Afin d'endiguer le flot de warez, les recherches (Ponte, 2008; Gopal & Sanders, 2000;. Bridy 2009) suggèrent donc de s'attaquer aux fournisseurs de warez et non aux consommateurs, de réduire le temps entre la présentation d'un film au cinéma et sa sortie en DVD, l'amélioration de l'expérience des consommateurs et l'indexation du prix des logiciels au PNB national (Ponte, 2008; Bridy, 2009 ; Gopal & Sanders, 2000).

2.1.2 La demande dans la scène des warez

La majeure partie de la recherche sur la scène warez se concentre sur les consommateurs qui téléchargent du contenu illégal fourni par les groupes de piratage. Beaucoup d'études essaient de comprendre la motivation des consommateurs au moyen d'enquêtes sur les étudiants (Chiang et Assane, 2002; Kini et al., 2004; Rahim et al., 1999; Sims et al., 1996). Les résultats de ces études tendent à être spécifiques à leur échantillon, à peine généralisable et frôlant la tautologie. Il n'est guère surprenant d'apprendre que les élèves qui ont plus de compétences techniques, qui utilisent davantage l'Internet et qui ont une éthique faible sont plus impliqués dans le téléchargement illégal de produits protégés (Hinduja, 2003). Ce même auteur a également constaté dans une étude précédente que la vitesse de la connexion Internet ainsi que le piratage physique de produits ont un impact positif sur le piratage en ligne (Hinduja, 2001). Certaines études dans ce domaine vont par contre à l'envers des croyances générales. Par exemple, les réseaux P2P ne seraient pas le premier choix des consommateurs de warez (Schultz, 2005). Les gens seraient plus enclins à télécharger des produits sur IRC et dans des newsgroups qui ont beaucoup moins attiré l'attention des services de police et des titulaires de droits d'auteur. Les consommateurs ne sont pas non plus insensibles aux efforts de réglementation décrits dans la section précédente (*la régulation de la scène des warez*). Ainsi, une hausse des risques perçus de piratage entraîne une réduction de la fréquence des téléchargements illégaux. L'acte de piratage est associé à un sentiment de culpabilité, mais ce dernier est neutralisé par la facilité avec laquelle les individus peuvent pirater et les avantages qu'ils en retirent. Nous noterons pour finir que les individus ont tendance à télécharger des fichiers qui ont une valeur monétaire élevée et une taille de fichier faible (surtout de la musique et des logiciels; voir Schultz, 2005).

2.1.3 L'offre dans la scène des warez

La recherche sur l'offre vise soit les groupes de pirates professionnels soit les amateurs. Tel que mentionné au début de cette section, les groupes de pirates sont des collectifs d'individus qui consacrent une partie importante de leur temps à la scène warez (Craig, 2005). Ce sont les pirates qui sont les plus prolifiques et qui distribuent la quasi-totalité des logiciels et des jeux dans la scène des warez (Goldman, 2004). Les amateurs sont des citoyens ordinaires qui offrent du contenu protégé par les droits d'auteur sur les réseaux poste-

à-poste (P2P) (Hinduja, 2007). La différence entre ces deux catégories est le niveau d'implication dans la scène warez. Il n'est pas rare pour les pirates de passer plus de 40 heures par semaine à travailler dans la scène des warez (Craig, 2005; Goode, 2006). Les amateurs eux sont généralement plus intéressés par ce qu'ils peuvent télécharger plutôt que ce qu'ils peuvent offrir. En général, ils distribuent des vidéos ou des fichiers musicaux qui nécessitent très peu de compétences et utilisent les réseaux P2P où ils deviennent des redistributeurs. Ils ne ressentent pas de culpabilité, ont des compétences informatiques décentes et sont surtout de sexe masculin (Hinduja, 2007). Alors que les pirates peuvent être vus comme des professionnels, les amateurs sont plutôt définis comme des passionnés (Goldman, 2005).

Les groupes de pirates ont grandi en popularité avec la démocratisation de l'ordinateur personnel et sont devenus des entités d'envergure internationale. Leurs membres utilisent des alias pour camoufler leur identité secrète et se rencontrent rarement en personne (Goode, 2006; Craig, 2005). Leur principal objectif est de devenir les pirates les plus respectés de la scène warez (Rehn, 2003; Craig, 2005). Pour ce faire, ils s'affrontent dans ce qui pourrait être qualifié de tournoi sans fin. La quantité et la qualité des produits piratés par chaque groupe sont mesurées et évaluées par la communauté. Chaque fois qu'un groupe distribue un nouveau warez, il lance un défi aux autres groupes qui doivent soit répondre en distribuant un produit de valeur égale ou perdre une partie de leur statut social dans la scène (Rehn, 2003). Les pirates sont motivés par leur ego, l'excitation du danger, leurs croyances (ex : toute information devrait être gratuite et libre) et leur besoin d'appartenance (Goldman, 2005). Ils ressentent le besoin de prouver leur valeur aux autres et la scène warez est la façon dont ils ont choisi de le faire.

L'importance de la réputation venant des pairs (et dans une moindre partie du public) est une différence notoire entre les criminels de la scène des warez et les autres criminels que nous étudierons dans les chapitres à venir. En effet, ces derniers visent à augmenter leurs gains financiers plutôt que leur niveau de prestige, à l'image des autres criminels à col blancs qui oeuvrent en dehors de l'internet (Kshetri, 2010). Cette différence au niveau de la motivation est majeure et a un impact important sur la prévention et le contrôle de cette forme de criminalité. Dans le cas des warez, la répression risque d'avoir un impact dissuasif moindre étant donné que les comportements des individus sont dictés par une motivation intrinsèque.

Ainsi, le fait de distribuer en ligne de la propriété intellectuelle vient d'un besoin d'appartenance, de réputation et de réalisation qui pourrait difficilement être compensé à court terme par d'autres formes de récompenses. Dans le cas des autres formes de criminalité (botnets, carding), une répression accrue ou du moins plus visible pourrait avoir un effet de déplacement tel que décrit par Eck (1993). Les besoins financiers des criminels pourraient en effet être aisément compensés à l'aide d'autres formes de criminalités et ces marchés pourraient donc s'adapter plus facilement aux interventions policières. La scène des warez devrait, elle, résister davantage aux attaques et perdurer dans le temps. Il est intéressant ici de constater que la scène des warez est une anomalie en ce sens qu'elle a peu changée au cours des quarante dernières années. La première génération de pirates informatiques était elle aussi motivée par un fort sens de curiosité et par un désir de tester les limites. Les générations suivantes ont réalisé le pouvoir qu'elles détenaient et ont su utilisé leur talent pour augmenter leur capital économique (Kshetri, 2010). Cette transition graduelle s'est opérée particulièrement au cours des dix dernières années et il sera intéressant de surveiller dans un futur rapproché si la scène des warez tend à suivre un chemin similaire et les tensions internes à cette scène si certains participants sont tentés de suivre l'exemple des autres criminels. La scène des warez est donc figée dans le temps et cela pourrait contribuer à nuire au recrutement de nouveaux pirates qui pourraient trouver cet environnement dépassé et donc décider de s'investir dans les marchés pirates qui sont davantage axés sur les gains monétaires plutôt que sociaux et relationnels.

La scène des warez est un milieu relativement fermé avec ses propres règles, ses coutumes et ses médias (Rehn, 2003; Craig, 2005). Il n'y a pas de lieu central où tous les groupes de pirates se rencontrent. Ils utilisent les canaux IRC ou distribuent des journaux clandestins pour se contacter les uns les autres. Bien que la scène se compose principalement de groupes de pirates, certains individus indépendants sont également autorisés à y participer (Goldman, 2005). Ces personnes sont soit des collectionneurs ou des amateurs qui recueillent d'anciens logiciels qui ne sont plus disponibles. L'éthique est très importante dans la scène (Craig, 2005; Rehn, 2003; Goldman, 2005). Aucune rétribution monétaire pour le travail dans la scène des warez n'est acceptée. Les groupes encouragent souvent le public à acheter les produits qu'ils aiment. En ce sens, les warez sont considérés comme une option pour essayer

avant d'acheter. Cette manière de concevoir la scène des warez permet de neutraliser tout sentiment de culpabilité ressenti par les pirates (Goode, 2006; Craig, 2005).

La recherche sur la scène des warez que nous venons de présenter n'est pas sans intérêt; bien au contraire. Elle est cependant limitée à quelques niveaux. Tout d'abord, les chercheurs se sont par le passé particulièrement concentrés à la demande, à la régulation ainsi qu'aux amateurs qui distribuent des warez en ligne. Cela a déplacé le moteur de cette activité illicite, les groupes de pirates professionnels, du point central d'intérêt vers la périphérie. Nous avons donc ici, comme dans le cas des botnets, un déficit de connaissances au niveau des acteurs principaux de la scène. Cela permet aux groupes de pirates de poursuivre leurs activités beaucoup plus aisément. La dynamique interne des groupes ainsi que les systèmes de promotion et d'intégration dans des groupes devraient être étudiés en détail afin de comprendre comment la scène des warez survit depuis des années. Il existe aussi beaucoup de répétition dans les études. Un même fil d'idée sera souvent repris. Ce trait est particulièrement frappant lorsque nous étudions les sondages auprès d'étudiants universitaires. Ce choix de sujets, bien que sans doute très pratique pour les chercheurs, reste très surprenant. Nous pouvons douter de la représentativité des étudiants universitaires; ils ne correspondent fort probablement pas au profil des criminels professionnels ou encore à tous les consommateurs de warez. Ainsi, les méthodologies employées ne permettent que rarement de généraliser les résultats en raison d'échantillons trop limités. Finalement, quelques chercheurs nous semblent être de simples relais des groupes industriels. En citant à répétition les statistiques non validées des groupes de pression, les chercheurs ne font qu'augmenter la campagne de peur créée par ces derniers et ajoutent à la vague de désinformation. Avec ses moyens financiers, les groupes de pression prennent beaucoup de place dans le débat sur la scène des warez et il serait important de séparer la recherche commanditée de la recherche impartiale.

Bien qu'absente de cette revue de littérature, la question de la légalité des warez se doit d'être attaquée. Tout comme bien d'autres pratiques questionnables, le fait d'offrir ou de télécharger des warez n'a pas été criminalisé dans la plupart des juridictions. Même dans celles qui sont passées à l'action et qui ont créé une nouvelle classe de crime, la pertinence et les motivations derrière ces modifications légales sont remises en doute (Leman-Langlois, 2004). Ce débat, bien qu'intéressant, est en dehors du champ de notre thèse. Notre revue de

littérature a démontré que les pirates s'organisent dans des entités dévouées au contournement des règles sur le droit d'auteur. Ils utilisent des pseudonymes pour camoufler leur identité, se rencontrent dans des chambres IRC secrètes et ont un discours de défiance face aux détenteurs de droit d'auteur. Les pirates du warez savent donc qu'ils encourent un risque de répression sociale en participant à la scène. Leurs comportements ne sont donc possiblement pas aussi criminels que d'autres, mais ils se situent malgré tout sur un continuum de comportements visés par la réprobation sociale. Leurs attitudes et comportements démontrent qu'ils sont bien au fait qu'ils s'exposent à des conséquences légales civiles voir même criminelles. Pour ces raisons, nous avons donc décidé d'inclure les pirates de la scène des warez dans notre échantillon de thèse.

2.2 Les botnets

Le mot *botnet* se divise en deux parties soit *bot* pour robot et *net* pour réseau (*network* en anglais). Dans la pratique, un botnet « réfère à une collection d'ordinateurs compromis (les *robots*) qui sont contrôlés par un botmaster » (Li & al, 2009 : p.1). Les criminels qui s'adonnent à ce type de déviance ont donc pour objectif d'infecter à l'aide de virus le plus grand nombre possible d'ordinateurs afin d'en prendre le contrôle à distance.

En plus de porter le nom de botmaster, les cybercriminels qui prennent le contrôle de ces ordinateurs sont aussi connus sous le nom de *bot herder* et d'*opérateur de botnet* (Krebs, 2006a). Pour infecter des ordinateurs, les botmasters utilisent plusieurs techniques (Boyd, 2008; Banday et al., 2009; Rossow et al., 2009). La voie la plus facile est d'infecter un site web (ou d'en créer un) et d'attaquer les ordinateurs des visiteurs. Le seul fait d'afficher un site web peut permettre à un criminel de prendre le contrôle de l'ordinateur qui le visite et ainsi de le transformer en *zombie*[4]. Infecter un site populaire permet de rejoindre un grand nombre de cibles sans avoir à les amener d'une manière détournée à visiter un site web créé par le criminel. L'autre alternative est d'utiliser les zombies afin de balayer l'internet à la recherche de systèmes vulnérables. Rares sont les utilisateurs qui mettent à jour régulièrement leurs signatures de logiciels antivirus et les systèmes d'exploitation. L'internet offre donc une quantité importante d'ordinateurs dont le botmaster peut tirer avantage. Une fois l'ordinateur

[4] *Zombie* est le terme utilisé pour décrire un ordinateur faisant partie d'un botnet.

compromis, celui-ci peut alors tenter de compromettre les autres ordinateurs sur son réseau local et ensuite se lancer sur l'internet à la recherche d'autres cibles. Dans le même ordre d'idée, les botnets se propagent aussi à l'aide de clés USB ou de fichiers joints dans des courriels. Le modus operandi est toujours le même : trouver une vulnérabilité et l'exploiter.

Une fois l'ordinateur compromis, l'opérateur installe alors le logiciel du botnet à proprement parler (Rossow et al., 2009). Ce logiciel remplit trois fonctions : permettre au botmaster de prendre le contrôle à distance de l'ordinateur, communiquer avec le botmaster et mettre en application les commandes du botmaster. La communication entre les zombies et l'opérateur de botnet pose plusieurs problèmes logistiques. Il n'est pas rare aujourd'hui de découvrir des botnets qui comptent plusieurs centaines de milliers d'ordinateurs zombies (Dunham et al., 2008). Transmettre rapidement et efficacement des instructions à un si grand nombre de machines est extrêmement difficile. Par ailleurs, ces communications se doivent d'être aussi discrètes que possible, car les chercheurs et les services de police surveillent activement l'internet afin de détecter les opérateurs de botnet. Les botmasters doivent aussi se méfier des autres criminels. Ceux-ci tentent régulièrement de prendre le contrôle des réseaux de zombies de concurrents afin d'augmenter leur propre botnet à faible coût. Certains chercheurs affirment qu'une guerre ouverte s'est créée entre certains botmasters (Doctorow, 2007). Devant évoluer dans un environnement si hostile, les botmasters ont grandement raffiné leurs méthodes de communication (Zhu et al., 2008).

La première méthode utilisée par les opérateurs de botnet était la chambre IRC (Patil, 2009). Celle-ci est d'ailleurs encore aujourd'hui la plus utilisée en raison de sa simplicité et de son efficacité. Dans ce type d'infrastructure, tous les zombies se connectent à une chambre IRC prédéfinie et attendent de recevoir des instructions de la part du botmaster. Cette chambre est connue sous l'appellation de centre de contrôle et de commande (C&C ou C2). Cette méthode permet de séparer les zombies entre plusieurs chambres et donc de limiter les pertes si une chambre devait disparaître. Elle permet aussi de distribuer des tâches différentes à des sections du botnet. Il existe aujourd'hui plusieurs logiciels clés en mai qui permettent à un utilisateur novice de monter un botnet sans avoir de connaissances en informatique (Krebs, 2011b). Une interface graphique de base permet au criminel de configurer le botnet qui sera géré à partir de la chambre IRC (Agobot, SDBot, phpBot, GT Bot). Ce type de logiciel adopte

généralement cette infrastructure et cela contribue à la popularité des botnets contrôlés par des chambres IRC. Cette infrastructure offre par contre un point de défaillance unique. Une fois la chambre de C&C connue, il est possible de prendre le contrôle des ordinateurs compromis en leur donnant comme instruction de télécharger un nouveau logiciel de contrôle.

Pour cette raison, les botmasters ont commencé à communiquer avec leurs zombies à l'aide de serveurs web (Lee et al., 2008; Borgaonkar, 2010). Au lieu d'utiliser une chambre IRC comme C&C, les opérateurs de botnet créent des pages web auxquelles les zombies se connectent ponctuellement pour prendre connaissance des dernières instructions. Contrairement à la première méthode, le botmaster ne peut donner d'ordre en temps réel aux zombies. Il doit plutôt attendre que ceux-ci se connectent au serveur pour leur transférer ses commandes. Plusieurs variantes de ce type d'infrastructure existent. Les plus évoluées sont à la fine pointe de la technologie (Nazario & Holz, 2008) et :

- chiffrent toutes leurs communications, empêchant les tiers d'épier les instructions ou les fichiers échangés entre les botmasters et les zombies;
- utilisent des relais intermédiaires (proxys) entre le zombie et le C&C. L'ordinateur infecté ne connaît donc jamais la véritable adresse du serveur contenant les instructions;
- créent des noms de domaines qui pointent vers des centaines d'ordinateurs (réseau à flux rapide). Le zombie qui se connecte à ce nom de domaine est redirigé au hasard vers l'un ou l'autre de ces ordinateurs. L'ingéniosité des pirates vient du fait que la quasi-totalité de ces ordinateurs ne sont que des leurres. Le zombie va donc essayer de se connecter au nom de domaine jusqu'à ce qu'il arrive, par chance, au vrai serveur et non à un ordinateur qui sert de leurre. Afin de rendre le processus encore plus opaque, la liste des ordinateurs associés à un nom de domaine peut être mise à jour toutes les trois minutes rendant presque impossible la détection du C&C.

Ces trois variantes peuvent être combinées pour créer des botnets opaques qui échappent aux systèmes de détection les plus évolués. Si les botmasters prennent autant de soin pour se camoufler, c'est en raison de la grande rentabilité des botnets (Krebs, 2006b). Les botmasters utilisent rarement leurs zombies à des fins personnelles. Ils vont plutôt vendre les services de leurs botnets sur des forums spécialisés (Thomas & Martin, 2006). Les acheteurs

dans ce marché recherchent des botnets pour leur efficacité à : 1) envoyer du pourriel; 2) faire des attaques distribuées de déni de service; 3) voler de l'information et; 4) faire de la fraude par clic (Boyd, 2008; Gutmann, 2007; de Oliveira, 2008; Mielke et al., 2008).

Les botnets permettent d'envoyer de grandes quantités de pourriels en répartissant l'envoi sur des milliers de machines. Cela permet de passer sous le radar des filtres qui se basent sur le nombre de messages envoyés et des listes d'adresses IP bannies pour empêcher le pourriel de se rendre à destination. Si une machine est inscrite à une liste noire, elle est tout simplement remplacée par une autre. Ces pourriels servent habituellement à répandre des virus (et augmenter ainsi la taille du botnet) ou encore à vendre des produits illicites comme des médicaments. Les attaques distribuées de déni de service sont des attaques coordonnées par des milliers de machines. Celles-ci envoient simultanément des demandes de connexion à un même ordinateur qui est alors inondé de demandes et ne peut répondre aux demandes tant légitimes qu'illégitimes. Il ne peut donc plus remplir les services pour lesquels il a été créé. Ce type d'attaque est utilisé pour se venger, nuire à un compétiteur ou encore faire de l'extorsion. Dans ce dernier cas, les cybercriminels demandent une rançon à défaut de quoi ils rendront inatteignable le site web d'une compagnie. Ce stratagème est particulièrement utilisé les jours de grands tournois sportifs alors que les sites de pari en ligne font des affaires en or. La plupart des logiciels de botnet surveillent les ordinateurs et les réseaux sur lesquels ils sont installés. Ils utilisent des enregistreurs de touches pour enregistrer les actions des utilisateurs et analysent le contenu des messages pour y dénicher des informations personnelles, des numéros de carte de crédit, etc. Certains botnets vont activement rechercher des informations particulières comme des secrets d'entreprise. Les botnets excellent finalement à la fraude par clic. Dans un tel scénario, des milliers d'ordinateurs visitent un site web qui génère des revenus à l'aide de publicités. Les compagnies paient en croyant que des clients potentiels ont vu leur annonce alors qu'en fait il ne s'agissait que de robots.

Avec autant d'informations sur les activités et la nature des botnets, il est surprenant de constater l'absence de connaissances sur les botmasters. Aucune étude scientifique n'a réussi à ce jour à dresser le portrait des opérateurs de botnet. Quelques journalistes ont publié des entrevues avec certains d'entre eux (Krebs, 2006a; Krebs, 2010b). Cet échantillon très limité contient des hommes âgés de 16 et 30 ans habitant un peu partout à travers le monde. Ils ont

des capacités techniques assez limitées et doivent utiliser des logiciels de botnet clé en main pour prendre le contrôle d'ordinateurs. Les revenus estimés de ces cybercriminels sont relativement importants avec des recettes mensuelles allant de 6 800 $ à 22 000 $. La motivation derrière leurs crimes serait donc exclusivement monétaire. Étant donné le caractère anecdotique de ces informations, il faut évidemment éviter de les généraliser à tous les opérateurs de botnet.

Il n'existe à notre connaissance aucune législation qui ait criminalisé le fait de contrôler un botnet. Cependant, au travers de leurs activités, les botmasters commettent plusieurs actes qui sont illégaux dans bien des juridictions. Il est premièrement très douteux que les botmasters remplissent des déclarations de revenus déclarant les revenus qu'ils tirent de leurs botnets. Ils commettent donc, dans le meilleur des cas, des fraudes fiscales. Par ailleurs, accéder à et prendre le contrôle de systèmes informatiques est une infraction criminelle dans la plupart des pays occidentaux. L'utilisation qu'ils font de ces systèmes est aussi criminalisée dans la plupart des juridictions qui se sont dotées de lois contre les pourriels et les attaques informatiques. Le fait de louer ou de mettre en location un botnet n'est pas illégal en soi – mais tout ce qui vient autour l'est.

Les botmasters qui créent eux-mêmes leur logiciel de botnet sont très rares. La plupart utilisent des forums de discussion et des chambres IRC pour acheter le logiciel leur permettant de créer, développer et contrôler leur botnet. Les versions les plus populaires ces dernières années sont Zeus et SpyEye (Krebs, 2011b). Tout dépendant des fonctionnalités requises (prendre le contrôle de la dernière version de Windows, finesse du contrôle sur les robots, etc.), un tel logiciel se vend entre quelques centaines de dollars et quelques milliers de dollars. Ce sont dans ces mêmes forums et chambres IRC que les opérateurs de botnet vendent les services de leurs réseaux d'ordinateurs infectés. Ces cybercriminels affichent publiquement le prix de location de leur botnet et négocient les ententes à l'aide de messages privés (Thomas & Martin, 2006). Ils recherchent avant tout des clients à long terme pour réduire les coûts de transaction. Les paiements se font à l'aide de monnaies virtuelles ou encore de bureaux de transfert de fonds comme Western Union. Les paiements en monnaie virtuelles sont excessivement difficiles à retracer et suivre car les transactions sont souvent anonymes. Dans le cas des bitcoins par exemple, chaque individu n'est connu que par son identifiant qui n'a

jamais besoin d'être associé à une identité réelle. Les bitcoins peuvent être conservés pendant des années avant d'être utilisé ou encore passer à travers des services d'échange de bitcoins qui permettent de camoufler l'identité de son détenteur. Ce genre de service récolte en effet l'argent de plusieurs individus et échange aléatoirement les numéros de série avant de rendre un montant équivalent – une façon rapide et pratique de blanchir ses bitcoins. Ce processus est facilité par le fait qu'il n'existe aucune autorité légale pour superviser ces monnaies. Elles sont complètement décentralisées et sont gérées par la communauté. Toute tentative de contrôle serait donc impossible. Même dans les cas où de l'argent réel est utilisé pour payer les services, il est éminemment difficile de retracer la véritable identité des criminels. En effet, ceux-ci font souvent transiter les paiements à travers le compte de mules qui n'ont aucune idée de la provenance ou de la destination des fonds (Birk et al., 2007). Les mules sont recrutées à travers de petites annonces offrant du travail à la maison et ne réalisent souvent pas qu'ils sont l'instrument de cybercriminels. Ils acceptent de recevoir des transferts dans leur compte puis de transférer l'argent à une tierce personne tout en conservant une commission. Dans d'autres cas, des scénarios plus risqués : un criminel peut ainsi acheter un bien sur un site de vente aux enchères comme eBay et faire transférer un trop grand montant au vendeur. Le criminel demande alors au vendeur de transférer le montant en trop dans un autre compte de banque, blanchissant l'argent au passage à travers le vendeur. Finalement, les compagnies de transfert d'argent comme Western Union sont reconnus pour fermer les yeux sur de possibles fraudes et laisser leur franchisés agir à leur guise. L'argent sale transféré étant une source d'importantes commissions, les compagnies de transfert n'ont tout simplement aucun avantage à augmenter les restrictions mises en place sur les transferts et les contrôles d'identité. Des ententes pour éviter des poursuites au niveau criminel qui ont couté des centaines de millions de dollars à ces compagnies pourraient cependant modifier leurs habitudes dans le futur (Holstege. 2010).

Pour se défendre contre la menace des botnets, les chercheurs ont proposé plusieurs scénarios (Li et al., 2009; Li et al., 2010; Ford et al., 2006; Stone-Gross et al., 2011). Dans la majorité des cas, la meilleure solution est de prendre le contrôle du C&C afin d'empêcher le botmaster de donner des instructions à ses zombies. Cela se fait traditionnellement en infectant volontairement une machine pour ensuite utiliser l'information générée par la machine compromise pour localiser le C&C et en prendre le contrôle. L'autre technique suggérée dans

la littérature est celle de l'interférence. Celle-ci peut se faire à plusieurs niveaux. Les chercheurs peuvent tenter de créer un grand nombre de faux zombies dans un même botnet. Ceux-ci feront semblant d'être sous le contrôle du botmaster, mais ne répondront pas à ses instructions. L'opérateur de botnet aura donc un réseau d'ordinateurs très peu efficace et impossible à louer en raison de l'imprévisibilité des résultats. L'interférence peut aussi s'appliquer au niveau du marché en tentant d'augmenter la méfiance entre les différents acteurs. En augmentant les coûts de transaction, le nombre de transactions devrait alors diminuer. Étonnamment, seulement une recherche s'est intéressée à la manière d'identifier les botmasters afin de s'attaquer à eux et non à leurs réseaux (Mielke et al., 2008). Leurs résultats offrent une technique qui permet d'identifier les opérateurs de botnet à l'aide de journaux de chambre IRC. Les techniques de défense s'orientent donc davantage vers une mitigation des conséquences plutôt que des causes de la présence des botnets.

Bien qu'intéressante, les connaissances actuelles sur les botnets sont limitées sous trois aspects. Premièrement, les chercheurs se concentrent particulièrement sur des aspects très techniques comme le fonctionnement des réseaux de communication ou encore les méthodes d'infection. Les botmasters sont mentionnés au passage, mais personne ne semble véritablement s'intéresser à eux. Cette méconnaissance permet aux botmasters de persévérer dans leurs activités illicites. Même si les connaissances actuelles permettent de mettre hors d'usage leur botnet, ils disposeront toujours de leur liberté et de leurs outils pour rebâtir un nouveau réseau de zombies. Par ailleurs, les chercheurs ne s'intéressent pas aux marchés qui permettent aux botmasters d'acheter leurs logiciels de contrôle et de vendre leurs services. Encore une fois, ces criminels profitent d'une certaine inattention de leurs conduites illicites. Deuxièmement, la recherche actuelle manque aussi de valeur prédictive. Les chercheurs sont toujours en mode réactif face à l'évolution du problème et il manque toujours un portrait général de la problématique des botnets. L'analyse des tendances permettrait de comprendre où nous en sommes et les chemins que pourraient prendre les botmasters à l'avenir. Au lieu de devoir éternellement bâtir de fausses victimes et d'analyser les ordinateurs infectés, les chercheurs pourraient alors monter des techniques de prévention au lieu d'être toujours à la traîne des cybercriminels. Finalement, la méthodologie et les questions admissibles sont différentes d'étude en étude. Il devient alors très difficile de standardiser les résultats et de les

comparer. Les nombreuses études de cas ne s'intéressent pas toujours aux mêmes caractéristiques. Ce ne sont pas non plus tous les aspects techniques qui sont examinés et des comparaisons deviennent alors très difficiles.

2.3 Le carding

La scène des warez a attiré une bonne partie de l'attention médiatique tournant autour des cybercrimes durant les années 2000. Plus récemment, une nouvelle menace semble avoir remplacé la scène des warez dans l'imaginaire populaire : le carding. Le *carding* est défini comme l'utilisation non autorisée d'informations financières à des fins frauduleuses (Peretti, 2008: p.6). Les personnes impliquées dans de telles activités sont connues dans la communauté des pirates sous le nom de *cardeurs*. Ces individus peuvent être impliqués soit dans le trafic et l'exploitation des données financières volées (DIBR, 2010; Goudey, 2004) soit dans la validation et la monétisation des données financières volées (ACC, 2011: p.5).

Comme démontré par Cornish (1994) dans son étude des scripts criminels, les activités criminelles doivent respecter un certain scénario, à l'image d'une pièce de théâtre. Les cambrioleurs, par exemple, doivent d'abord bâtir des relations avec des receleurs afin d'écouler la marchandise qu'ils vont voler. Les voleurs de voitures, eux, ont besoin de contacts en mesure de leur fournir les outils spécialisés nécessaires à leur métier. Les cardeurs fonctionnent de la même façon que ces criminels et ont besoin de tisser des liens avec de multiples professionnels qui peuvent leur fournir les outils et l'expertise qu'ils recherchent. En Europe occidentale et orientale, ces relations d'affaires se forment souvent sur internet à travers des forums en ligne. Les cardeurs peuvent s'y rencontrer virtuellement, partager leurs connaissances et de s'engager dans des transactions commerciales illégales.

La figure 3 montre un message typique d'un forum de carding. Ici, un utilisateur du nom de M. Crooks offre de fausses cartes d'identité et de crédit. Les forums de carding les plus importants ont des dizaines de milliers de sujets de discussion contenant chacun des dizaines voire des centaines de messages. Cet accès direct aux fournisseurs et revendeurs de cartes de crédit et d'informations bancaires permet aux cardeurs d'échanger instantanément des informations et de transformer des données financières volées en argent liquide.

Figure 1 : Message de cardeur dans un forum de discussion

2.3.1 Comment les cardeurs volent, vendent et utilisent les informations financières volées

Les chercheurs s'intéressent de plus en plus à ce qu'ils appellent l'économie souterraine. Cárdenas et al. (2009) comparent cette économie souterraine à un écosystème qui dispose d'un large éventail d'acteurs tels que des experts en sécurité, des distributeurs de logiciels malveillants (*malware*), des botmasters, des fournisseurs d'accès à l'internet frauduleux, des compagnies d'hébergement de sites web et des mules d'argent. Chacun de ces groupes a une fonction spécifique et vend des biens et services à l'image de l'économie légale. Il existe, dans cette économie souterraine, une forte division du travail. Par exemple, les auteurs de logiciels malveillants hésitent généralement à utiliser eux-mêmes leurs créations et préfèrent les vendre à d'autres qui sont disposés à les lancer sur l'internet. Les forums en ligne sont des outils efficaces pour gérer les relations de tous ces acteurs, car ils augmentent la communication et l'accès aux ressources criminelles.

Le processus du carding plus spécifiquement est lui-même divisé en quatre phases ou étapes de développement: la production de logiciels malveillants, la distribution de logiciels malveillants et le vol de données financières, le recel et finalement la monétisation. Au début de la chaîne, les auteurs de logiciels malveillants sont les individus qui développent les virus qui permettent de voler des informations de cartes de crédit et de débit. De nos jours, une portion importante des logiciels malveillants qui sont développés tourne autour de cette activité de collecte illégale d'informations financières. Pour mettre au point ces logiciels malveillants, les auteurs peuvent soit acheter des vulnérabilités sur les marchés gris ou noirs,

ou encore trouver les leurs. Une fois complétés, les logiciels malveillants sont habituellement vendus à des distributeurs.

Ceux-ci entrent en action dans la seconde phase du processus qui vise à faire télécharger les logiciels malveillants sur autant de systèmes informatiques que possible. Plusieurs techniques sont utilisées pour y arriver. Dans le cas de *drive-by downloads*, les internautes sont attirés vers des sites Web compromis en utilisant des appâts (ex.: un lien vers une vidéo drôle ou séduisante sur Facebook). Lorsqu'un utilisateur visite le site, son ordinateur est automatiquement infecté par un logiciel malveillant sans aucune action de sa part. Dans le cas des vers, les logiciels malveillants prennent le contrôle d'un ordinateur à distance en tirant parti d'une vulnérabilité dans un logiciel ou un système d'exploitation. L'attaquant prend alors le contrôle total de la machine infectée et est en mesure de surveiller le comportement de son utilisateur. Les informations bancaires sont captées et copiées dans un fichier qui est acheminé aux distributeurs de logiciels malveillants.

Ces cybercriminels n'ont pas l'habitude de monétiser directement l'information financière qu'ils recueillent. Cela nous amène à la troisième étape, le recel. Les données recueillies par les distributeurs de logiciels malveillants sont vendues à des grossistes ou à de petits cardeurs. Les forums en ligne servent de marchés où les distributeurs de logiciels malveillants peuvent rencontrer des grossistes et des cardeurs.

Pour monétiser les données, certains cardeurs font de fausses cartes de crédit en plastique pour acheter des marchandises dans des magasins (Sullivan, 2010: p.8). Tout l'équipement et l'expertise nécessaires pour ce type d'opération peuvent être trouvés facilement dans les forums de carding (Poulsen, 2011). D'autres cardeurs préfèrent passer leurs commandes sur des sites de commerce en ligne pour commander des biens et des services. L'authentification sur ces sites est minime et ne nécessite que quelques informations qui sont souvent vendues avec les données de la carte elle-même (Prabowo, 2011: p.376). Les cardeurs les plus sophistiqués louent les services de personnes connues sous le nom de mules à qui ils envoient des transferts d'argent ou encore des produits achetés en ligne. Ces mules transmettent alors les biens ou l'argent à d'autres complices qui revendent les produits ou vont retirer l'argent en personne. Chaque mule est payée un pourcentage ou un taux fixe pour son

travail. Les cardeurs avec de faux papiers d'identification peuvent finalement également louer des cases postales où les articles achetés en ligne peuvent être envoyés par la poste, supprimant ainsi la nécessité de recruter des mules (Peretti, 2008: p.14).

Les forums en ligne sont des lieux parfaits pour ce type de transactions puisque les vendeurs et les acheteurs peuvent afficher ce qu'ils ont ou recherchent et trouver facilement un partenaire d'affaires (Peretti, 2008: p.14; Holt & Lampke, 2010: p.42). Les individus à la fin de la chaîne ne possèdent souvent que des capacités techniques limitées, car leur expertise est dans la monétisation des informations financières. À l'inverse, les individus au début de la chaîne n'ont souvent que peu de moyens pour transformer les informations qu'ils volent en argent liquide.

2.3.2 La taille et l'impact du carding

La question de la taille et de l'impact financier du carding sur l'économie légale est encore largement débattue tant dans la recherche académique que dans les rapports de spécialistes (Erbschloe, 2010; Kshetri, 2010). Holt et Lampke (2010) ont utilisé des messages de vendeurs d'information pour estimer la taille de la scène du carding, mais n'arrivent qu'à des résultats très approximatifs. En effet, comme il est impossible de connaître la proportion des informations offertes qui sont vendues, un chiffre d'affaires total ne peut être calculé. Holz et al. (2009) ont quant à eux utilisé la quantité de données volées comme outil d'approximation de la taille et l'impact, mais encore une fois, il n'existe aucune certitude qu'une information volée sera utilisée à de mauvaises fins. Finalement, plusieurs rapports corporatifs ont été produits sur le sujet, mais on ne peut que douter de leur fiabilité, car ils représentent des intérêts économiques qui ont tout intérêt à gonfler la menace du carding (Wall, 2007).

Malgré tout, l'estimation annuelle des pertes dues à la fraude sur des cartes de crédit émises au Royaume-Uni a atteint 574 millions de dollars US en 2010 (UK Cards Association, 2012: p.19). Ce chiffre est en nette baisse par rapport aux estimés précédents. Plus de 60 % des pertes sont le résultat d'achats en ligne, une tendance à la hausse sur une période de cinq ans. Sullivan (2010: p.11-12) estime qu'en 2006, les pertes reliées aux cartes de paiement étaient plus élevées aux États-Unis qu'au Royaume-Uni, en Australie, en Espagne et en

France. Il explique ces différences par les différentes technologies utilisées, les normes de sécurité et les types de paiements.

Verizon publie chaque année son propre rapport en lien avec ses données d'enquête (DBIR, 2011). Ces études sont principalement basées sur l'expérience personnelle des employés de Verizon et d'enquêtes menées conjointement avec les services secrets américains. Selon ce rapport, la scène du carding a considérablement changé depuis 2010. Le nombre de vols a atteint de nouveaux sommets, mais chaque vol a donné lieu à un nombre plus limité d'informations compromises. Le rapport suggère que l'attention portée à ce genre de fraude et la condamnation récente de cybercriminels de grande envergure ont eu un impact positif sur la réduction de la taille de l'économie souterraine. La dernière DBIR a également montré que 96 % des vols visaient des cartes de paiement. Ces vols étaient toutefois plus petits, entraînant un déclin dans le volume d'informations financières qui sont négociées illégalement. Étant donné la faiblesse actuelle du marché, Verizon estime par ailleurs que plusieurs joueurs pourraient attendre patiemment que le prix des informations volées remonte pour revenir sur le marché. (DBIR, 2011: p.48-50).

2.3.3 La scène du carding

Les analyses empiriques montrent que les données financières sont l'un des produits les plus échangés sur le marché noir en ligne (Franklin et al., 2007; Holt & Lampke, 2010; Holz et al., 2009 : p.11). Les premières études empiriques sur le carding se sont concentrées sur les marchés noirs d'IRC. Franklin et al. (2007) ont collecté de grandes quantités de conversations et ont analysé les biens et services offerts ainsi que les stratégies qui pourraient être développés pour interférer avec ces marchés. Ils ont constaté que la loi de l'offre et de la demande s'applique aussi à l'économie souterraine. Par conséquent, en surveillant les fluctuations de prix, il serait possible de connaître la taille actuelle de la scène. Pour interférer avec de tels marchés, Franklin et al. (2007) suggèrent d'utiliser une attaque à la Sybil qui implique la création de fausses identités et la manipulation des liens de confiance entre les participants. Fallmann et al. (2010) ont pour leur part développé un système automatique de surveillance de plusieurs canaux IRC et de forums en ligne. Ce système de surveillance a recueilli plus de 43 millions de messages de clavardage et environ un million de messages sur des forums. Les chercheurs ont constaté que les forums souterrains étaient utilisés

principalement pour le partage de connaissances, mais qu'une partie d'entre eux contenait également une section réservée aux transactions illégales. Ils ont également remarqué que le faible ratio de messages par utilisateur tendait à indiquer que les forums avaient de la difficulté à contrôler les pourriels. Franklin et al. (2007) et Fallmann et al. (2010) s'entendent tous deux pour dire que les marchés noirs sur IRC sont un terrain fertile pour les transactions illicites. Ce n'est pas le cas de tous les chercheurs cependant. Herley et Florêncio (2009) ont plutôt conclu que les marchés en ligne, en particulier ceux sur les canaux IRC, comportent trop de risques pour être d'intéressants marchés. Ils ont également fait valoir que la taille des marchés IRC serait exagérée. Finalement, les salles de clavardage seraient principalement fréquentées par des utilisateurs novices qui seraient des proies faciles pour les professionnels du milieu.

La recherche sur le carding s'est également intéressée aux structures sociales des marchés de forums en ligne. Holt et Lampke (2010) ont utilisé des méthodes qualitatives pour décrire les relations entre les acteurs du marché. Les vendeurs ayant les meilleurs produits et les plus recherchés accapareraient la plus grande part de marché, mais personne ne paierait pour la valeur réelle de l'information volée. Holt et Lampke (2010) ont également détecté le problème de victimisation des criminels par leurs pairs. Pour éviter de tels problèmes, les administrateurs de forums recommandent d'utiliser des services de dépôt fiduciaire lorsqu'une transaction implique un membre non validé. Les administrateurs ont également mis en place un système de rétroaction où les notes négatives nuisent grandement à la performance des cardeurs. Ces systèmes se sont avérés relativement efficaces pour prévenir la victimisation. Les vendeurs se doivent de surveiller attentivement leur réputation en ligne et même d'avertir leurs clients quand ils doivent partir en vacances.

Enfin, Yip (2011) a suggéré que l'analyse des réseaux sociaux pourrait être appliquée à l'analyse de l'économie souterraine. Il a analysé la structure de ligne des marchés noirs dans différentes zones géographiques et a reconnu l'importance de l'aspect social de la cybercriminalité organisée. Selon Yip (2011), les plates-formes de communication diffèrent entre les cardeurs occidentaux et chinois. Les forums fermés et hiérarchisés seraient fréquents en Occident alors qu'en Chine, l'offre de biens et services serait séparée des transactions elles-mêmes. Les offres seraient habituellement affichées dans des sites accessibles au public alors que les transactions seraient négociées par des intermédiaires autonomes et anonymes à l'aide

de services de messagerie privés et de messagerie instantanée. Malgré ces différences, le but de tous les marchés noirs serait d'obtenir des avantages économiques et d'améliorer sa réussite par son réseau social.

2.4 Conclusion

Ces trois formes particulières de cybercrimes partagent plusieurs aspects. Tout d'abord, elles ont toutes recours à une division du travail très marquée entre des individus plus ou moins reliés. Dans le cas de la scène des warez, les criminels se sont regroupés en clans officiels qui se séparent les tâches entre eux afin d'arriver à distribuer illégalement le plus de propriétés intellectuelles possible. La réalité est quelque peu différente pour les cardeurs et les botmasters qui évoluent plutôt dans un écosystème complexe où des créateurs de code malveillant, des distributeurs et des fraudeurs se côtoient. Ceux-ci se doivent par contre de travailler en étroite collaboration, car leur spécialité ne leur permet pas de remplir un script criminel à eux seuls.

Alors que la reconnaissance apparaît comme la motivation principale chez les pirates du warez, les deux autres types de criminels ont des objectifs strictement monétaires. La littérature indique qu'ils agissent à l'image d'entrepreneurs et qu'ils gèrent donc l'équivalent d'une petite ou moyenne entreprise de biens et services. Dans ce contexte, les relations interpersonnelles deviennent excessivement importantes afin d'augmenter les parts de marché et fidéliser la clientèle. Nous verrons à ce sujet dans le deuxième article de cette thèse que les individus qui se présentent sous un jour favorable à l'aide messages positifs ont un avantage marqué sur les autres qui ont de la difficulté à rester positifs.

Il est finalement étonnant de voir le nombre de similitudes entre le monde légitime et illégitime qui transpire de cette brève revue de littérature. Nous mentionnons dans le paragraphe précédent que les criminels adoptaient les comportements d'entrepreneurs licites. Cela transparaît dans leur tendance à l'autopromotion. Les criminels doivent en effet se démarquer des autres et tentent d'attirer l'attention par des offres sensationnelles ou des garanties sur les produits. Le troisième article de la thèse introduira la notion de prise de risque et démontrera que les criminels sont particulièrement propices à adopter de tels

comportements. Tout comme dans le monde légitime, le taux d'échec des entreprises criminelles est assez élevé. Plus de détails viendront sur le sujet dans nos propres recherches, mais la réussite criminelle semble être un objectif difficile à atteindre pour bien des participants à cette communauté.

Le centre d'intérêt de cette thèse tourne exactement autour de ces questions qui semblent relier le monde légitime au monde illégitime. Nous avons en effet soulevé plusieurs lacunes dans les connaissances actuelles dans ce chapitre et il est frappant de constater à quel point nous en savons beaucoup sur la façon de commettre des crimes, mais beaucoup moins sur les personnes qui les commettent tout comme sur les caractéristiques qui permettent à certains individus de se démarquer des autres. Nous expliquerons plus en détail l'importance de ces questions pour la criminologie en général, mais il nous apparaît important pour le moment de souligner que cette performance criminelle devrait en toute logique être associée de près au maintien dans une vie de crime et à un haut taux de récidive. Il est en effet assez rarissime de voir un homme d'affaires qui multiplie les profits à la bourse changer soudainement de carrière. Si tel que nous le supposons les mondes légitimes et illégitimes ne sont pas si différents l'un de l'autre, il pourrait alors être payant pour les chercheurs qui s'intéressent à une nouvelle question en criminologie d'étudier les connaissances sur le sujet dans d'autres milieux afin d'évaluer la pertinence d'importer des façons de faire et des modèles conceptuels dans leur domaine. Cette approche mixte gagne de plus en plus d'intérêt dans les cercles de recherche, et ce, avec raison. Le troisième chapitre appliquera cette méthodologie et abordera la question de la réputation tant dans le contexte légitime qu'illégitime. La littérature sur le sujet de la performance est unanime sur l'importance pour les acteurs de développer une bonne réputation. Le troisième chapitre viendra confirmer cette proposition et démontrera comment le concept de réputation pourrait et devrait s'appliquer à la notion de réussite dans le contexte criminel.

CHAPITRE 3 – LA RÉPUTATION

La notion de réputation est apparue à quelques reprises déjà dans les deux premiers chapitres de cette thèse. Nous avons bien évidemment souligné son rôle de motivateur dans le contexte de la scène des warez (Craig, 2005). La réputation est aussi ressortie dans d'autres discussions incluant celle sur les relations interpersonnelles. Nous avons ainsi vu que la réputation se développait sur le long terme au gré des interactions entre individus. Tant les relations d'affaires que la participation à des forums de discussion contribuaient à la réputation d'un individu. Cette réputation était essentielle pour augmenter la fluidité des marchés illicites. Étant donné le manque de contrôles dans ces environnements, il est extrêmement difficile de connaître les vraies intentions des autres acteurs et de prédire l'apparition de comportements opportunistes. La réputation est un des rares signaux que les criminels peuvent utiliser pour juger de la qualité des partenaires. Holt & Lampke (2010) soulignent tous les efforts que les pirates font pour maintenir et augmenter leur niveau de réputation. Ceux-ci vont même jusqu'à prendre le temps d'avertir leurs clients potentiels qu'ils seront absents pour quelques heures. Comme la méfiance est toujours élevée dans les marchés illicites, une absence même temporaire pourrait inquiéter et alimenter de fausses rumeurs.

Ce portrait de la réputation tirée de la littérature criminologique est des plus fragmentaires. Nous tenterons dans le présent chapitre de remédier à cette lacune et de développer une compréhension criminologique du phénomène en utilisant toutes les sources d'informations possibles. Nous verrons que plusieurs analogies peuvent être tracées entre les marchés licites et illicites et que la réputation est un rouage important du monde des affaires, que celles-ci soient légales ou non.

3.1 Définitions

La réputation est un concept flou qui est souvent associé à l'idée de confiance dans le langage populaire. Jøsang et al. (2007 : p.5) définissent la réputation comme étant ce qui est "généralement dit ou cru à propos du caractère ou du statut d'une personne ou d'une chose". Cette image publique est le résultat des informations qui circulent dans les cercles sociaux associés à ces personnes ou ces choses. La réputation est donc une mesure de la perception et non de la réalité.

La confiance pour sa part est “l’évaluation subjective par un individu A de la probabilité qu’un individu B agisse d’une certaine manière alors que son bien-être en dépend “ (Jøsang et al., 2007: p.3). Cette définition repose sur deux concepts soit l’interdépendance de deux individus et la statistique probabiliste. Cette définition implique donc une analyse stratégique des risques et des bénéfices, mais repose sur une asymétrie d’informations où A ne peut prédire avec certitude le comportement de B. Le terme asymétrie d’information est régulièrement utilisé dans les recherches portant sur la réputation et la confiance et fait référence au manque d’informations sur l’une et/ou l’autre des parties impliquées dans une relation.

Souvent, la décision de donner ou non sa confiance est basée sur la réputation d’un individu. Une personne ayant la réputation d’être en mesure de dénicher des films avant leur sortie en salle sera plus à même de se faire recruter par un groupe de pirates du warez et obtiendra ainsi accès à leurs salles de clavardage privées ainsi qu’à leurs serveurs. Dans certains cas cependant, la confiance peut être accordée malgré la présence d’une mauvaise réputation. Dans ce scénario, la confiance est influencée par d’autres facteurs que la simple réputation. Nous pouvons penser ici à des expériences personnelles passées ou encore à des références externes. La réputation est donc un élément pesant dans la balance de la confiance et son poids varie énormément selon le contexte. Dans les contextes d’asymétries d’information exacerbées, l’importance de la réputation aura tendance à augmenter, car il s’agira d’un des rares facteurs permettant de prendre la décision d’accorder ou non sa confiance.

Il est important de différencier finalement le concept de reconnaissance de celui de réputation. La reconnaissance est un signal dirigé vers une entité (individu, groupe d’individus, entreprise, etc.) qui vise à souligner un trait ou une caractéristique de cette entité. La réputation étant l’image publique d’une entité, elle peut aussi être comprise comme étant la somme de toutes les reconnaissances reçues de la part des autres. Il se pourrait que dans certains cas la somme des parties soit plus grande que leur simple addition. Ainsi, certains effets d’interactions pourraient contribuer à faire augmenter ou diminuer plus rapidement la réputation d’une entité. Nous verrons dans cette thèse plusieurs exemples de ce type d’effet.

3.2 Le concept de réputation

Accorder sa confiance à quelqu'un fait nécessairement référence à la notion d'échanges. Homans (1958) s'intéresse à ce concept dans le contexte de petits groupes. Il affirme que chacun de nos comportements sociaux a des coûts et aussi des bénéfices. Plus un comportement est renforcé positivement (c'est-à-dire que plus les bénéfices sont importants), plus ce comportement aura tendance à se répéter dans le temps. Un équilibre naturel aura alors tendance à apparaître au niveau des coûts et des bénéfices. Un groupe d'individus qui offre beaucoup de bénéfices sera en droit d'exiger en échange un investissement (des coûts) important de chacun de ses membres. Les personnes déviantes ont tendance à recevoir, dans un premier temps, plus qu'elles ne donnent au groupe. Il s'agit ici d'un effort du groupe pour transformer la déviance en conformisme. Si ce déséquilibre perdure trop longtemps cependant, les bénéfices qui sont adjugés aux personnes déviantes vont décroître rapidement pour être réinvestis vers des membres plus productifs du groupe.

Homans (1958) applique cette théorie au monde du travail en examinant les relations d'entraide entre collègues. Dans un contexte professionnel, la personne la plus apte à nous aider lorsque nous rencontrons un obstacle est bien souvent notre supérieur immédiat. Comme cette personne est celle qui évalue la qualité de notre travail, nous ne pouvons constamment la déranger de peur qu'elle ne se fasse une image négative de nos capacités. Pour cette raison, les employés auront plutôt tendance à chercher de l'aide auprès de leurs collègues plutôt qu'auprès de leurs supérieurs. Chaque fois qu'ils sollicitent l'aide de quelqu'un, les employés reçoivent une information utile qui devient leur bénéfice. Ils doivent en échange sacrifier une certaine quantité d'amour-propre et reconnaître publiquement qu'ils sont inférieurs à la personne auprès de qui ils sollicitent de l'aide. À l'inverse, la personne qui sacrifie du temps en aidant son collègue (le coût) augmente sa réputation et la perception de ses compétences dans son milieu (le bénéfice). L'équilibre dans les échanges dont Homans (1958) parlait plus tôt se voit parfaitement dans ce type de relation. À la longue, certains individus seront plus sollicités que d'autres en raison de leur bonne réputation. S'enclenche alors un cercle vicieux dans lequel ces personnes accumulent de plus en plus de reconnaissance, mais perdent aussi de plus en plus de temps à aider les autres plutôt qu'à accomplir leur propre travail. Le coût pour échanger avec ces individus deviendra donc de plus en plus grand, car leur temps aura pris de

la valeur. Bien des partenaires passés seront alors tentés d'échanger des informations contre de la reconnaissance auprès de collègues moins réputés afin de limiter leurs coûts de transaction.

La théorie d'Homans (1958) nous permet de modéliser les comportements sociaux en tant qu'échanges de biens matériels et immatériels. Les personnes qui reçoivent beaucoup dans ces échanges seront sous pression pour eux-mêmes partager énormément avec les autres. Même si les profits sont difficiles à générer dans ce contexte, chaque personne tente malgré tout de tirer son épingle du jeu du mieux qu'elle le peut afin de s'élever au-dessus des autres. Les comportements auront tendance à rester stables lorsque les profits (bénéfices – coûts) sont élevés et à changer rapidement lorsque les profits seront faibles.

Cette vision de la reconnaissance en tant que monnaie d'échange a été reprise plus récemment par divers auteurs, dont Deephouse (2000) et Rao (2006) qui conceptualisent la notion de réputation comme une ressource qui peut procurer un avantage compétitif sur le long terme. Selon cette approche développée pour le monde des affaires, chaque entité a une quantité différente de ressources sur lesquelles elle peut compter. Certaines ressources sont tangibles (bâtiments, employés, produits) alors que d'autres sont immatérielles. Pour être considérée comme une ressource, une caractéristique d'une entité doit posséder quatre propriétés spécifiques: être précieuse, difficilement imitable, non substituable et rare.

Dans son texte, Deephouse (2000) démontre en quoi la réputation remplit ces critères et se doit d'être considérée comme une ressource. Son utilité provient de sa capacité à réduire le coût des biens et services achetés et à augmenter les marges de profits sur les ventes de produits et services. Une bonne réputation aura tendance à réduire les incertitudes associées à n'importe quelle transaction et diminuera ainsi les coûts. Parallèlement, des firmes qui possèdent une réputation sans taches, comme *Apple* dans le domaine de l'électronique, pourront se permettre d'exiger un prix de vente plus élevé que les autres sans crainte de perdre des clients. La réputation est aussi difficilement imitable, car elle nécessite une longue période de temps pour se bâtir et se propager dans une communauté. Une fois perdue, une réputation prend encore plus de temps à se rebâtir (Hall, 1992). De par cette longue période de gestation, il est donc très difficile d'imiter une bonne réputation selon Deephouse (2000). Pour clore le débat sur le sujet, celui-ci mentionne également qu'il est impossible d'acheter une réputation

(Caves, 1980) ou même de la truquer en raison de sa «nature complexe et sociale» (Deephouse, 2000: p1099).

La réputation n'est également pas substituable. Barney (1991) met en évidence le fait que les firmes cherchent souvent à améliorer leur réputation, tout en offrant des garanties et des contrats formels pour leurs produits et services. Dans tous les cas, ces techniques servent à rassurer les clients et les partenaires de la fiabilité de la firme. Comme ces trois approches sont utilisées en parallèle, Barney (1991) affirme que l'une ne peut remplacer l'autre, et qu'il n'existe donc pas de technique substituable à la réputation. Finalement, Deephouse (2000) conclut en notant que la réputation est rare, car elle n'est pas répartie également entre tous les participants d'un marché et qu'elle ne peut pas être générée quand et comme on le voudrait. Cette difficulté à produire une bonne réputation implique nécessairement que tous n'y auront pas un accès égal et qu'elle est donc rare par le fait même.

Rao (1994) a appliqué cette conceptualisation de la réputation en tant que ressource à une recherche portant sur les débuts de l'industrie automobile à la fin du 19^{e} siècle et au début du 20^{e} siècle. À cette époque, bien des acteurs s'opposaient à la légalisation de ce nouveau mode de transport. Des craintes au niveau des risques pour la population et de la qualité des produits étaient notamment soulevées. Pour contrer leurs opposants, les compagnies automobiles se sont alors inscrites à des courses, ce que Rao (1994) qualifie de tests sociaux. Ces évènements publics permettaient aux compagnies de démontrer hors de tout doute les caractéristiques et la qualité de leurs produits. Rao (1994) a démontré que les gagnants de ces épreuves accumulaient ainsi de la réputation, ce qui leur permettait de survivre statistiquement plus longtemps que leurs compétiteurs. Les grands journaux, souvent les promoteurs de tels évènements, s'assuraient de diffuser à un large public les résultats des concours. Dans ce contexte, acquérir une bonne réputation était difficile de par les défis technologiques imposés. Cette dernière était aussi difficilement imitable, car seuls les grands journaux avaient le pouvoir d'en faire la promotion. Elle était rare de par le faible nombre de firmes qui étaient en mesure de remporter des épreuves. Finalement, elle était non substituable, car elle était la variable ayant le plus d'impact sur la survie d'une entreprise. D'autres tests sociaux ont suivi ces premières courses comme les concours de certification organisés par l'industrie. Ceux-ci ont eu un impact et un mécanisme similaire aux courses automobiles.

Bien que cet exemple des débuts de l'automobile provienne d'une industrie aujourd'hui bien différente, l'argumentaire soutenant la modélisation de la réputation comme une ressource est ici claire et convaincante. La reconnaissance gagnée lors des courses et plus tard lors des concours de certification était l'élément majeur expliquant la survie des compagnies. Cette ressource représentait donc le salut des entreprises désireuses de se lancer dans ce domaine.

En théorie, la réputation apparait être une ressource illimitée. Rien n'empêche en effet une entité d'offrir de la reconnaissance à tous ses partenaires plutôt qu'un seul en particulier. Chaque entité peut donc générer à sa guise de la reconnaissance. Dans la pratique, la situation est beaucoup plus complexe. Tout d'abord, tel que décrit par Homans (1958), certains coûts sont associés au transfert de reconnaissance. Les émetteurs de la reconnaissance sacrifient une partie de leur image et les récepteurs sacrifient de leur temps et de leur énergie en échange. Dans les deux cas, ces ressources ne sont pas infinies et limitent donc artificiellement la quantité de reconnaissance disponible à tout moment. Par ailleurs, dans le cas de systèmes automatisés de reconnaissance de type eBay (voir plus bas pour plus de détails), des contraintes inhérentes aux systèmes existent. Dans certains cas par exemple, une interaction doit avoir lieu pour que de la reconnaissance soit transmise. Dans d'autres cas, chaque individu ne peut émettre de la reconnaissance qu'un certain nombre de fois par jour. Pour ces raisons, bien que la quantité de reconnaissance disponible soit souvent vaste et apparemment sans fin, certaines contraintes viennent circonscrire cette ressource qui devient en pratique limitée.

Si la réputation est une ressource, il est alors inévitable que des coûts et des bénéfices y soient rattachés. Nous avons déjà mentionné brièvement qu'une bonne réputation permettait de réduire les coûts des achats à cause de la faible incertitude entourant des transactions impliquant des entités aux réputations solides. Pour mieux comprendre ce jeu des vases communiquant, nous nous tournerons vers Akerlof (1970) qui fut le premier à introduire la notion de marché de citrons. Dans un tel marché de citrons, la qualité des biens est difficilement mesurable à l'avance. Un client ne peut donc départager les biens de qualité des biens de mauvaise qualité avant de payer. Les producteurs offrant un produit de qualité supérieure ne pourront trouver d'acheteurs en raison de l'incertitude et de l'asymétrie

d'information qui règnent sur le marché. Très rapidement, tous les biens devront être vendus au même prix qui sera nivelé par le bas en raison de la présence potentielle de mauvais produits. Cela poussera les producteurs de qualité à se retirer du marché et les consommateurs se retrouveront dans un marché de citrons, soit un marché où seulement des produits de qualité inférieure sont disponibles.

Pour sortir de ce cercle vicieux, les producteurs de qualité se doivent d'investir dans leurs produits et accepter de les vendre, au départ, au prix des produits de qualité inférieure (Shapiro, 1983). Ce faisant, ils se bâtiront une réputation positive auprès des consommateurs, mais devront assumer des pertes importantes. Cette stratégie a pour objectif d'envoyer un signal au marché témoignant de la confiance d'une entreprise en son produit. Cette confiance est démontrée par la volonté d'une compagnie de se maintenir dans un marché malgré les pertes. Au fur et à mesure que le message de la compagnie se propagera auprès des consommateurs, le prix de ses produits pourra graduellement augmenter pour refléter la qualité supérieure maintenant connue des produits (Shapiro, 1983). À long terme, une entreprise ayant investi dans des produits de qualité pourra donc se démarquer de ses compétiteurs et exiger un prix de vente plus élevé que les autres. Ce prix sera par ailleurs beaucoup plus élevé que ses coûts de production. Cette différence se justifie comme un retour sur l'investissement pour la compagnie. En effet, après avoir vécu une période de déficit servant à bâtir la réputation, l'entreprise peut maintenant récolter le fruit de ses efforts, soit des profits plus importants.

Dans un contexte où il n'est pas possible de bâtir une réputation, les entreprises auront tendance à agir de manière opportuniste avec les consommateurs (Shapiro, 1983). La meilleure stratégie dans cet environnement est de jouer sur le volume et de vendre autant de produits que possible en abusant de la faible confiance du marché. Dans ce scénario, les joueurs ne seront actifs que pour une période de temps limité avant de disparaître et de renaître sous un nouveau nom. Dans le cas des marchés où une réputation peut se développer, les firmes auront au contraire avantage à agir dans un mode de collaboration. Dans cette optique, le souci de produire des produits d'une qualité qui se maintient dans le temps sera le meilleur gage de succès. Le fait de conceptualiser la réputation comme une ressource nous permet alors, tel que Shapiro (1983) le fait, d'évaluer pour chaque marché une courbe des coûts et bénéfices et de

modéliser les investissements nécessaires pour bâtir une réputation et atteindre un niveau de profitabilité sur le long terme.

La réputation sera dans ce contexte un gage, pour les consommateurs, de la qualité persistante des produits. Les producteurs qui possèdent de vastes ressources de réputation ne voudront pas voir leur image ternie par des produits de seconde qualité. Cela aurait pour effet de diminuer le prix qu'ils sont en mesure d'exiger des consommateurs et affecterait leurs profits. Les gestionnaires d'entreprises peuvent il est vrai être tentés de couper leurs coûts de production afin d'augmenter leurs profits à court terme, mais cela aura un impact à long terme qui pourrait être beaucoup plus important. Pour que la réputation puisse avoir un effet positif, il faut donc que le retour sur l'investissement de la réputation soit plus important que les coûts d'investissement eux-mêmes (McDonald, 1999). Dans ce calcul, il faudra également tenir compte de la durée de vie des producteurs et de la capacité des producteurs à vendre faussement des produits de qualité alors qu'il s'agit de biens de faible qualité.

Plusieurs chercheurs ont suivi les recherches de Shapiro (1983) sur le sujet (Camerer & Weigelt, 1988; Raub & Weesie, 1990; McDonald, 1999; Roberts & Dowling, 2002). Plusieurs de ces recherches se basent sur la théorie du jeu (voir Camerer & Weigelt (1988) par exemple) afin de déterminer plus précisément les forces et les formules qui expliqueraient l'allocation optimale de ressources à investir dans une réputation. Ces recherches confirment sans équivoque l'importance de l'analyse stratégique dans la compréhension du phénomène de la réputation. Cette validation s'est faite à l'aide de tests de laboratoire comme dans le cas de Camerer & Weigelt (1988) et à l'aide de données empiriques (Roberts & Dowling, 2002). Dans ce deuxième cas, des données financières permettent d'établir avec précision que non seulement la réputation permet d'atteindre le seuil de profitabilité, mais que celle-ci permet même de dépasser la moyenne des profits d'entreprises similaires qui ont une réputation inférieure. La réputation permet par ailleurs une plus grande stabilité dans la santé financière des entreprises (Roberts & Dowling, 2002).

La réputation peut aussi amener d'autres bénéfices que la simple profitabilité. Milgrom & Roberts (1981) se sont intéressés à l'effet de la réputation sur la dissuasion et la prédation entre entreprises. La théorie veut que les comportements menant à l'atteinte d'un monopole

dans un marché (chute des prix, contrats d'exclusivité) soient en fait nocifs pour l'entreprise qui les instaure. En effet, de telles mesures sont souvent coûteuses pour la compagnie qui les adopte. Les compétiteurs peuvent accepter ces baisses en comprenant qu'elles ne sont que passagères. Il n'existe donc aucune garantie que de telles techniques fonctionnent malgré les coûts importants qu'elles entraînent. De plus, même si ces techniques devaient fonctionner et qu'une entreprise atteignait un certain niveau de monopole, celle-ci pourrait difficilement hausser ses prix pour profiter de son statut sans attirer de nouveaux venus désireux de profiter de la forte rentabilité du marché.

Pour empêcher l'entrée sur le marché de nouveaux joueurs, Milgrom & Roberts (1981) soutiennent qu'une réputation de prédateur peut être fort efficace. Dans un tel scénario, l'entreprise dominante se doit d'être intransigeante et de ne reculer devant aucun coût pour éliminer toute nouvelle compétition qui pourrait apparaître dans le marché. Cette pratique pourrait fort bien nécessiter des investissements importants de la part de l'entreprise monopoliste qui désire protéger son marché. À première vue, il pourrait être illogique de gaspiller ainsi autant de ressources. Cependant, l'objectif ici n'est point d'écraser un compétiteur, mais d'envoyer un message à tous les nouveaux venus qui seraient tentés de se lancer sur le marché. Ce message doit être clair : toutes les mesures seront prises pour éliminer la concurrence, peu importe le coût. Ces possibles compétiteurs se retrouveront alors devant un choix difficile en raison, encore une fois, de l'asymétrie d'information qui existe dans les marchés. Ne pouvant connaître l'étendue des ressources ni la véritable intention du monopole, la concurrence ne peut qu'utiliser les comportements passés pour prédire le futur. Dans ce contexte, les compétiteurs imputeront logiquement que leur entrée sur un marché enclencherait une réaction similaire à la précédente et tenteront alors leur chance dans un autre marché. Ainsi, une entreprise monopoliste qui se développe une réputation de prédateur n'aurait qu'à dépenser des ressources une seule fois (son investissement) pour protéger son marché de la compétition à long terme (le retour sur l'investissement).

La réputation peut aussi avoir un impact sur le comportement et les perceptions des consommateurs. Tan (1999) utilise pour ce faire l'exemple du commerce en ligne. Ce type d'achat posait et pose toujours beaucoup de problèmes en raison des problèmes de sécurité et de la difficulté à évaluer les biens achetés à l'avance. Bien des individus ont une crainte

raisonnable d'utiliser une carte de crédit en ligne pour faire des achats. Pour réduire les perceptions du risque, deux études (Tan, 1999; Jarvenpaa et al., 2000) démontrent que la réputation peut être un outil qui fait diminuer les craintes des consommateurs et augmente les probabilités qu'ils achètent des produits en ligne. Pour y arriver, la confiance doit cependant dépasser celle liée à un marchand en particulier et s'étendre à un écosystème de traitement des transactions au complet. La réputation dans ce contexte permettrait de modifier durablement le comportement d'individus et cela pourrait même se traduire par des changements de comportement dans d'autres sphères que la seule sphère des achats en ligne.

Bien que nous nous soyons concentrés sur les conséquences positives de la réputation jusqu'à maintenant, il existe un corpus de recherche dédié à l'étude des dangers de la réputation. Celui-ci inclut entre autres l'étude de Gaulthier-Gaillard (2011) qui souligne les dangers qui guettent les entreprises si elles ne font pas une gestion responsable de leur réputation. Lorsque cette dernière est attaquée, une perception de la réputation peut rapidement prendre le dessus sur la vraie nature de l'entreprise. L'auteur souligne l'importance dans ce contexte de surveiller auprès de ses partenaires et du milieu l'évolution de sa réputation afin de détecter rapidement les mouvements et d'y réagir dès que possible. Le texte laisse ici entrevoir une possibilité importante pour des firmes de consultants qui seraient chargées de constamment garder l'entreprise informée de l'état de ses concurrents et de sa propre réputation. Paquerot et al. (2011) sont pour leur part plus précis et soulignent les dommages que les sites d'évaluation en ligne peuvent avoir sur les affaires des hôteliers. De mauvaises critiques peuvent encourager les clients à se tourner vers d'autres établissements. Comme le disent Paquerot et al. (2011 : p.295) : "avec l'essor du web 2.0, chaque internaute est tout autant un client potentiel qu'un danger en puissance". Les entreprises ont peu de moyens pour se défendre contre des attaques de supposés clients passés qui pourraient très bien être en fait des compétiteurs. Les sites d'évaluation servent souvent de défouloir à des clients qui n'ont pas apprécié leur expérience, que ce sentiment soi légitime ou non. Les impacts de tels comportements sont très réels et ont un impact sur le chiffre d'affaires des entreprises visées. La réputation qui était une source de profits élevés peut donc aussi se transformer en danger qui menace les fondations même des entreprises.

Si les clients ont tant de pouvoir sur les fournisseurs de produits et services, c'est en grande partie en raison de l'arrivée de l'internet. Celui-ci a eu un impact à deux niveaux sur la génération et la distribution de la distribution : la diversité et la quantité (Cadel, 2010). Alors que l'information devait auparavant circuler de bouche à oreille, il existe aujourd'hui de multiples échelles, sites web et services qui ont pour unique d'objectif de collecter et diffuser de l'information en lien avec la réputation d'individus et d'entreprises. Ces services surveillent des centaines de milliers de blogues, de sites web et de médias sociaux. L'information sur la réputation est donc créée et diffusée sur toujours plus de plateformes, rendant la tâche d'intégrer toutes les données beaucoup plus difficile.

Qui dit sources plus importantes dit aussi quantité d'informations beaucoup plus grande aussi. À l'ère des blogues qui se doivent de publier pour survivre, l'information sur la réputation des individus et des firmes est constamment mise à jour et les défis associés à son analyse sont amplifiés. Des logiciels de forage de données sont aujourd'hui indispensables pour suivre à la trace l'évolution des tendances et des courants de pensée. Bien qu'utiles, ces logiciels se heurtent malgré tout à de nombreux problèmes au niveau de la forme et du contenu de la réputation (Cadel, 2010). Chaque source en ligne offre son contenu dans un format différent et il peut être difficile d'automatiser complètement le processus de collecte et d'analyse des informations. Les outils doivent donc être adaptés à chaque cas afin d'éviter de manquer des informations ou de créer des bouchons dans les systèmes d'analyse. Le contenu de la réputation peut aussi laisser planer beaucoup de doute. Il est souvent difficile, sur internet, d'identifier avec certitude le ton et l'attitude derrière les messages. Cela est encore plus difficile dans le contexte de brefs messages comme ceux retrouvés sur les microblogues comme Twitter. Les faux positifs et les faux négatifs sont fréquents et viennent à leur tour teinter le résultat des analyses. Un travail efficace requiert donc une part importante d'analyse manuelle et visuelle de la part d'humains plutôt que de logiciels de traitement automatisés.

Jøsang et al. (2007) adoptent un point de vue complémentaire et soulignent les différences dans l'évaluation des signaux dans le monde virtuel et dans le monde réel. Alors que l'attitude, les vêtements et l'accent sont des indices souvent utilisés pour juger de la réputation d'une personne, de tels signaux n'existent pas sur internet et d'autres mesures doivent donc être adoptées afin de compenser cette lacune. Les chercheurs soulignent aussi à

leur tour les limites de la diffusion d'une réputation dans le monde réel alors que l'internet ouvre toutes grandes les portes de la connaissance et de la diffusion d'information de manière globale et instantanée. Ce phénomène serait dû en grande partie aux systèmes de reconnaissance qui ont été implantés dans plusieurs sites d'enchères et dans des forums de discussion. La prochaine section nous permettra de mieux comprendre l'impact exact de ces systèmes sur la transmission de la reconnaissance.

3.3 La transmission de la reconnaissance

Glückler & Armbrüster (2003) identifient trois types de transmission de reconnaissance. La plus générale, dite publique, provient des médias, des rumeurs ou encore de connaissances qui nous donnent quelques bribes d'informations en passant. Cette information est souvent très large, mais de faible qualité. Elle permet d'accumuler beaucoup d'informations sur un large nombre d'entités sans pour autant être en mesure d'en identifier la source ou la validité. À l'opposé, la réputation basée sur l'expérience est, comme son nom l'indique, basée sur les rencontres et interactions passées. À travers les individus et les compagnies côtoyés, une image de ces entités se forme; cette image devient la réputation de l'entité. La réputation basée sur l'expérience a l'avantage d'être très fiable, car basée sur des expériences personnelles, mais est limitée en terme de portée, car une personne ne peut interagir avec un nombre illimité d'individus et de compagnies. Cette réputation sera possiblement partagée à d'autres dans ce que Glückler & Armbrüster (2003) appellent la réputation réseautée. Cette réputation représente l'ensemble des informations qu'une personne a amassées ainsi que celles qui lui sont partagées par son réseau social. La réputation réseautée propose le meilleur des deux mondes en offrant une plus grande quantité d'informations tout en conservant un certain regard sur la qualité de par l'origine de l'information. Le réseau social dans ce cas-ci peut inclure autant les amis proches que les relations d'affaires qui semblent dignes et capables de rassembler des informations crédibles. Le réseau social est donc un filtre à la réputation publique.

La montée en puissance de l'internet a quelque peu bousculé la façon dont la reconnaissance est transmise dans le modèle de Glückler & Armbrüster (2003). En effet, plutôt que de gérer de façon individuelle la réputation, plusieurs plateformes en ligne ont adopté des systèmes automatisés de reconnaissance qui ont pour objectif de collecter, gérer et diffuser de

l'information sur la réputation d'entités (Bolton & Ockenfels, 2004). Ces systèmes sont responsables de centraliser à un même endroit toute l'information disponible sur des individus ou des entreprises, d'en faire un sommaire pour ensuite le rendre disponible. Ces banques d'informations peuvent être centralisées dans un même endroit ou encore distribuées sur les ordinateurs de ses utilisateurs (Jøsang et al., 2007). L'avantage des systèmes décentralisés est qu'ils sont beaucoup plus résistants aux attaques malveillantes, car ils ne reposent pas sur un seul lieu névralgique.

Il existe plusieurs façons de synthétiser l'information relative à la réputation (Jøsang et al., 2007). La plus répandue est celle utilisée par les grands sites de mises aux enchères et de vente en ligne comme eBay et Amazon. Il s'agit d'une moyenne ou du total de tous les scores de réputation. Cette méthode a le mérite d'être extrêmement simple et facile à implanter. Une cote positive indique une bonne réputation alors qu'une cote négative implique une mauvaise réputation. D'autres modèles plus évolués sont basés sur des modèles probabilistes bayésiens. Ces systèmes peuvent prendre en compte une multitude de facteurs dont les interactions entre deux individus, les tendances dans l'attribution des points de réputation ainsi que les caractéristiques de chaque personne. Ces modèles sont toutefois beaucoup plus difficiles à mettre en ligne en raison des algorithmes qui y sont associés. Une troisième voie est l'utilisation de cotes qualitatives plutôt que quantitatives comme dans les deux premiers modèles. Les administrateurs des plateformes décident alors d'une échelle de termes qui peut par exemple aller de malhonnête à très honnête. Chaque utilisateur peut alors attribuer une note à ses pairs sur cette échelle. Les résultats sont alors affichés en pourcentage pour chaque catégorie. Une dernière façon d'instaurer un système de reconnaissance automatisé est d'utiliser l'inférence pour évaluer les réputations. Dans un tel scénario, si Alice fait confiance à Bob et Charlie et que Bob et Charlie font confiance à David, le système infère qu'Alice devrait faire confiance à David. Ce principe de l'inférence laisse plus de place à l'erreur, mais permet de créer des liens de confiance là où il n'y en avait pas explicitement.

La plupart des recherches qui s'intéressent aux systèmes automatisés de reconnaissance se sont concentrées sur le modèle implanté par eBay (Resnick et al., 2000; Resnick & Zeckhauser, 2001; Block-Lieb, 2002). Les résultats indiquent que plus de la moitié des utilisateurs prennent le temps de noter leurs partenaires d'affaires même si cela ne les aide

pas personnellement étant donné le faible nombre de transactions récurrentes dans les dyades (Resnick & Zeckhauser, 2001). Ceux-ci sont donc motivés par le désir d'aider la communauté et de souligner le bon (ou moins bon) travail des autres. Dans une écrasante proportion, les notes de réputation sont positives sur eBay. Cela tend à indiquer que les fraudes sont l'exception et non la règle dans ce milieu. Ceci est un premier indice de l'efficacité de tels systèmes pour prédire la performance des individus et limiter les comportements opportunistes des membres. Cela pourrait aussi être une limite découlant de l'évaluation mutuelle des participants. La personne qui reçoit un commentaire négatif et justifié peut décider de répliquer en laissant elle aussi une note négative à son partenaire afin de se venger. Pour éviter de telles situations, les participants aux enchères auraient donc intérêt à toujours laisser des commentaires positifs, nuisant ainsi au bon fonctionnement du système.

Ceci n'est qu'une critique parmi tant d'autres de la plateforme de réputation d'eBay. Block-Lieb (2002) renchérit sur le sujet en affirmant qu'il est impossible de vérifier la véracité des informations disponibles et que leur valeur en est donc affectée. L'auteure souligne aussi le manque d'explications sur le faible taux de critiques négatives. Aucune hypothèse n'a été testée et validée sur le sujet, rendant les chiffres offerts par eBay suspects à ses yeux. Plusieurs attaques délibérées contre le système sont aussi difficilement détectables (Bhattacharjee & Goel, 2005). Plusieurs complices peuvent par exemple conclure de fausses transactions ensemble pour monter l'un l'autre leur cote de réputation. Une fois bien établis, ils seraient alors en mesure de tromper les utilisateurs les plus conservateurs en utilisant cette fausse réputation. Les utilisateurs qui ont accumulé une mauvaise réputation peuvent par ailleurs simplement se créer un nouveau compte sous un autre nom afin d'effacer leur historique. De telles techniques sont très difficiles à contrer de par les services d'anonymisation du trafic et des identités en ligne.

Plusieurs études ont tenté de développer des systèmes alternatifs à ceux proposés par eBay pour éliminer certaines de ces lacunes (Chen & Singh, 2001; Sabater & Sierra, 2002; Miu et al., 2002; Xiong & Liu, 2003). Nous ne reprendrons pas ici le détail des algorithmes mis en valeur dans ces recherches, mais ces modèles offrent tous des solutions plus ou moins compliquées qui mettent en valeur l'importance des liens sociaux et des tendances. Des courbes d'accumulation de réputation peuvent paraître plus suspectes que d'autres et celles qui

se rapprochent trop de fraudeurs passés peuvent alors être identifiées et inspectées. Des chercheurs se sont intéressés plus particulièrement au problème des nouveaux venus dans un marché (Friedman & Resnick, 2001; Malik & Bouguettaya, 2009). Plutôt que de commencer leur carrière avec un score neutre, il serait possible selon ces auteurs de faire la moyenne des nouveaux comptes qui sont créés par des fraudeurs. Tout dépendant du taux de cas problèmes du moment, il serait alors possible d'attribuer une note positive ou négative dès le départ. Il serait aussi possible d'instaurer un coût qui rendrait l'option de se créer un nouveau compte moins attrayante.

Les systèmes automatisés de reconnaissance viennent combler les lacunes inhérentes aux marchés en ligne où la confiance est faible en raison de l'impossibilité de vérifier la qualité des produits à l'avance et du manque de relations personnelles. Bolton et al. (2004) confirment cet effet positif des systèmes de reconnaissance sur les marchés en relevant que les marchés qui l'utilisent ne se transforment pas en marchés de citron. Bien au contraire, les marchés qui utilisent ces systèmes semblent plus dynamiques et fluides. Block-Lieb (2002) affirme que la performance de ces systèmes n'est pas importante. Il faut au contraire s'intéresser à la perception que les gens ont de ces systèmes. Il ressort de son étude que les participants sont convaincus qu'il existe un bénéfice pour la communauté à utiliser ces systèmes et qu'ils sont efficaces pour contrôler les comportements opportunistes.

3.4 La performance et la réputation

Les systèmes automatisés de reconnaissance ne servent pas qu'à contrôler les mauvais comportements. Dans la perception des acteurs de marchés, ils sont aussi associés de près à la réussite et à la performance. Cette performance peut être mesurée de trois manières : un plus haut taux de vente de produits, un plus grand nombre de clients et/ou un prix de vente plus élevé. Bien des auteurs se sont intéressés à la relation entre la performance et la réputation, particulièrement en lien avec le système de reconnaissance implémenté sur eBay (Houser & Wooders, 2005; Resnick et al., 2006; Lucking-Reiley et al., 2000). Ces études utilisent l'un ou l'autre des trois indicateurs de performance comme variable dépendante. Le total de points de réputation (points positifs moins points négatifs) est lui opérationnalisé comme une variable explicative de la performance. D'autres variables contrôles sont aussi incluses dans les modèles comme la durée des enchères, l'heure de fin des enchères, la présence de photos et les

coûts d'envoi. Les résultats diffèrent au niveau des variables contrôles, mais la plupart des études s'entendent pour dire que la réputation a un impact significatif et positif sur la performance. Houser & Wooders (2005) notent une augmentation du prix de vente de 0.17 % par 10 % d'augmentation dans le total de points de réputation. Resnick et al. (2006) notent pour leur part une différence de 8.1 % entre le prix de vente d'un même produit par un individu ayant une bonne réputation versus un individu n'ayant pas de réputation, toutes choses étant égales par ailleurs. Lucking-Reiley et al. (2000) mesurent finalement une hausse de 0.3 % du prix de vente par tranche d'augmentation de 10 % de la réputation.

Snijders & Zijderman (2004) poussent un plus loin leur modèle prédictif et identifient des tendances différentes pour les grands utilisateurs d'eBay comparés aux ordinateurs occasionnels. Les grands utilisateurs auraient en effet le loisir d'attendre le bon acheteur pour accepter de vendre leurs produits, un facteur qui aiderait à augmenter le prix de vente de leurs produits. Des annonces complètes qui incluent des photos et des descriptions détaillées seraient aussi bénéfiques lorsque vient le temps de mesurer la performance d'un utilisateur. Cet effet de la réputation ne s'appliquerait cependant que pour les vendeurs. Comme ceux-ci attendent toujours de recevoir un paiement avant d'envoyer leur produit, leurs risques seraient minimes et la réputation de l'acheteur ne serait donc pas un facteur important.

La réputation a aussi été reliée à la performance dans plusieurs autres contextes. Dans le cas des appels publics à l'épargne par exemple, la réputation de la firme de comptable est utilisée pour augmenter le prix de vente des actions (Beatty, 1989). En s'associant (à fort prix) à une firme respectée, les compagnies désireuses de s'inscrire à la bourse envoient un signal fort au marché. En effet, les firmes de comptables ayant bonne réputation ne voudront pas, en théorie, perdre leur capital de réputation en publiant de faux résultats sur une compagnie. Leur réputation est précisément ce qui leur permet de facturer un prix plus élevé et d'attirer de nouveaux clients, comme nous l'avons vu précédemment dans la section sur l'analyse stratégique. Une compagnie qui utilise les services d'une telle firme comptable pourra donc profiter de la bonne réputation de leur contractant qui garantira hors de tout doute la santé financière de l'entreprise. Les compagnies paient donc une prime pour profiter de la réputation des grandes firmes de comptables qui leur remet la pareille en augmentant leur rendement lors de l'émission d'actions.

Les jeunes entreprises peuvent aussi se démarquer en utilisant leur réputation auprès de leur réseau social (Shane & Cable, 2002). Les firmes d'investissement sont en effet toujours à la recherche de possibilités d'affaire où investir et elles utilisent fortement leur réseau social pour obtenir de l'information sur la réputation de cibles potentielles. L'important dans ce calcul n'est pas de connaître les bonnes personnes, mais bien que l'information pertinente se rende aux bonnes personnes. La réputation vient donc combattre l'asymétrie d'information et permettre à certaines jeunes entreprises de performer davantage en obtenant plus de financement que les autres. Cet investissement initial par une firme d'investissement est directement responsable de l'augmentation des ventes de ces entreprises (Kotha et al., 2000). L'impact positif se répercute aussi sur la valeur de l'entreprise. En étant endossée par un investisseur connu, une firme réduit en effet l'incertitude qui l'entoure et les risques perçus par les consommateurs.

Le même effet positif de la réputation sur les ventes s'observe aussi dans d'autres industries comme celle du vin (Landon & Smith, 1997). L'origine d'appellation d'un vin et le nom du producteur ont un grand impact sur les ventes d'un produit. La qualité d'un produit à court terme n'est pas importante étant donné que les consommateurs se fient principalement à la réputation des produits. Dans ce cas précis, la réputation collective est plus importante que la réputation individuelle. Ainsi, même les firmes qui ne contribuent pas à augmenter la valeur de la réputation collective peuvent profiter de ces retombées. Sur le long terme, il est important que les producteurs conservent une certaine qualité dans leurs produits afin que leur réputation ne s'érode pas.

La réputation n'est pas que positive pour les entreprises. Au niveau individuel, Stickel (2012) démontre qu'être reconnu ses pairs dans le concours du *All-American Research Team*, une liste des meilleurs analystes des États-Unis, entraîne une hausse dans le salaire des individus élus. L'auteur affirme que les individus qui se retrouvent sur cette liste ont des qualités supérieures aux autres, mais que les individus sur la liste performent mieux au niveau du salaire que les autres. Stickel (2012) termine son texte en soulignant que ces as de l'analyse ont tendance à moins suivre les autres et sont moins prévisibles. Ils sont donc des leaders naturels de leur profession.

Finalement, Boot et al. (2006) démontrent aussi le grand pouvoir de la réputation sur la performance dans le contexte des contrats entre entreprises. Les compagnies peuvent choisir entre trois types de relations pour leurs transactions: aucun contrat, un contrat non contraignant et un contrat contraignant. La première option est de se fier à la parole de son partenaire, une avenue toujours périlleuse en affaire. La deuxième option est un contrat qui n'engage aucune pénalité en cas de non-respect. La dernière est un contrat formel avec des clauses qui peuvent être protégées par un juge. Il ressort de l'étude de Boot et al. (2006) que le contrat non contraignant est souvent le meilleur outil. Chaque entreprise possède deux types de capitaux : le capital de réputation et le capital financier. Si une compagnie honore un contrat non contraignant, elle augmente son capital de réputation, car elle tient parole, mais diminue son capital financier, car elle se doit d'agir pour respecter les termes de l'entente. Au contraire, si elle décide de ne pas honorer ce contrat, elle perd de son capital de réputation, car elle n'a pas tenu parole, mais sauvegarde son capital financier actuel. Avec les contrats non contraignants, la compagnie a la flexibilité de choisir le scénario qui l'avantage le plus à un moment précis. Cela lui permet de ne pas avoir à faire une vente précipitée pour respecter ses engagements formels. Par ailleurs, quand elle honore un contrat non contraignant, une entreprise augmente son capital de réputation ce qui lui permettra de diminuer ses coûts dans le futur. Il s'agit donc une situation gagnante dans la plupart des cas. Quatre prédictions sont faites par les auteurs: 1) plus une compagnie a de la réputation, plus il sera bénéfique de faire des contrats non contraignants; 2) les contrats non contraignants rapporteront moins que les contrats contraignants; 3) un contrat non contraignant d'une compagnie réputée vaut plus qu'un contrat contraignant d'une compagnie non réputée et; 4) la valeur d'un contrat non contraignant est corrélée à la réputation de l'entreprise. Ainsi, bien qu'à court terme les contrats non contraignants soient moins rentables, les profits à long terme seront normalement plus élevés.

3.5 La réputation criminelle

Il peut sembler étrange de s'intéresser autant, dans une thèse en criminologie, à la notion de réputation dans un contexte légitime. En effet, la quasi-totalité des références des textes utilisés jusqu'ici est issue du domaine des affaires et du marketing. Cette approche n'était cependant pas un choix délibéré. Au contraire, il s'agit plutôt du seul moyen de conceptualiser et comprendre la réputation dans un contexte de marché étant donné que la

littérature en criminologie ne s'est que très rarement et indirectement intéressée au concept de réputation criminelle jusqu'ici. La discussion portant sur ce concept se voulait donc une démonstration de ce qu'est la réputation et de son utilité potentielle en criminologie, surtout dans un contexte de marché.

Plusieurs raisons peuvent expliquer le manque d'intérêt pour la réputation criminelle. Dans un premier temps, la difficulté à évaluer chez les criminels cette notion pourrait être une première piste de réponse. Alors que l'internet et ses systèmes automatisés de reconnaissance offrent un laboratoire tout désigné pour la recherche sur le sujet, les criminologues n'ont eu que peu d'accès à ce genre de données pour leurs travaux. Il est aussi difficile, traditionnellement, d'évaluer la réputation d'individus dans un marché fermé où les gens ont intérêt à ne pas se connaître. Les criminels seraient donc moins au fait de tous les acteurs dans un marché donné et l'information circulerait aussi plus difficilement au sujet de chacun des acteurs. L'accès aux données est donc un grave problème potentiel.

Dans un deuxième temps, la réputation est surtout utilisée, du côté légitime, pour expliquer les succès ou la performance. Les recherches en criminologie sur le sujet sont pour le moment on ne peut plus limitées. Les quelques chercheurs qui se sont penchés sur la question ont surtout étudié l'impact des réseaux sociaux, des mentors (Morselli et al., 2006), des capacités techniques, de l'expérience (Nguyen & Bouchard, 2010) et des organisations criminelles (Tremblay et al., 2009) sur la performance criminelle. Dans ce cas, la performance ou réussite criminelle peut se mesurer par les revenus criminels ou encore le taux de détection. Les facteurs permettant d'atteindre un certain niveau de performance dans le monde criminel sont donc encore flous et les recherches n'ont tout simplement pas eu la chance d'aborder la question de la réputation jusqu'à maintenant.

Indirectement, cette question de la réputation a été approchée par des auteurs bien connus comme Reuter (1983) et Gambetta (2009). Reuter (1983) s'est fait connaître avec une recherche qui allait à l'encontre de l'ordre établi. Selon l'approche bureaucratique traditionnelle, la Mafia aurait le contrôle sur des marchés illicites comme le prêt usuraire, les paris illégaux et la protection. La Mafia utiliserait par la suite les marchés licites pour blanchir son argent et ainsi augmenter davantage son pouvoir. En adoptant une approche empirique,

Reuter (1983) prouve cependant que dans le cas de ces trois marchés illégaux, les entreprises criminelles sont généralement petites, qu'il y a peu de barrières à l'entrée et que les efforts de collusion ont été vains jusqu'à maintenant. Les firmes ne sont pas toutes aussi profitables les unes que les autres et la violence n'est pas la méthode privilégiée pour régler les conflits. Selon Reuter (1983), le rôle de la Mafia se situe avant tout dans l'arbitrage des conflits. Étant donné le manque d'institutions pour régler les différends entre criminels, la Mafia aurait cherché à combler le vide juridique en devenant une sorte de juge du monde criminel et prendrait un pourcentage sur les ententes qu'elle aide à négocier. Ici aussi, plusieurs familles de Mafia seraient en compétition pour ce marché et cette lutte permettrait de limiter les coûts d'arbitrage.

Les recherches de Gambetta (2009) se situent pour leur part dans un contexte plus large et s'intéressent à la théorie des signaux. Celle-ci tente d'expliquer comment deux entités arrivent à communiquer ensemble. Cette communication peut se faire à l'aide de signaux ou de signes. Les signes sont des messages passifs qui sont décodés par un destinataire alors que les signaux sont des messages qui sont dirigés activement vers un récepteur. Gambetta (2009) utilise l'exemple d'un tatouage pour différencier les signes des signaux. Une personne qui montre son tatouage de gang envoie un signal alors qu'une personne qui a un tatouage sans chercher à attirer l'attention d'autrui sur lui envoie un signe. Tous les signaux ne peuvent être acceptés tels quels, surtout dans le monde interlope. Une personne qui se dit être un expert en fraude bancaire pourrait très bien être un agent-double de la police; le coût du signal qu'il émet (sa voix) étant très faible. Pour s'assurer de la véracité des signaux, leurs récepteurs peuvent tenter d'augmenter leurs coûts. Plutôt que de croire une personne sur parole, un criminel pourrait exiger que l'émetteur du signal commette un crime que seul un criminel serait prêt à commettre (ex : tuer une personne). Le coût d'un tel signal serait alors trop élevé pour n'importe qui sauf un vrai criminel. L'objectif de Gambetta (2009) est de comprendre toutes les subtilités des signaux que nous envoyons et recevons quotidiennement et qui guident nos interactions sociales. Pour ce faire, il se concentre beaucoup sur le monde carcéral, mais utilise aussi plusieurs fois le récit de la vie de Joseph Pistone, l'agent infiltrateur mieux connu sous son nom d'emprunt Donnie Brasco.

Reuter (1983) et Gambetta (2009) se lancent dans une quête de la compréhension des interactions sociales. Reuter (1983) tente de comprendre empiriquement les relations entre criminels dans un contexte particulier alors que Gambetta (2009) utilise une approche beaucoup plus macro et théorique. Les deux auteurs se retrouvent cependant dans la présentation qu'ils font du tigre de papier développée initialement par Reuter (1983) pour discuter de l'importance de la réputation. Selon cette formule, les firmes criminelles ont dû se bâtir, à l'origine, une réputation de violence importante. Cette réputation était très coûteuse tant en terme de ressources humaines que financières. Les organisations se devaient de payer un grand nombre de membres et les comportements violents ont tendance à attirer davantage l'attention des services de police. Ce que Reuter (1983) nous explique ici est exactement est le calcul coût-bénéfice décrit plus haut dans cette section. Avec le temps, en effet, les organisations criminelles n'ont plus eu à prouver leur capacité et leur volonté à utiliser la violence. Elles ont alors pu diminuer leurs coûts et utiliser la menace de la violence plutôt que la violence elle-même pour atteindre leurs objectifs. C'est la raison pour laquelle Gambetta (2009) affirme que seules les entités qui durent dans le temps chercheront à se bâtir une réputation. Comme des investissements importants sont nécessaires dès le départ, les groupes temporaires qui ont peu de chance de survivre sur le long terme auront tendance à agir de manière opportuniste et à ne pas investir les coûts initiaux associés à la création d'une réputation. Cette question de la réputation n'est qu'un argumentaire, une parenthèse dans le discours de ces auteurs. Cette idée est donc loin d'être l'accent de leurs œuvres respectives.

C'est aussi le cas de plusieurs ethnographes comme Anderson (2000) et Steffensmeier (1986) qui se sont intéressés respectivement à la vie d'un quartier pauvre et noir de Philadelphie et au monde du recel. Dans le premier cas, la réputation transparaît sous la notion de respect et est utilisée à plusieurs reprises dans ce qu'Anderson appelle le code de la rue (Anderson, 2000). Ce code non écrit indique qu'une personne se doit de mériter le respect des autres. Ce respect est difficilement gagné, mais très facile à perdre. Il est très utile, car il permet de réduire les victimisations potentielles en donnant une image qui incitera les autres à garder leurs distances. Cette réputation ou respect évolue constamment dans le temps et chaque affront à la réputation se doit d'être vengé. Si son titulaire reste passif, il incitera alors les autres à s'attaquer à lui. À l'image des échanges d'Homans (1958), une personne perdant

du respect verra celui de son agresseur augmenter. Comme cette ressource est extrêmement importante, le moindre regard sera perçu comme un affront qui nécessitera une réponse. Ce cercle vicieux serait à l'origine de bien des violences dans les quartiers défavorisés. Steffensmeier (1986) mentionne aussi l'importance de la réputation, mais dans un angle plus affairiste. En effet, un receleur qui n'a pas la réputation d'être juste et loyal envers ses fournisseurs de bien volés perdra rapidement ses approvisionnements et ne sera plus en mesure d'opérer. Les receleurs ont donc tout intérêt à bien traiter les voleurs avec qui ils font affaire et à ne pas agir de manière opportuniste. Eux aussi doivent donc investir dans des coûts initiaux comme payer davantage pour les biens volés afin de s'assurer de bonnes grâces de leurs fournisseurs. Leur carrière criminelle en dépend.

Le code de la rue décrit par Anderson (2000) se voit confirmé dans les travaux de Topalli et al. (2002) sur les vendeurs de drogue de rue. Ceux-ci sont régulièrement attaqués en raison de l'argent et de la drogue qu'ils ont toujours sur eux. S'ils ne réagissent pas fortement en luttant pour leur argent et en cherchant à se venger par la suite, ils acquièrent alors la réputation d'être des proies faciles et cela augmente leurs risques de victimisation. Ici aussi, l'investissement initial pour la réputation est assez important, car les vendeurs peuvent subir de graves blessures lorsqu'ils sont attaqués. Ceux-ci sont aussi parfois obligés de prendre des mesures drastiques contre leurs agresseurs, allant jusqu'au meurtre. Malgré tout, l'investissement sur le long terme est bénéfique et leur permet d'être plus efficaces par la suite dans leur travail. Le même phénomène se répète chez les narcotrafiquants mexicains (Livingston, 2011) et les gangs de rue anglais (Densley, 2012). Dans tous les cas, la réputation est un facteur de protection et un facteur de performance.

Plus récemment, certaines études se sont intéressées à la notion de réputation dans un contexte similaire à celui présenté dans les sections précédentes, les marchés en ligne. Dans ce cas, il s'agit de forums de discussion où des pirates connus sous le nom de cardeurs achètent et vendent illégalement des produits et service en lien avec de l'information personnelle volée. Motoyama et al. (2011) affirment que la réputation est positivement corrélée au nombre de réponses à des offres de vente. Un investissement initial qui se calcule en implication sur les forums (nombre de messages mis en ligne) est nécessaire à l'accumulation de la réputation. Les personnes qui disposent de cette réputation sont en mesure de faire bannir plus aisément

les autres acteurs du marché. Cette technique d'élimination des indésirables et des compétiteurs semble efficace, car 20 % des comptes enregistrés ont été bannis.

Monsma et al. (2010) se sont intéressés à d'autres forums du même genre et affirment que pour accéder à certains d'entre eux, une excellente réputation et des connexions sont un prérequis. Chaque acteur est en mesure d'évaluer la réputation des autres personnes à l'aide de systèmes automatisés de reconnaissance. Cette libre circulation de l'information devrait augmenter sa valeur selon Monsma et al. (2010). Au niveau des opportunités d'affaires, les données indiquent que plus le niveau de réputation et le statut des membres sont élevés, plus la probabilité de recevoir un message augmente. Plusieurs parallèles peuvent être tissés entre ce marché illicite et d'autres marchés légaux comme le fait que les plus grands acheteurs ont un réseau social plus développé, que ceux qui ont les meilleurs produits sont les plus populaires et que les acteurs recherchent surtout à contacter les personnes à la haute réputation ou au haut statut. En ce sens, les criminels qui œuvrent dans ce milieu peuvent pleinement être considérés comme des entrepreneurs.

Mell (2012) reprend aussi certains thèmes propres au monde des affaires lorsqu'il mentionne le besoin de développer des mécanismes pour augmenter la confiance dans les marchés illicites. Celui-ci viendrait de la difficulté à différencier les bons des mauvais vendeurs et à évaluer les nouveaux venus dans un marché. Comme n'importe qui peut effacer sa mauvaise réputation en créant un nouveau compte, il est important selon Mell (2012) d'instaurer un coût à la création de comptes pour limiter ce genre de comportement. L'objectif est donc de rendre les investissements initiaux en réputation plus élevée. Comme le volume de transactions sur les marchés illicites est important, Mell (2012) pose l'hypothèse que les systèmes automatisés de reconnaissance répondent à un besoin et sont perçus comme efficaces. Étrangement, tout comme dans le monde légitime, très peu de commentaires sur la réputation sont négatifs. La recherche ne permet malheureusement pas ici non plus de comprendre les raisons des faibles plaintes à travers ce système.

L'auteur se surprend à constater le faible niveau de citrons dans ce marché. Cela pourrait être dû au fait que les acteurs cherchent surtout des partenaires pour le long terme. Ces relations de confiance se bâtissent, car les vendeurs sont prêts à vendre des produits de

qualité à un prix inférieur au départ afin d'attirer des partenaires et ensuite de les augmenter graduellement. Les acheteurs eux sont prêts à prendre des risques, car les coûts initiaux sont faibles. Il existe donc un modèle des échanges et un équilibre qui se crée entre les coûts et les avantages pour chacune des parties. Pour déstabiliser ce système, Mell (2012) suggère de s'attaquer au système de reconnaissance en rendant son utilisation beaucoup plus difficile. Pour ce faire, il faudrait que des personnes ayant une bonne réputation commencent à agir de façon erratique afin de créer de l'incertitude envers ce type de profil. Comme il n'existe pas de régulation formelle, les acteurs se doivent dans ce contexte de se rabattre sur la confiance et surtout sur les systèmes de reconnaissance.

3.6 Conclusion

La réputation est un concept clé qui a été largement étudié dans les domaines des affaires et du marketing. Synthèse de l'image d'une personne ou d'une chose, la réputation a d'abord été abordée dans les travaux d'Homans (1958) qui visaient à définir les comportements sociaux en tant qu'échanges. Dans ce contexte, la réputation devenait une ressource, une monnaie d'échange permettant aux acteurs d'interagir entre eux. Les individus recherchant une plus grande réputation pouvaient offrir de leur temps et de leurs connaissances en échange de la reconnaissance des autres.

Cette façon de conceptualiser la réputation a été reprise dans maintes recherches au cours des trente dernières années. Des recherches, telles celles de Deephouse (2000) et Rao (2006), ont confirmé que la réputation avait toutes les caractéristiques d'une ressource soit la valeur, la non-substituabilité, l'inimitabilité et la rareté. Aborder la réputation sous un angle des ressources implique nécessairement d'adopter un langage économique où l'analyse coût-bénéfice est omniprésente. Shapiro (1983) fait partie d'un courant de chercheurs (Raub & Weesie, 1990; Herbig & Milewicz, 1993, McDonald, 1999) à noter qu'un investissement initial élevé était nécessaire pour récolter d'importants profits sur le long terme. Les acteurs du marché comprennent en général cet échange et réduisent leurs comportements opportunistes à court terme pour se mieux se positionner sur le long terme. Cette stratégie est particulièrement importante dans le contexte de marchés où la confiance est à son plus bas.

La transmission de la réputation se fait habituellement à travers les réseaux sociaux (Glückler & Armbrüster, 2003). Autant l'information de première que de secondes mains circulent ainsi. Avec l'internet, de nouveaux systèmes automatisés de reconnaissance ont permis aux acteurs de collecter et d'accéder à des informations complètes sur la réputation d'un grand nombre d'individus. Ces systèmes réduisent les asymétries d'information ainsi que les incertitudes inhérentes aux marchés. Ils viennent aussi combler certaines difficultés associées au traitement de la réputation dans un contexte virtuel (Cadel, 2010). En effet, la toile mondiale a considérablement diversifié le nombre de sources de la réputation ainsi que la quantité d'informations à traiter. En utilisant des systèmes automatisés, les acteurs s'assurent qu'ils auront accès à une information de qualité facilement digérable.

La réputation est associée de près à la performance. Ce lien s'observe le plus facilement dans les plateformes d'échange en ligne où les systèmes automatisés de reconnaissance sont présents. Les recherches s'entendent pour dire qu'une augmentation de la réputation entraîne automatiquement une hausse du prix de vente de biens et services (Snijders & Zijdeman, 2004). Le même phénomène s'observe aussi dans d'autres milieux comme l'industrie du vin et de la finance (Landon & Smith, 1997; Stickel, 2012). Dans ces deux cas, les personnes ou groupes ayant une réputation supérieure peuvent espérer recevoir de meilleurs salaires et faire de meilleures ventes. La réputation devient donc un outil de promotion qui permet d'orienter le comportement des autres à notre égard.

Ces recherches sur le concept de réputation dans le monde légitime démontrent l'importance de s'intéresser à ce même concept, mais dans une optique de marchés illicites. Les travaux d'Anderson (2000) et Topalli et al. (2002) prouvent en effet que les criminels s'évaluent entre eux et qu'ils s'accordent aussi une cote de réputation de façon formelle et informelle. La réputation d'un individu expliquera souvent son degré de victimisation et sa performance dans la vente de drogue. Une mauvaise réputation entraînera une carrière criminelle dangereuse, voire très brève.

Les mêmes mécanismes de création et de valorisation de la réputation s'appliquent aussi tant au monde légitime qu'au monde illégitime. En effet, les criminels utilisent eux aussi l'analyse coût-bénéfice pour justifier les investissements initiaux en réputation (Reuter, 1983).

La mafia étudiée par Reuter (1983) l'a bien compris et a démontré qu'une fois la réputation établie, la menace de violence était aussi efficace que la violence elle-même. Les études démontrant la grande profitabilité de la vente de drogue par des entités importantes laissent souvent de côté cette première phase d'expansion où les acteurs doivent se prouver aux autres. Les profits peuvent paraître importants, mais ils ne sont que le retour sur un investissement initial.

Une bonne réputation permet de bâtir des relations d'affaires dans le monde illicite et de réduire ses coûts d'approvisionnement sur le long terme (Steffensmeier, 1986; Mell, 2012). Des partenariats stables diminuent les risques et les incertitudes associés aux transactions illégales. Toutes les parties profitent d'un tel climat et il n'est pas surprenant de constater que les criminels préfèrent avoir de longues relations commerciales plutôt que des échanges avec des nouveaux venus. Une bonne réputation aide à instaurer un climat de confiance qui est nécessaire à l'établir des liens durables.

Les criminels, comme les entrepreneurs, utilisent de plus en plus les systèmes automatisés de reconnaissance pour gérer leur réputation dans le contexte de plateformes en ligne. Ces systèmes sont utilisés de la même manière dans le monde légitime et illégitime (Motoyama et al., 2012; Mell, 2012). Plusieurs parallèles entre ces deux univers sont même frappants. En effet, les utilisateurs ont tendance à inscrire beaucoup plus de commentaires positifs que négatifs. De plus, les personnes ayant une bonne réputation sont plus populaires, reçoivent plus de communications et leur compagnie est recherchée. Cela nous permet de comprendre comment la réputation criminelle est associée au succès dans le monde illégitime. Les individus disposant de la meilleure réputation ont accès à plus d'opportunités criminelles et peuvent donc performer plus efficacement que les autres. D'autres travaux en cours tendent dans la même direction (Décary-Hétu & Leppänen, à venir).

Tous ces parallèles entre le monde légitime et illégitime laissent sous entendre qu'ils existe probablement peu de différences entre des ceux mondes et qu'il s'agit possiblement de sphères d'activités assez poreuses. Cela ouvre la porte à une étude formelle de la réputation dans un contexte criminel. Notre compréhension du phénomène n'est que très fragmentaire pour le moment et ne nous permet pas encore de pleinement comprendre le rôle que la

réputation peut jouer dans les marchés illicites. Étant donné l'importance de la réputation dans le monde légitime et les similitudes entre les marchés légaux et illégitimes, le concept de réputation criminelle nous apparaît comme un champ de recherche prometteur et important à développer. Les objectifs généraux de cette thèse seront donc de comprendre comment s'articule le concept de réputation dans les marchés illicites en ligne ainsi que son impact sur la performance criminelle.

À l'image des quelques études récentes portant sur la réputation criminelle, nos recherches se concentreront sur des données issues de cybercrimes. Deux raisons expliquent ce choix. Tout d'abord, les cybercrimes sont en pleine ascension (Brenner, 2007) et représentent la plus grande menace dans un futur rapproché. Chaque criminel peut aisément attaquer un nombre important de personnes où qu'elles se trouvent dans le monde en une période de temps très limité. Les dégâts de ces attaques se font déjà sentir chez plusieurs petites et moyennes entreprises qui sont prises pour cibles (Krebs, 2012a). Les impacts de ces attaques ne sont pas à sous-estimer : plusieurs compagnies sont obligées de fermer leurs portes suite au vol de toutes les liquidités de ces compagnies. Les cyberattaques sont aussi nommées comme source de transfert illégal de technologies entre états. Le crime organisé se spécialise maintenant dans la fraude de propriété intellectuelle et cette activité peut être la source de très importants profits. Il est donc urgent de développer nos connaissances sur ces types de crimes aux caractéristiques particulières.

Par ailleurs, tel qu'il a été démontré dans cette section, collecter de l'information sur la réputation d'individus n'est pas chose aisée. Plusieurs études se sont concentrées sur les systèmes automatisés de reconnaissance pour contourner ce problème. D'autres recherches ont aussi utilisé des sources innovatrices de données comme les palmarès d'entreprises les plus réputées ou encore des analystes les plus en vus. D'autres ont choisi de s'inspirer de résultats officiels de courses automobiles. L'alternative à ces méthodes serait de faire un sondage d'opinion qui viserait une population criminele. L'envergure d'un tel projet est bien au-delà d'une simple thèse et nous nous devons donc de limiter le champ d'études de cette thèse à la question des cybercrimes.

CHAPITRE 4 – MÉTHODOLOGIE

Notre premier contact avec la littérature spécialisée en cybercriminalité s'est fait à l'aide des recherches portant sur la scène des warez. La majorité d'entre elles pouvaient être classées en deux catégories. Dans la première, nous retrouvons les sondages d'opinion d'étudiants universitaires qui répondent à des questions sur leurs habitudes de piratage, les raisons qui les poussent ou non à pirater des produits ainsi que leur profil sociodémographique. Il est saisissant de constater le nombre d'études sur la scène des warez qui reprend le même devis de recherche et qui rapporte, à chaque fois, les mêmes résultats dans des populations différentes. De l'aveu même des auteurs de certaines de ces recherches (que nous ne citerons pas ici), cette méthodologie était utilisée pour sa facilité et sa rapidité. Les sujets étaient accessibles et jouissaient d'une liberté limitée à répondre aux questionnaires. Les questionnaires n'étaient pas très compliqués à monter, car plusieurs exemples existaient déjà dans le corpus scientifique. Il suffisait donc d'additionner les deux pour arriver à une étude scientifique au maximum d'impact et au minimum de coût. Hagan & McCarthy (1997) soulèvent les problèmes reliés à ce type d'étude dans leur discussion distinguant la criminologie de l'école de la criminologie de la rue. La criminologie de la rue est celle est anthropologues et des ethnographes qui se sont intéressés à la vie des personnes marginalisées comme les jeunes de la rue, les prostituées et les itinérants. La criminologie de l'école fait plutôt référence aux types d'études décrites dans ce paragraphe. Celle-ci est basée sur des sondages distribués aux écoliers, surtout au primaire et au secondaire. Hagan & McCarthy (1997 : p6) dénoncent le passage d'une criminologie de la rue à une criminologie de l'école en affirmant que cette dernière a des impacts néfastes : "less theoretically relevant characteristics […] are now used to explain less serious behaviors […] of less criminally involved persons." Ces commentaires, bien qu'écrits plusieurs années avant la montée en puissance de la scène des warez, s'appliquent parfaitement à son cas. La méthodologie employée dans cette thèse s'inspira fortement de la criminologie de la rue.

L'autre catégorie de recherche est composée de livres et d'articles journalistiques. Nous y retrouvons par exemple l'excellente enquête de Craig (2005) qui a réussi à percer l'univers des groupes de pirates en fréquentant les mêmes salles de clavardage qu'eux et en s'imprégnant de leur culture. Cette approche donne des résultats très riches en contenu et nous

permet de comprendre la sous-culture criminelle du milieu, mais sans permettre de valider la rigueur et les sources utilisées. Nous retrouvons peu de citations pour les propos rapportés dans le livre et nous devons nous fier à la parole des journalistes quant aux libertés qu'ils prennent entre l'histoire qu'ils désirent raconter et la réalité.

Ce point de départ, bien que décevant à certains égards, était malgré tout stimulant. En effet, ces recherches démontraient que les criminels étaient beaucoup plus accessibles que ce que nous aurions pu penser. Plusieurs chercheurs que nous avions rencontrés au cours des premiers mois de notre thèse doutaient qu'il soit possible d'entrer en contact avec de "vrais" cybercriminels. Les études journalistiques prouvaient pourtant le contraire.

Évidemment, il est impossible de travailler sur des questions en lien avec la cybercriminalité sans connaître parfaitement ses sujets d'étude. Un ethnographe qui désirerait étudier le phénomène des gangs à Harlem et qui se promènerait au hasard dans le quartier seul le soir pourrait faire de fortes mauvaises rencontres. La phase de préparation est cruciale afin de comprendre la sous-culture visée par nos recherches et les endroits que fréquentent les criminels. Un chercheur se doit d'avoir le savoir-être et le savoir-faire nécessaire avant de se lancer à l'eau. Toutes les mésaventures scientifiques ne peuvent se terminer aussi heureusement que celle de Venkatesh (Levitt & Venkatesh, 2000). Bien que ce code de conduite s'applique à toutes les sciences en général, il nous fut d'une précieuse aide dans notre étude de la cybercriminalité.

Pour comprendre les pirates, nous avons d'abord cherché à comprendre les endroits qu'ils fréquentaient sur internet. Comme ils ne se rencontrent que peu voir pas en réel, des lieux publics d'interactions devaient exister pour qu'ils puissent socialiser, trouver des partenaires et apprendre de nouvelles techniques. Trouver ces endroits n'est pas pour autant chose aisée. L'internet peut être divisé en deux classes : l'internet public et l'internet obscur. L'internet public est composé de tous les services et plateformes qui sont accessibles publiquement. Les moteurs de recherche indexent inlassablement son contenu et il est relativement aisé d'y trouver l'information désirée. L'internet obscur, lui, est composé de toutes les bases de données et services privés qui sont protégés par des mots de passe et qui bloquent l'accès aux moteurs de recherche. Le cas le plus connu de ce genre de contenu est le

réseau social Facebook qui garde jalousement toute l'information de ses utilisateurs pour lui et qui n'autorise que son propre moteur de recherche à indexer son contenu.

Évidemment, le rêve de tout chercheur serait d'avoir accès à cet internet obscur où la criminalité la plus exclusive se cache. L'accès à ces forums de discussion et autres plateformes nécessite cependant un investissement que nous n'avons pas été en mesure d'atteindre pour le moment. Krebs (2011a), un journaliste et chercheur de renommée internationale, s'est donné comme mission d'apprendre le russe afin de pouvoir infiltrer plus aisément les milieux criminels d'Europe de l'Est. Il s'agit selon lui d'une nécessité et non d'un luxe. Il mentionne d'ailleurs que certains forums utilisent maintenant des questions de culture générale lorsque des individus désirent s'enregistrer pour s'assurer que seulement des individus originaires d'une certaine région puissent le faire. Les personnes qui utiliseraient un service comme un traducteur automatisé ne serait ainsi pas en mesure de comprendre la subtilité de la question et de fournir une réponse adéquate. Il s'agit d'un exemple parmi plusieurs autres où les cybercriminels tentent de mettre un mur entre eux et les membres des forces de l'ordre et de la communauté scientifique.

Si ceux-ci se donnent autant de mal pour camoufler leurs activités sur le web obscur, c'est en partie pour empêcher que les succès passés des forces de l'ordre ne se répètent dans le futur. Cette thèse démontre qu'il est en effet possible d'arriver à obtenir des informations très précises sur un grand nombre de cybercriminels en se limitant à l'internet public. Pour y arriver, il est nécessaire de développer une compréhension fine du mode de fonctionnenent des criminels. Dans le cas de la scène des warez, nous sommes tombés un peu par hasard, au fil des recherches sur les moteurs de recherche, sur une archive de journaux publiés par et pour les pirates informatiques impliqués dans le warez. Ces journaux nous ont permis de nous immiscer dans le quotidien des pirates et de comprendre encore davantage la culture criminelle de ces individus. Bien que les recherches passées comme celles de Rehn (2003) soulignent la dynamique de tournoi perpétuel entre les pirates, ces articles de journaux, éditoriaux et lettres ouvertes nous ont permis de vivre cette compétition et de réaliser sa force. La lecture de ces journaux nous a aussi permis de découvrir que la scène des warez était friande d'échelles, de décomptes et de listes où les groupes étaient notés les uns par rapport aux autres. De telles informations nous ont alors menés à enquêter plus à fond sur cette tendance et à découvrir des

sites d'index où les pirates revendiquaient chacun de leur produit piraté. Ces sites contenaient une liste de plusieurs dizaines voir plusieurs centaines de milliers de produits piratés ainsi qu'une série d'informations à leur sujet. La décentralisation de la scène avait jusqu'à maintenant limité les recherches portant sur la communauté. Cette découverte nous permettra, comme nous le verrons sous peu, de modéliser la communauté dans son entier et d'identifier les liens entre la réputation et la performance chez ces pirates.

Dans le cas de la scène des warez, une bonne connaissance de la sous-culture incluant le jargon utilisé par les pirates et des heures de recherche nous ont permis d'atteindre notre objectif initial : découvrir une source d'information innovatrice et riche de données. Ceci n'est cependant que la première étape de quiconque désire se lancer dans l'étude de cybercriminels. Une fois découvertes, ces données doivent encore être collectées. Pour y arriver, les chercheurs se doivent d'apprendre de leurs sujets d'étude. Tout comme les ethnographes qui adoptent la couleur du milieu dans lequel ils travaillent, les chercheurs en cybercriminalité doivent apprendre à utiliser certains outils développés dans le milieu de la sécurité informatique et du développement web. Dans nos recherches, nous avons eu recours à plusieurs reprises à un outil connu en anglais sous le terme de *scraper* et que nous traduirons par grattoir. Ce type de logiciel permet de télécharger et d'extraire de pages web les données désirées. Des logiciels commerciaux existent et peuvent être achetés, mais ces outils sont souvent dispendieux et rigides. Ils ont donc de la difficulté à s'adapter aux complexités de l'internet évolutif. Étant donné que nous avions des connaissances poussées en informatique, nous avons été en mesure de concevoir et d'opérer nos propres logiciels grattoirs qui imitaient le comportement d'usagers normaux des sites hébergés par des pirates. Il est très important que les chercheurs prennent le maximum de précaution quand ils procèdent à leur collecte de données afin de ne pas alerter les criminels de la surveillance dont ils font l'objet. Une telle alerte pourrait teinter les données et encourager les criminels à déménager leurs bases de données vers des zones plus obscures de l'internet.

L'utilisation de logiciels grattoirs n'est pas le seul outil à la disposition des chercheurs en cybercriminalité. Il existe en effet une multitude de sites web, de blogues et surtout de baladodiffusions qui se concentrent sur la sécurité informatique. Dans l'une d'elles par exemple, les animateurs racontaient comment ils avaient été en mesure d'adapter un logiciel

pour continuellement surveiller les réseaux postes à postes comme Kazaa, eMule et Gnutella afin de détecter des documents personnels confidentiels. Ils avaient ainsi été en mesure de découvrir que des milliers d'individus partageaient avec la planète des copies de leur passeport, de leur relevé d'impôt et de leur relevé de compte en banque. De telles sources d'informations sont très utiles pour stimuler la curiosité des chercheurs et offrir des pistes de recherche. Elles sont le fruit du travail d'experts en sécurité qui sont plus intéressés par le comment que le pourquoi des cyberattaques. En tant que criminologue, il nous est cependant possible d'utiliser les outils et les connaissances de ces individus pour nous permettre de bâtir des devis de recherche innovateurs. Les deux premiers articles de cette thèse sont basés sur la découverte de sources de données innovatrices et ont eu recours à l'utilisation d'un logiciel grattoir pour collecter les données. Pour le troisième article cependant, nous nous sommes inspirés d'une baladodiffusion où les animateurs mentionnaient qu'une guerre entre administrateurs de forums illicites avait mené à la compromission d'un forum au complet. Ceux-ci s'amusaient à l'idée de lire tous les messages privés, mais craignaient l'impact du dévoilement possible de milliers ou de millions de numéros de carte de crédit.

Les données de notre troisième article sont issues de ce forum qui a été distribué sur plusieurs sites d'échanges de fichiers. Même si trouver les données était relativement facile, les manipuler l'était beaucoup moins, car elles étaient infectées par des virus et dans un format peu convivial d'analyse. Ici encore, les chercheurs doivent faire preuve de créativité et s'imprégner des sujets qu'ils étudient. Il existe plusieurs outils de virtualisation qui permettent d'isoler des fichiers de façon sécuritaire afin d'en extirper les informations. De telles techniques sont utilisées autant par les cybercriminels que les experts en sécurité qui doivent travailler dans des milieux hostiles. Tous les guides et instructions nécessaires, encore une fois, sont disponibles en ligne aux personnes qui désirent apprendre et parfaire l'art de la recherche sur les cybercrimes.

Cette introduction de notre section de méthodologie avait pour objet d'offrir une vue d'ensemble des méthodes et techniques utilisées dans chacun des trois articles que nous présenterons ci-dessous. La recette d'une bonne étude en cybercriminalité n'est pas des plus complexes. Il s'agit avant tout d'investir le temps et les efforts nécessaires à l'assimilation de la sous-culture visée afin d'en comprendre le jargon, les méthodes ainsi que les coutumes. Le

chercheur peut alors utiliser les points névralgiques des communautés criminelles afin d'identifier les sources d'information les plus appropriées. Il faut être attentif et se maintenir au fait des derniers développements afin de ne pas rater la chance de mettre la main sur des données précieuses qui ne seraient disponibles que pour une durée de temps précis. Les chercheurs doivent, finalement, s'engager à apprendre comment fonctionnent les outils informatiques afin d'arriver, eux aussi, à pirater les pirates.

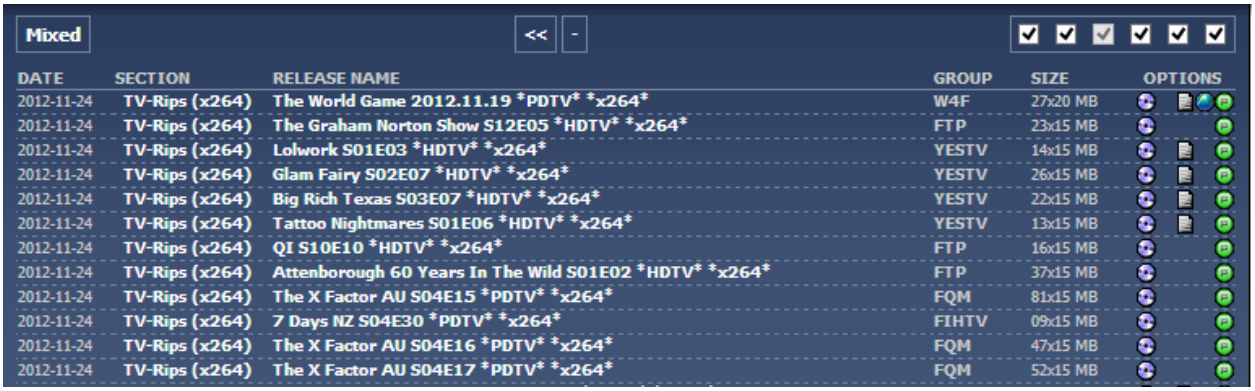
4.1 Les warez

Comme mentionnées dans le Chapitre 2, les études portant sur la scène des warez posaient problème à plusieurs niveaux. Les deux problèmes les plus criants étaient l'attention portée aux consommateurs de warez ainsi que le manque de connaissances sur la structure de la scène. Lorsque nous avons sélectionné cette communauté de pirates informatiques, notre objectif principal était de répondre à ces critiques et d'amorcer un mouvement de réorientation de la recherche portant sur le sujet. Nous voulions alors démontrer qu'il est possible pour les chercheurs d'obtenir une information de première main sur ce type de criminels, et ce, sans avoir de contacts privilégiés avec l'un d'entre eux.

Plusieurs recherches (Craig, 2005; Rehn, 2003) font état de l'importance de la réputation dans cette communauté virtuelle. Celle-ci serait d'ailleurs la principale motivation des individus impliqués dans ce trafic; il s'agirait donc pour les pirates d'une quête de validation sociale par des pairs.

L'objectif général de cet article est de comprendre comment la reconnaissance est distribuée dans la scène des warez afin d'expliquer la survie de certains groupes et la mort de d'autres. Pour ce faire, nous nous sommes lancés à la recherche d'informations sur cette communauté à travers le moteur de recherche de Google. Nous avons rapidement découvert qu'il existait des bases de données publiques contenant des listes de tous les produits piratés par les participants de la scène tel qu'illustré dans la Figure 1.

Figure 1 : Site d'index de la scène des warez

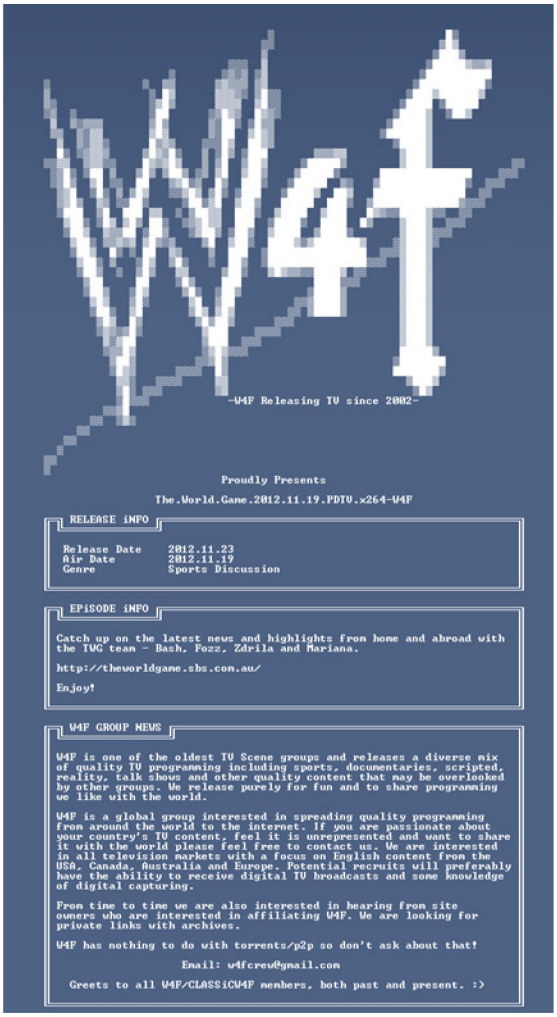


Il peut paraître étonnant à première vue de constater que des individus maintiennent une liste des crimes passés des membres de leur communauté. L'existence de tels index se justifie aisément dans la mentalité de la scène cependant. En effet, les groupes de pirates sont en compétition– un tournoi perpétuel selon Rehn (2003) - les uns avec les autres afin de livrer le plus rapidement possible le plus de produits piratés. Seul le groupe qui arrive le premier à distribuer un produit recevra la reconnaissance associée à cet acte. La réputation globale d'un groupe est la somme de toutes les petites reconnaissances amassées au fil des actes de piratage. La scène des warez est loin d'être centralisée et il est possible de distribuer en ligne un produit piraté à partir de plusieurs serveurs. Ces derniers sont opérés par des individus ne faisant partie d'aucun groupe, mais qui offrent une infrastructure de distribution aux groupes. En échange, ils ont accès à tous les fichiers distribués dans la scène et reçoivent la reconnaissance de leurs pairs. Des groupes différents pourraient, en théorie, mettre en ligne un même produit sur des serveurs différents et ensuite s'affronter sur la paternité de tel ou tel produit piraté. Pour limiter ces points de discordes, les sites d'index mentionnés plus haut ont vu le jour et servent de listes officielles des exploits de chaque groupe. Avant de mettre en ligne un produit, chaque groupe est tenu par les règles officieuses de la communauté de vérifier si la propriété intellectuelle a déjà fait l'objet d'un lancement par un autre groupe (c.-à-d. a déjà été distribué par quelqu'un d'autre). Si ce n'est pas le cas, le groupe peut alors ajouter ses informations sur l'index et mettre en ligne son fichier piraté. Ce système simple permet d'éviter les conflits et les malentendus alors qu'un groupe pourrait croire être l'auteur crédité d'un piratage alors que ce ne serait pas le cas.

Les sites d'index de la scène des warez offrent une fenêtre des plus intéressantes sur la communauté. Ils exposent en effet une liste qui contient plusieurs centaines de milliers d'actes de piratage ainsi que plusieurs informations nominatives sur les groupes responsables de cette déviance. Il s'agit ici d'un rare cas où des criminels signent et publient ouvertement l'étendue de leurs crimes.

Pour les besoins de cette recherche, nous nous sommes limités à un seul site d'index qui contenait de l'information sur près de 100,000 produits piratés entre juin 2003 et janvier 2009, moment de la collecte de données. Nous avons choisi l'index illustré à la Figure 4 pour deux raisons. Premièrement, ce site offrait des données plus complètes que les autres. Nous avions notamment accès au nom du produit piraté, à la date du piratage, au nom du groupe responsable, à la taille du fichier et au nombre de téléchargements du fichier piraté. Chaque profil de produit piraté contenait aussi un lien vers le fichier NFO associé. Les fichiers NFO sont de simples fichiers textes qui sont distribués avec chaque produit piraté. Ils contiennent habituellement quatre sections : (1) des informations nominatives sur le produit piraté (par exemple, la date de sortie, le type de produit, la plateforme); (2) une description détaillée du produit (par exemple, le scénario d'un film ou d'un jeu); (3) des informations sur le groupe de pirate ayant distribué le fichier (nom du groupe, annonces); et (4) des salutations ou "greetz" faites par le groupe de pirates informatiques à d'autres groupes. Ces salutations sont présentées sous la forme d'une liste de groupes que les pirates souhaitent saluer. Une telle pratique permet de tisser des liens avec d'autres groupes de pirates et aussi de reconnaître la qualité du travail de l'élite de la scène. Il s'agit donc d'une technique pour flatter l'ego de certains membres de la communauté. La Figure 2 est un exemple typique de fichier NFO.

Figure 2 : Exemple de fichier NFO



En plus d'offrir une information variée et complète, l'index que nous avons choisi était aussi l'un des plus reconnus (TopSite, 2010). Comme nous n'étions pas en mesure de valider l'origine des données affichées sur cet index, nous nous en sommes remis à la communauté des pirates qui semblait apprécier le travail de cet index.

Comme l'objectif de cette recherche est de comprendre la distribution de la reconnaissance dans la scène des warez, nous avons tout d'abord isolé, pour chaque groupe de pirates, le nombre de groupes distincts qui les saluaient dans les fichiers NFO. Cette mesure de la réputation est au cœur de toutes les analyses que nous présenterons. Les groupes de pirates ont tendance à réutiliser les mêmes fichiers NFO dans le temps. Ceux-ci sont vus comme des

œuvres d'art par les pirates qui investissent énormément de temps et de ressources humaines dans leur création. Chaque caractère doit en effet être positionné afin de donner l'impression qu'une image a été insérée dans un fichier texte (voir Figure 5). Un calcul du nombre pur de salutations serait donc biaisé par les groupes plus productifs qui utiliseraient toujours le même modèle de fichier NFO. C'est pour cette raison que nous avons opté pour une méthode d'analyse qui ne tient compte que du nombre de groupes qui saluent chacun des autres groupes. Étant donné le grand nombre de fichiers NFO à analyser (près de 100,000), nous avons conçu un logiciel qui a parcouru les fichiers à la recherche de noms de groupes de pirates. Une validation manuelle a ensuite été nécessaire pour s'assurer de la fiabilité du résultat et pour nettoyer les données des groupes qui portaient des noms comme *Legend* ou *TV* et qui auraient pu être confondus par notre logiciel automatisé avec les mots communs.

Pour expliquer la distribution de la reconnaissance, nous avons transformé les données collectées décrites ci-dessus. Nous avons tout d'abord mesuré la *durée de vie* de chaque groupe en calculant le nombre de jours entre le premier et le dernier produit piraté. Pour les groupes avec seulement un lancement de produit piraté, la durée de vie a été fixée à 1. Le *nombre de produits piratés* est la deuxième variable du modèle. Il s'agit d'une variable continue qui mesure le nombre de lancements de chaque groupe. La *productivité* mesure le nombre de jours entre chaque distribution de produit piraté. La *taille de tous les fichiers* mesure le nombre de gigabits distribués par chaque groupe. Des fichiers plus gros devraient en théorie attirer plus de reconnaissance, car il est plus difficile de distribuer rapidement de larges fichiers. Une *moyenne de la taille des fichiers* a aussi été calculée pour chaque groupe. Le *nombre total de téléchargements* et la *moyenne de téléchargements* mesurent le nombre de fois qu'un fichier a été téléchargé par le public en général. Il s'agit donc d'une mesure de la réputation populaire des groupes. Le *prix total, le plus haut prix et le plus bas prix des fichiers* ont été calculés en utilisant le site de vente en ligne d'Amazon. Nous avons à nouveau conçu un logiciel qui a utilisé le nom des produits piratés pour en obtenir la valeur marchande sur le site d'Amazon. Cette technique est limitée de par le fait que nous n'avions accès qu'au prix actuel des produits. Ainsi, un film lancé en 2003 vaudra assurément beaucoup moins six ans plus tard. Notre logiciel ne pouvant inférer le prix original, il était donc obligé d'utiliser le prix actuel. Pour finir, nous avons également regroupé en cinq catégories les 22 types de produits

affichés sur le site d'index : films, jeux de console, jeu pour PC, logiciels, vidéo XXX. Une mesure de la *spécialisation* des groupes a été calculée pour vérifier si les groupes qui participaient à chacune de ces sous-scènes étaient à même de créer davantage de liens et ainsi d'augmenter leur réputation.

Pour bien comprendre la dynamique derrière la distribution de la reconnaissance, nous nous devions aussi de nous intéresser aux liens sociaux qui unissent les différents groupes de pirates. Ce type d'analyse mieux connu sous le nom d'analyse de réseaux sociaux (ARS) cherche à identifier la structure des réseaux ainsi que la position de chacun de ses participants (Wasserman & Galaskiewicz, 1994: 4).

Les analyses de réseaux sont basées sur des matrices de relations. Ces matrices permettent de mesurer l'absence ou la présence de liens entre chacun des acteurs d'un réseau (une matrice binaire dirigée en termes de réseaux sociaux). Chaque groupe de pirates est un acteur et chaque salutation dans un fichier NFO est un vecteur entre deux acteurs. Nous avons utilisé le logiciel Ucinet 6 (Borgatti, Everett et Freeman 2002) pour dériver des variables de réseau pour chaque groupe et pour le réseau dans son ensemble. Les variables de réseau incluent des mesures de densité et de centralité. Il s'agit des mesures les plus couramment trouvées dans la recherche d'ARS. La *densité* est définie comme le niveau de cohésion au sein d'un réseau social et est mesurée en divisant le nombre de liens directs (ou dyades) observés sur le nombre maximum de liens directs qui sont possibles dans le réseau. C'est donc une mesure de la connectivité des acteurs au niveau du réseau. Nous avons également examiné la densité au niveau local avec le *coefficient d'agglomération*. Cette mesure évalue la densité au niveau des sous-groupes d'une population et est essentiellement une mesure de la densité du réseau personnel au sein d'un réseau complet (Watts, 1999). Il est un bon indicateur de la présence de sous-groupes ou cliques dans un réseau. Le degré entrant et le degré sortant tiennent compte du sens des relations et indiquent, respectivement, le nombre de *contacts entrants* et *sortants* de chaque acteur (Freeman, 1979). La *centralité d'intermédiarité* évalue la mesure dans laquelle un acteur se positionne sur le plus court chemin entre deux autres personnes. Plus un individu se situe entre deux acteurs, plus sa centralité d'intermédiarité sera élevée (Freeman, 1979). Ce type d'acteur est connu sous le nom de courtier et joue un rôle très

important dans les réseaux, car il contrôle les flux d'informations. Il décide donc quelles informations ils laissent passer et quelles informations ils retiennent (Morselli, 2009).

Les analyses de ces variables sont divisées en deux parties dans l'article. Dans la première, des analyses descriptives qui incluent le minimum, le maximum, la moyenne, la médiane et l'écart-type sont offertes pour toutes les variables. Dans la seconde, nous utilisons une corrélation de Pearson (Pearson, 1895) pour comprendre la relation qui unit la reconnaissance aux autres variables contrôles. La corrélation de Pearson explique un lien de covariance entre deux variables. Le coefficient peut varier de +1 à -1 tout dépendant du sens de la relation. Une corrélation près de 0 indique une faible covariance et une corrélation près des extrêmes indique que les deux variables mesurent deux phénomènes au comportement très similaire. Les analyses de corrélation sont de par leur nature bivariée et ne permettent pas d'établir des relations de cause à effet. Elles ne nous renseignent que sur les différences entre les mouvements dans les données pour chaque variable.

4.2 Les botnets

Ce deuxième article a aussi été rédigé en réaction face à la littérature actuelle portant la cybercriminalité. Dans ce cas en particulier, plusieurs chercheurs en sciences informatiques ont réussi à mettre la main sur des données des plus intéressantes de marchés illicites en ligne (Motoyama et al., 2011 par exemple). Dans tous les cas, les données étaient analysées de façon descriptive et superficielle. Ces recherches furent une grande source d'inspiration et nous permirent de comprendre tout le potentiel que de tels marchés pouvaient receler. La question de la réputation dans ces articles n'était abordée que rapidement sans être développée à l'aide d'un cadre théorique quelconque. Il s'agit d'une lacune que nous tenions à corriger en rédigeant cet article qui vise à comprendre pourquoi certains individus arrivent à amasser une meilleure réputation que d'autres dans le contexte d'un marché criminel de botmasters. Le marché étudié pour ce papier est un forum de discussion où des individus venaient pour discuter, acheter ou vendre des biens et services en lien avec les botnets.

Un tel nexus de criminels est un point de départ intéressant pour l'étude de la réputation criminelle de par la diversité des profils des individus qui le fréquente. Nous y retrouvons tout d'abord des programmeurs qui viennent y vendre des logiciels de commande et de contrôle

d'ordinateurs infectés. Ceux-ci fréquentent aussi ce type de forum pour développer leurs connaissances techniques ou trouver d'autres codeurs malveillants en mesure de les aider. Comme ces programmeurs n'utilisent pas eux-mêmes les logiciels de centre de contrôle, ceux-ci se doivent d'interagir avec des gestionnaires de botnets. Ces derniers utilisent ces logiciels pour infecter des machines et gérer les activités de leur botnet. Bien que le botnet fonctionne plus ou moins de façon autonome sur une base quotidienne, il a toujours besoin d'un minimum de surveillance humaine. Par exemple, des serveurs d'entreposages doivent être configurés pour recevoir toutes les informations volées par les botnets. D'autres serveurs doivent aussi être loués afin d'héberger des sites de fraude en ligne. Encore une fois, ces services ne sont que rarement utilisés à des fins personnelles. Les botmasters préfèrent louer leurs ressources à d'autres criminels qui se chargeront, eux, de mettre à bon escient les ressources des botnets. Les botmasters ne sont donc que des grossistes qui offrent au plus offrant les services illicites dont ils ont besoin. À la lumière de ces faits, un forum en ligne de botnets est donc un marché florissant où des codeurs, des gestionnaires de réseaux de zombies et des acheteurs se rencontrent pour acheter et vendre des logiciels et des services. Cette promiscuité entre différents types de criminels nous est apparue comme un milieu tout indiqué pour mieux comprendre la distribution de reconnaissance dans un contexte de marché criminel. Comme les différents acteurs sont issus de milieux différents et qu'ils ont des expériences distinctes, les relations interpersonnelles et les liens de confiance entre eux s'annoncent difficiles dans le meilleur des cas. La réputation promet alors de prendre davantage d'importance dans un tel contexte. Tout son impact sur les relations et la performance devrait donc être on ne peut plus transparent dans un tel environnement.

Il existe un grand nombre de marchés illicites qui offrent l'opportunité aux botmasters de se retrouver. Tous ne sont malheureusement pas accessibles publiquement. Afin de respecter les règles d'éthiques les plus strictes, nous nous sommes tournés vers un forum ouvert au public et actif depuis plusieurs années. Les individus qui contribuent à cette plateforme ne bénéficient d'aucune protection de leur vie privée, car l'information qu'ils publient est accessible à tous. Nos résultats montrent que tout comme dans le cas des médias sociaux, les individus laissent souvent filtrer plus d'informations qu'ils ne le voudraient.

Afin de pouvoir extirper le maximum de données de ce marché, nous avons conçu un programme connu dans le monde informatique sous le nom de *scraper* qui permet de copier dans une base de données des parties d'une page web. Ce logiciel maison nous a permis de télécharger une copie de tous les messages mis en ligne entre le 3 février 2007 et le 26 novembre 2011. Il nous a aussi permis d'obtenir une copie du profil personnel de chacun des membres de ce marché. Au total, la banque de données de ce marché comptait 20 270 profils ayant mis en ligne 248 634 messages.

Tout comme dans tous les marchés illégitimes, il n'existe aucun recours juridique pour les botmasters en cas de différend avec un partenaire d'affaires. Pour se protéger contre les membres adoptant des comportements opportunistes, les membres du forum utilisaient un indice de réputation (voir section précédente sur les systèmes automatisés de reconnaissance). Les membres ayant atteint un certain niveau de confiance et de réputation dans la communauté en ligne ainsi que ceux qui payaient une redevance recevaient de la part des administrateurs du forum le droit de donner et/ou d'enlever des points de réputation aux autres utilisateurs. Ce processus était simple et rapide; il s'agissait pour cela d'utiliser un formulaire en ligne qui n'était jamais à plus d'un clic ou deux de souris. L'utilisateur pouvait alors choisir le nom de l'usager à qui il désirait ajouter ou retirer des points ainsi que le nombre de points désiré. Il n'était pas nécessaire que deux membres aient eu une transaction entre eux pour qu'ils aient le droit de modifier la réputation l'un et l'autre. Un simple message ou un acte de courtoisie étaient parfois suffisants pour hausser le niveau de réputation d'un individu.

Chaque utilisateur commençait sa carrière sur le forum avec un total de 0 point et gagnait (ou perdait) des points au fil du temps. Dans le cas du forum étudié, le système de reconnaissance était basé sur la reconnaissance des pairs et non des administrateurs. Cela signifie que les personnes responsables du forum refusaient de modifier la réputation d'un membre à moins d'un cas de force majeure. Les administrateurs étaient d'ailleurs fiers de ce libre marché de la reconnaissance. Tel que mentionné dans le Chapitre 3, ce système automatisé de reconnaissance n'est pas unique aux forums criminels et est utilisé dans de nombreuses plates-formes en ligne pour diminuer les comportements opportunistes des membres. En général, les personnes qui visitent ces forums en ligne ont tendance à connaître

comment ces systèmes fonctionnent et comptent sur eux pour sanctionner les comportements criminels.

En plus de connaître le score de réputation de chaque membre, nous étions aussi en mesure d'inférer plusieurs informations en parcourant les messages téléchargés. Chaque message mis en ligne comprenait le nom de son auteur, l'heure et la date de sa publication ainsi que le message lui-même. Les profils personnels des membres étaient aussi une source très importante de données et contenaient pour leur part un nom d'utilisateur, la date d'enregistrement du profil, la date de la dernière visite sur le forum, la date de naissance, l'heure locale de l'utilisateur, le nombre de fois où l'utilisateur a changé son nom d'utilisateur, le nombre total de messages mis en ligne, le nombre de personnes référées sur le forum, le nombre de clans dont faisaient partie l'utilisateur, des mentions honorables ainsi qu'un score de réputation.

La plupart de ces variables n'ont pas besoin de davantage d'explications. Deux variables font cependant exception : les clans et les mentions honorables. Dans ce forum, huit clans étaient actifs. À l'image d'une équipe de sport professionnel, bien des gens auraient aimé faire partie de ces clans, mais seulement un nombre limité de personnes y était invité. Les clans fonctionnaient donc sur un mode d'invitation et conféraient à leurs membres une reconnaissance accrue et exclusive ainsi qu'un accès à des sections privées du forum. Il s'agissait donc d'une forme de reconnaissance recherchée. Les mentions honorables pour leur part étaient décernées par les administrateurs du forum et soulignaient certains accomplissements particuliers d'un utilisateur. Il existait plus de cinquante mentions honorables différentes, dont celui signalant les talents graphiques (*Graphic Master*) ou encore l'acumen en affaires (*Businessman*). Tout comme pour les clans, ces distinctions n'étaient remises que sur invitation et étaient très recherchées par les membres.

Toutes ces données sont à la base d'un modèle prédictif multiniveau qui mesure quantitativement l'effet de variables indépendantes statiques et dynamiques sur notre variable dépendante, la réputation (Raudenbush et al., 2004). Cette réputation a été mesurée à l'aide du système automatisé de reconnaissance décrit ci-dessus. Elle varie de -729 à 2297 et la moyenne pour chaque membre est de 21.94 points.

Au niveau des variables indépendantes, nous avons tout d'abord mesuré le *nombre de jours passés sur le forum* en calculant la différence entre la date d'enregistrement sur le forum et la date de la dernière visite. Chaque profil contenait par ailleurs l'*âge* tel que décliné par le membre. Les informations sur l'âge ne peuvent être vérifiées dans le contexte de marchés en ligne et la distribution des âges (Min = 12; Max = 101) soulève des doutes sur la validité de l'ensemble des données de la population. Une étude manuelle des données montre cependant une distribution de l'âge censurée vers la gauche tel qu'espéré dans le contexte de cybercriminels. Étant donnée le grand nombre de profils, les quelques valeurs extrêmes ne seront pas en mesure de modifier la tendance lourde et de noyer le signal dans une mer de bruit.

L'activité des membres sur le forum a été mesurée à l'aide du *nombre de messages* mis en ligne. Il était important en effet de tenir compte de l'implication de chaque membre, car à durée de vie égale, les membres totalisant le plus de messages risquaient d'avoir un impact plus important sur la communauté et ainsi d'obtenir un score de réputation plus élevé. Cette implication a aussi été mesurée de plusieurs manières en utilisant le *nombre de mentions honorables*, le nombre d'*abonnements à des clans* ainsi que le *nombre de personnes référées* par chaque membre.

L'*origine* de chaque botmaster a été estimée en comparant l'heure locale de l'individu comme indiqué sur le forum avec l'heure locale des chercheurs. La différence en heures représente le nombre de fuseaux horaires séparant les chercheurs du botmaster. Les profils ont été divisés en cinq catégories soit : 1) l'Amérique; 2) L'Océanie; 3) L'Europe, l'Afrique et l'Asie; 4) l'Asie et; 5) Inconnu. Cette typologie crue et imparfaite donne une idée générale de l'endroit où se trouvaient les acteurs de ce marché. Certains fuseaux horaires traversent plusieurs continents et ne nous permettaient pas malheureusement d'identifier avec précision l'origine des acteurs. Ainsi, les membres asiatiques ont dû être séparés en deux catégories distinctes étant donné que certains fuseaux traversent autant l'Europe, l'Afrique que l'Asie. C'est d'ailleurs dans cette dernière catégorie qu'une majorité (55.19 %) des membres du forum résidait.

Pour acquérir une compréhension plus approfondie des messages sur le forum, nous nous sommes tournés vers un logiciel spécialisé dans l'analyse automatique de contenu appelé SentiStrength. Ce dernier a été utilisé avec succès dans le passé pour estimer les sentiments tant positifs que négatifs de messages (Thelwall et al., 2010; Thelwall et al., 2012). Le programme a été évalué dans des revues et journaux académiques et a prouvé sa capacité à mesurer avec une relative précision les sentiments des messages. Le logiciel attribue une note à chaque message sur une échelle de 1 à 5 pour son sentiment positif et sur une échelle de -1 à -5 pour son sentiment négatif. Chaque message reçoit donc à la fois un score positif et négatif, car il peut contenir des sentiments divergents (ex.: "je m'aime moi-même, mais je vous hais tous»). Selon l'échelle de SentiStrength, les scores de 1 et de -1 indiquent messages neutres. Pour faciliter les analyses, nous avons soustrait 1 de tous les scores positifs et ajouté 1 à tous les scores de sentiments négatifs. Une somme totale des points positifs et des points négatifs a été mesurée pour chacun des membres afin d'indiquer la *qualité des relations* de chacun des membres. Un échantillon aléatoire de messages a été testé manuellement pour s'assurer de la validité des résultats fournis par SentiStrength.

Pour bonifier cette compréhension des relations interpersonnelles, nous avons également mesuré le *capital social* des membres du forum à travers deux paramètres soit la taille du réseau personnel de chaque membre ainsi que son niveau de contrainte. La taille du réseau personnel fait référence au nombre de personnes en contact direct avec un individu. La contrainte est un concept développé par Burt (1992) et mesure la présence de liens redondants dans un réseau personnel. Lorsque tous les amis d'un individu se connaissent personnellement, ils n'ont plus besoin de leur ami commun pour entrer en contact les uns avec les autres. Il devient évident que le pouvoir ou le contrôle de l'ami commun est faible dans ce contexte, car il est redondant dans son cercle social. La littérature indique qu'il est beaucoup plus stratégique d'éviter ces liens redondants afin de se maintenir en position de force (Morselli, 2001).

Pour construire les matrices de relations entre membres du forum, nous nous sommes basés sur les messages publics affichés sur le forum. Les messages de forums sont divisés en sujets de conversation. Chaque sujet de discussion contient une liste de messages classés en ordre chronologique inverse. Dans un tel contexte, déterminer automatiquement à qui

s'adresse chacun des messages est une tâche impossible, car ils pourraient être dirigés à l'ensemble des personnes ayant pris part à la conversation auparavant ou encore à un membre en particulier. Pour maximiser la représentativité et réduire les ressources nécessaires au processus de création des liens, nous avons conçu un algorithme que nous expliquerons à l'aide du Tableau 1.

Tableau 1 : Exemple de liste de messages dans une conversation

RANG DU MESSAGE	NOM
8	Peter
7	Mike
6	Donald
5	Mike
4	Jeff
3	Holly
2	Mike
1	James

Dans l'exemple du Tableau 1, une conversation contient huit messages mis en ligne par six personnes (James, Mike, Holly, Jeff, Donald et Peter). Notre algorithme commence toujours par le dernier message affiché (dans ce cas-ci Peter) et enregistre un lien entre l'auteur du message et tous les membres ayant participé à la discussion avant lui. Dans ce cas, Peter serait lié aux cinq autres personnes avant lui (James, Mike, Holly, Jeff et Donald). Il en irait de même pour Donald qui serait lié à Mike, Jeff, Holly et James. Si une personne a affiché plusieurs messages (comme Mike dans cet exemple), nous n'enregistrons qu'un seul lien avec cette personne. Ainsi, dans le cas présent, même si Mike parle à deux reprises avant Donald, il n'y aurait qu'un seul lien entre eux. Le cas de Mike est légèrement différent de celui des autres et est représentatif de bien des sujets de conversations. Le premier message de Mike (rang #2) s'adresse uniquement à James. Nous pouvons cependant supposer que son deuxième message (rang #5) ne s'adresse qu'aux personnes ayant pris la parole depuis son dernier message (Jeff et Holly). Notre algorithme tient ainsi compte des auteurs qui inscrivent

plusieurs messages nous permettant ainsi de raffiner notre mesure des interactions entre les individus. Le dernier message de Mike (rang #7) ne serait donc adressé qu'à Donald.

La dernière variable indépendante du modèle mesure finalement le *nombre de changements de surnoms* de chaque membre. Comme ce surnom est l'identifiant principal de chaque individu sur les marchés, un changement de nom indique une tentative de camoufler son identité à la communauté. Chaque membre recevait un identifiant numérique unique qui ne pouvait être modifié. En changeant son surnom, un acteur pouvait ainsi se faire passer pour un autre membre auprès de la communauté en général. Il conservait par contre son identifiant unique ce qui lui permettait de prouver sa vraie identité à ses contacts passés. Les membres les plus attentifs pouvaient aussi par contre remarquer que deux membres avaient le même identifiant et dénoncer publiquement le changement de surnom d'un individu.

Toutes ces variables indépendantes ainsi que la variable dépendante sont d'abord présentées dans l'article sous la forme de statistiques descriptives qui incluent le minimum, le maximum, la moyenne et la médiane. La seule exception est la variable d'origine qui est présentée en termes de pourcentage de distribution. Cette première étape nous donne un portrait global de ce marché illicite ainsi que des personnes qui y participent.

Pour la seconde partie des analyses, nous présentons cinq modèles d'analyses multiniveaux qui prédisent la distribution de reconnaissance dans un marché illicite en ligne. Pour atteindre cet objectif, nous avons utilisé la modélisation linéaire hiérarchique (MLH) aussi connue sous le nom d'analyses multiniveaux (Raudenbush et al., 2004). Cette méthode statistique permet de prédire le comportement d'une variable en tenant compte des variations d'une même personne au fil du temps (niveau 1), ainsi qu'entre différentes personnes (niveau 2). Pour réaliser ces analyses, nous avons utilisé le logiciel HLM 7 qui est spécialisé dans le calcul de modèles multiniveaux (Raudenbush et al., 2004). Fischer et al. (2008) en décrivent le fonctionnement.

Une MLH commence par une équation de régression pour chacun des individus de la population. Ce premier niveau est connu sous le nom de niveau 1. Cette régression évalue la probabilité qu'un événement se soit produit pendant une période de temps donnée. Dans notre cas, nous avons estimé la probabilité qu'un individu reçoive ou perde des points de réputation

au cours d'un mois donné. Cette régression est donc basée sur les variables dynamiques du modèle. Chaque variable dynamique ainsi que la variable indépendante sont mesurées à intervalle régulier; pour chaque mois dans le cas de nos données. Notre échantillon s'étend sur une période de 26 mois allant d'octobre 2009 à décembre 2011. Les variables dynamiques incluent le nombre de jours passés sur le forum, l'âge, le nombre de messages écrits, le nombre de mentions honorables, le nombre de points de sentiment positif, le nombre de points de sentiment négatif, la taille du réseau personnel et le niveau de contrainte.

La MLH inclut aussi des données qui sont statiques dans le temps et qui sont classées dans le niveau 2. Dans notre cas, il s'agit du nombre de changements de surnoms, du nombre d'abonnements à des clans, du nombre de personnes référées et de l'origine. Une seule mesure de ces variables a été réalisée, et ce, pour l'ensemble de la durée de la période d'observation. De toutes les variables de niveau 2, seulement une peut être classée comme théoriquement statique : l'origine. Pour les autres, nos données n'étaient pas suffisamment sensibles pour nous permettre de calculer sur une base mensuelle l'évolution des tendances. Nous avons donc dû classer ces variables au niveau 2 même si, du point de vue théorique, il s'agit en fait de variables dynamiques.

La combinaison des deux régressions (niveau 1 et niveau 2) produit deux coefficients qui nous permettent de mesurer l'impact des variables (coefficient Y) et la taille relative de chacune des variables par rapport aux autres (coefficient T). Un coefficient T égal ou supérieur à 1,96 indique que la relation entre une variable indépendante et la variable dépendante est statistiquement significative. Cinq modèles linéaires hiérarchiques sont présentés dans la section des résultats. Pour chacun d'eux, la variable dépendante est le nombre de points de réputation reçus ou perdus chaque mois. Cette mesure a été recodée sous le format -1/0/1 en fonction de la perte, du gain ou statu quo de la réputation. Nous avons opté pour cette stratégie d'analyse afin de faciliter l'interprétation des résultats ainsi qu'en raison du grand nombre de cas où aucune reconnaissance, tant positive que négative, n'était donnée. Cette transformation nous permettait donc ne normaliser d'avantage la distribution de notre variable. Ce faisant, nous perdons il est vrai une certaine sensibilité dans nos résultats car un individu qui recevrait plus de reconnaissance positive que négative dans un même mois serait classé dans la catégorie positive (+1) malgré le fait que certains de ses comportements l'ait amené à amasser

une reconnaissance négative. Pour mesurer l'impact de cette perte de sensibilité, nous avons calculé la distribution de tous les scénarios possibles :

1) Recevoir de la reconnaissance positive : 13.1%
2) Recevoir de la reconnaissance positive et négative (plus de positif que de négatif) : 2.1%
3) Recevoir autant de reconnaissance positive que négative : 0.3%
4) Ne pas recevoir de reconnaissance : 81.9%
5) Recevoir de la reconnaissance positive et négative (plus de négatif que de positif) : 0.8%
6) Recevoir de la reconnaissance négative : 1.8%

Cette distribution indique qu'il existe en effet un biais dans nos analyses, particulièrement dans le cas de la catégorie -1 où le tiers de l'échantillon a accumulé de la reconnaissance positive et négative. Cette limite n'est cependant pas aussi problématique qu'il n'y parait à priori. En effet, les participants du forum n'avaient en général accès qu'au score total de réputation des individus plutôt qu'au détails de toutes les marques de reconnaissance. Dans ce contexte, la majorité des participants au forum n'étaient témoins que du résultat final de toutes ces transactions de reconnaissance. Notre méthodologie reproduit donc ce que les membres réguliers du forum voyaient soit la somme totale de toutes les marques de reconnaissance.

Un modèle de régression linéaire a été choisi pour ces analyses compte tenu de la répartition de la reconnaissance auprès de la population. Le modèle 1 présente un modèle de base sans variables indépendantes. Le modèle 2 et le modèle 3 présentent respectivement l'impact des variables de niveaux 1 (variance dans le temps) et 2 (variance entre les individus). Le modèle 4 inclut toutes les variables indépendantes dans un même modèle. Enfin, le modèle 5 est le modèle parcimonieux qui incorpore uniquement les variables statistiquement significatives.

4.3 Le carding

Ce troisième et dernier article de thèse avait pour but de finalement répondre à notre principale question de recherche et donc de déterminer s'il existe bien un lien entre la

réputation et la performance criminelle. Étant donné l'écrasante littérature sur le sujet dans le monde légitime et les nombreux parallèles entre les marchés licites et illicites, notre hypothèse de départ est qu'une bonne réputation peut significativement augmenter la performance dans un contexte de marché criminel. Les deux premiers articles nous ont permis de comprendre comment la reconnaissance se distribue dans deux contextes criminels soit la scène des warez et la communauté des botmasters. Les données de ces deux études ne se portaient malheureusement pas à ce genre d'analyse de par le manque d'informations sur les transactions entre criminels. Pour comprendre la distribution de la performance et ses corollaires, nous nous sommes donc tournés vers un autre marché en ligne où les cardeurs se réunissaient pour acheter et vendre des données financières volées. Nous retrouvions dans cet écosystème la même diversité de criminels qui se trouvaient dans le marché étudié dans la recherche précédente. À la différence de l'autre marché cependant, l'origine des données nous permettait d'avoir un accès complet à la communauté et de pirater les pirates en quelque sorte.

Cet accès particulier est une conséquence directe de la constante compétition à laquelle se livrent les marchés illicites. La source de cette compétition vient des administrateurs de ces plateformes virtuelles. Chaque marché est géré en effet par sa propre équipe d'administrateurs qui est chargée de l'élaboration du code de conduite ainsi que de sa mise en application. Pour ce travail, les administrateurs se rémunèrent indirectement en prélevant un pourcentage des ventes ou en offrant des services comme la validation d'informations achetées ou encore un service de compte en fidéicommis. Les transactions peuvent ainsi se dérouler avec moins d'incertitude étant donné que l'argent ne sera versé au vendeur que lorsque la marchandise aura été inspectée. Conséquemment, les marchés ayant le plus de transactions ont le potentiel de rapporter beaucoup d'argent à leurs administrateurs. Afin de nuire à la compétition et augmenter l'achalandage de leurs marchés, les administrateurs sont souvent tentés de pirater leurs adversaires afin de voler des informations confidentielles ou encore nuire à leur réputation. Dans quelques cas, de telles attaques ont porté fruit et ont conduit à la distribution publique de copies entières de forums en ligne hébergeant des marchés illicites. Ces fuites contiennent habituellement tous les messages privés et publics des membres des forums ainsi que tous leurs profils personnels. Certaines des recherches que nous avons mentionnées ci-dessus (Monsma et al., 2002) ont profité de l'accès à de telles bases de données afin de mieux

comprendre les marchés criminels. Leurs études étaient cependant très limitées, superficielles et n'étaient basées sur aucun cadre théorique.

Pour remédier à ces lacunes, nous avons été téléchargé une copie d'un marché illégitime en utilisant le moteur de recherche de Google. De telles données sont relativement aisées à trouver, mais sont souvent infectées par des virus et autres codes malveillants. Nous avons donc utilisé une machine non connectée à l'internet afin de nettoyer les fichiers contenant les données. Le résultat est un portrait complet d'un marché de cardeurs actif entre 2007 et 2009. Cet ensemble de données comprend tous les messages publics et privés ainsi que tous les profils des membres. Au total, c'est 858 744 messages publics, 501 913 messages privés et 18 834 profils qui ont pu être récupérés. Comme les cardeurs utilisent habituellement la messagerie privée du forum pour négocier des transactions, un accès à ces échanges était nécessaire pour la réalisation de cette étude. Un autre point central de cette recherche est la notion de réputation. Comme bien des marchés, cette plateforme utilisait aussi un système automatisé de reconnaissance, mais ce système n'a été activé par les administrateurs que le 25 août 2009 soit 85 jours avant le piratage du forum. Cela nous a malheureusement forcé à ne tenir compte que des données issues de cette période fenêtre de 85 jours où le système de reconnaissance était actif. Toutes les analyses sont donc basées sur l'activité des cardeurs entre le 25 août 2009 et le 18 novembre 2009.

Il existe plusieurs façons de modéliser la performance criminelle dans le contexte de marchés illicites. Un devis de recherche idéal nous permettrait de mesurer la qualité et la quantité des biens et services vendus ainsi que le montant des revenus associés à ces transactions. En théorie, une telle étude serait possible, mais requerrait un investissement important de ressources pour passer au travers de tous les messages publics et privés (plus d'un million dans notre cas). Par ailleurs, plusieurs marchés illicites sont organisés autour de populations ne parlant pas anglais. Dans ce contexte, toute étude sérieuse nécessiterait des chercheurs qu'ils parlent des langues comme le russe ou l'allemand ou encore qu'ils engagent des traducteurs spécialisés dans le domaine de la cybercriminalité. Certains chercheurs ont opté pour cette méthodologie, mais ont dû se limiter à un nombre très limité de messages afin de limiter les coûts. Leurs travaux ne peuvent donc être généralisés à l'ensemble du forum.

Pour contourner ce problème, nous avons plutôt décidé d'aborder la question de la performance criminelle sous l'angle des opportunités criminelles. Ce concept mesure l'accès à des opportunités de commettre des crimes et a été associé à la réussite dans le cas de marchés criminels dans le passé (Charette, 2012; Charest, 2007). Il n'existe pas un ratio de 1 :1 entre les crimes commis et les opportunités criminelles, mais la corrélation entre les deux concepts est forte et positive. Ces opportunités peuvent être mesurées de deux façons soit en fonction du nombre de transactions auxquelles un individu a accès ou encore par le montant des gains qui y sont associés. Pour cette recherche, nous nous concentrerons sur la première méthode. La variable dépendante de cette étude sera donc la fréquence des opportunités criminelles pour chacun des membres. Encore plus spécifiquement, nous regarderons le nombre de jours qui sépare deux opportunités afin de comprendre les variations dans les variables indépendantes qui ont rallongé ou réduit ce délai.

Détecter automatiquement les opportunités criminelles n'est pas une chose aisée. Pour y arriver, nous avons recherché, dans les messages privés, tous les messages contenant un chiffre précédé ou suivi des symboles ou mots suivant : "$", "dollar", "dolar", "€" ou "euro". Cela nous a permis d'identifier rapidement les messages qui font référence à une opportunité criminelle. Comme mentionné dans la section sur les formes particulières des cybercrimes, les cardeurs ont l'habitude d'afficher publiquement une liste des produits et services qu'ils ont à offrir et d'attendre des réponses dans leurs messages privés. En identifiant les messages contenant un montant en dollar ou en euro, nous sommes en mesure d'identifier rapidement les discussions portant sur une possible transaction. Afin de limiter les possibles doublons, nous n'avons conservé qu'une seule dyade pour chaque période de 48 heures. Ainsi, si deux personnes échangeaient plusieurs messages contenant des montants d'argent au courant de la même période de 48 heures, une seule connexion était conservée. De notre échantillon initial de 18 834 profils, 1 773 membres ont envoyé ou reçu un tel message durant notre période fenêtre. Les autres (n = 14 841) ont été retirés de nos analyses. Ce type de données ne donne malheureusement pas le sens des transactions. Nous ne pouvons qu'affirmer que deux personnes ont eu accès à une opportunité criminelle à une date précise. Notre échantillon de 1 773 personnes a eu accès à un total de 3 409 opportunités criminelles au cours de la période fenêtre. La moyenne d'opportunités est donc de 1.92 par membre (Écart-type = 2.04). Un peu

plus de la moitié de ces opportunités (50.3 %) ont été suivies par d'autres opportunités. En moyenne, le temps entre deux opportunités était de 50.3 jours (Écart-type = 102.09).

La variable dépendante de cette étude est donc le temps nécessaire pour obtenir une seconde opportunité criminelle. Notre objectif est de comprendre comment certaines variables indépendantes peuvent influencer à la hausse ou à la baisse cette mesure de la performance. Pour ce faire, nous utiliserons tout d'abord une mesure de la réputation de chaque membre en nous référant à la théorie de Glückler & Armbrüster (2003). Les trois types de réputation (publique, basée sur l'expérience et réseautée) ont été opérationnalisés pour le bien de cette recherche. La réputation publique a été mesurée à l'aide du système automatisé de reconnaissance du marché illicite. Les membres étaient responsables de l'attribution des points à chacun des participants du marché et il leur était impossible de retirer des points aux autres. Cette échelle de réputation offre une bonne image de la réputation publique de chacun des membres. En moyenne, chaque acteur avait 1.57 point de réputation au moment de leur première opportunité criminelle (Écart-type = 6.59). La réputation basée sur l'expérience a été mesurée en examinant si deux membres impliqués dans une même opportunité avaient déjà eu une relation dans le passé. C'était le cas dans 10,3 % (n = 352) des opportunités. Finalement, la réputation réseautée a été mesurée en se penchant sur les relations indirectes des partenaires d'affaires. Si ceux-ci avaient déjà eu une opportunité criminelle avec un ami commun, ils avaient alors utilisé la réputation réseautée. Tout comme sur Facebook, il était possible pour les membres du marché de se bâtir une liste d'amis officiels sur le forum. Nous nous sommes basés sur ces listes officielles d'amitié pour déterminer les liens entre les membres et la présence de réputation réseautée. Dans 8,3 % (n = 283) des opportunités, les participants avaient déjà eu une opportunité avec un ami commun.

Il existe aussi d'autres façons de mesurer la réputation dans le contexte de marchés illicites. Chaque membre était en effet libre de porter plainte contre tout autre membre ayant enfreint les règlements du marché. Les administrateurs étaient alors responsables d'évaluer le bien-fondé de la plainte et le cas échéant de donner un avertissement à la personne fautive. Dans le cas d'infractions répétées, un individu pouvait se voir banni de la communauté. Ces deux actions (avertissement et exil) sont des mesures de la réputation négative des individus. Les membres avaient accumulé en moyenne 1.2 avertissement (Écart-type = 2.1). De notre

échantillon, 318 (9,3 %) individus ont finalement été bannis du marché avant la fin de la période fenêtre.

Pour s'assurer d'une fiabilité maximale, nos analyses incorporent aussi plusieurs variables contrôles. Nous avons tout d'abord tenu compte du nombre de transactions antérieures ainsi que du nombre de sujets de discussion créés par les membres. Cette dernière variable nous permettait de mesurer l'implication des membres dans le monde du carding. Ces discussions étaient généralement commencées afin de vendre des biens ou des services illicites. Un plus grand nombre de discussions lancées par un individu indiquent donc indirectement la présence d'un plus grand fournisseur. Nous avons aussi inclus dans nos analyses une mesure du nombre de jours écoulés depuis les débuts du forum (M = 891.91; Écart-type = 26.63) afin de contrôler pour la fin abrupte de la période d'observation.

Notre modèle tenait finalement compte de la structure des réseaux sociaux pour mieux comprendre les activités des participants et la façon dont ceux-ci s'intégraient dans le réseau. La matrice de relation a été bâtie à l'aide des messages privés échangés par les membres. Ces données riches nous ont permis de calculer non seulement le nombre de liens entrants et sortants, mais aussi la direction des messages (qui écrivait à qui). Trois mesures ont été utilisées pour décrire la structure du capital social de chaque membre: le degré de centralité, la centralité d'intermédiarité et la contrainte du réseau. Les membres avaient en moyenne un degré de centralité de 134.2 (Écart-type = 287,50). La centralité d'intermédiarité était en moyenne de 80,557.37 (Écart-type = 600,617.44). Finalement, la contrainte du réseau s'établissait en moyenne à 0,21 (SD = 0,30).

La première série d'analyses de cette recherche a tenté de comprendre l'impact des trois types de réputation sur la performance criminelle dans un modèle bivarié. Pour ce faire, nous avons utilisé des courbes de survie générées à l'aide de l'estimateur Kaplan-Meier (1958) et comparées entre elles en utilisant la méthode de classement par log de Mante-Cox (Mantel, 1966).

Nous avons par la suite poursuivi ces analyses en mode multivarié. Tout comme dans le cas des courbes de survie bivariées, toutes les variables dépendantes et indépendantes définies jusqu'ici ont été utilisées dans un modèle d'analyse de survie à mesures répétées.

Dans ce type d'analyse, une mesure des variables indépendantes est prise à chaque occurrence de la variable dépendante. Dans le cas présent, nous avons donc pris un relevé de chacune des variables indépendantes pour chaque individu à chaque jour pour lesquels nous avions détecté une opportunité criminelle. Les variations dans les variables indépendantes devraient en théorie être capables d'expliquer le délai plus ou moins long entre deux opportunités.

Cette technique d'analyse est mieux connue sous le nom d'analyse de survie multivariée pour évènements récurrents. Elle a été réalisée à l'aide d'un modèle de risque proportionnel de Cox à estimation robuste (Anderson & Gill, 1982; Therneau & Grambsch, 2000). Ce type d'analyse s'applique particulièrement bien, car il tient compte de la censure à droite dans les valeurs de la variable dépendante. Comme la probabilité de rencontrer une nouvelle opportunité diminue plus nous approchons de la fin de la période d'observation, un modèle de régression n'aurait pu donner une estimation rigoureuse de l'impact des variables indépendantes. Par ailleurs, l'hypothèse principale de cette étude est que le capital de réputation est un facteur qui influence le rendement criminel. Il serait cependant théoriquement aussi possible que la performance ait elle aussi influencé la réputation. La décision d'utiliser une analyse de survie a été motivée par notre volonté de contrôler pour cette possibilité. En introduisant un modèle dépendant du temps, nous nous assurons que la direction de l'effet est vraiment dans le sens de nos hypothèses. Des coefficients standardisés (β) ont été calculés pour chacune des variables indépendantes en utilisant un score Z.

Pour nous permettre une meilleure compréhension de la performance au niveau individuel plutôt qu'au niveau des opportunités, nous avons aussi agrégé certaines variables indépendantes au niveau personnel. Pour cette seconde vague d'analyse, nous avons mesuré le nombre total de transactions pour chacun des membres (M = 1.92; Écart-type = 2.04). Nous avons aussi mesuré la durée de vie des individus en calculant la différence entre la date de création du profil et la dernière activité sur le forum. En moyenne, les membres étaient actifs pendant 6.82 mois (Écart-type = 4,54). Le rapport entre ces deux dernières mesures a été calculé afin d'obtenir une approximation de la productivité des membres. La moyenne était de 0.55 (Écart-Type = 0.97) opportunité par mois. Pour analyser ces données, nous avons comparé les moyennes de notre échantillon total de 1 773 membres en les séparant en quatre groupes : (1) les personnes qui n'avaient pas de stratégie (n = 806; 45,5 %); (2) les personnes

qui ont eu au moins un point de réputation au cours de leur durée de vie, mais pas d'avertissements (n = 228, 12,9 %); (3) les personnes qui ont eu au moins un avertissement, mais pas de points de réputation (n = 503; 28,4 %) et; (4) les personnes qui ont eu au moins un avertissement et un point de réputation (n = 236, 13,3 %). Comme les postulats d'homogénéité de la variance n'étaient pas respectés dans les distributions (p de Levene < 0.05), nous avons utilisé un processus de classification non paramétrique (Kruskal & Wallis, 1952). Toutes les analyses, tant pour les données agrégées au niveau des opportunités qu'individuel, ont été réalisées à l'aide de la version 2.14.2 du logiciel R (R Core Team, 2012) et de l'extension d'analyse de survie version 2.36-14 (Therneau, 2012).

CHAPITRE 5 – WELCOME TO THE SCENE

Auteurs:
David Décary-Hétu
Carlo Morselli
Stéphane Leman-Langois

Publication :
Décary-Hétu, D. & C. Morselli & S. Leman-Langlois. (2012). "Welcome To The Scene: A Study Of Social Organization And Recognition Among Warez Hackers." *Journal Of Research In Crime And Delinquency*. 49(3): 359-382.

Abstract

OBJECTIVES. This paper seeks to describe and understand the social organization as well as the distribution of recognition in the online community (also known as the warez scene) of hackers who illegally distribute intellectual property online.

METHODS. The data was collected from an online index which curates a list of illegal content that was made available between 2003 and 2009. Sutherland's notion of behavior systems in crime as well as Boase and Wellman's notion of network individualism are used to theorize the social organization and the distribution of recognition in the warez scene. These were then analyzed using social network theory.

RESULTS. There is a strong correlation between the productivity of the hacking groups and the recognition they receive from their peers. These findings are limited by the lack of data on the internal operations of each hacking groups and by the aggregate nature of the network matrix.

CONCLUSIONS. We find that hacking groups that make this online community generally have a very limited life span as well as low production levels. They work and compete in a very distributed and democratic community where we are unable to identify clear leaders.

Keywords

Cybercrime, warez, hackers, social organization, recognition

Introduction

Peer-to-peer networks have become increasingly popular with internet users and terms such as BitTorrent are becoming part of common language. While some of the files distributed on these networks may be homemade videos or free and open software, most of the files available for download are pieces of intellectual property that were uploaded without the owner's direct consent (Craig, 2005). Such illegally distributed products are commonly known in the hacking underground under the term *warez* (Craig, 2005). While it is true that some of the warez comes from individuals who have shared their personal collections, current research on the phenomenon has shown that there exists a community of hackers who are specializing in the removal of copy-protection schemes and distribution of copyrighted material (such as books, music, movies, games, software). These hackers gather in groups (hacking groups) which have unique names and logos. The environment (or online community) they thrive in is called the warez scene (Craig, 2005).

In recent years, researchers have looked deeper into this scene using surveys and ethnographic accounts. This has generated a first glimpse into the inner workings of this illegal underground community. However, such research has only exposed segments of this scene at different times. The present study focuses on the overall warez scene through methods that have essentially allowed us to hack the hackers and discover the social organization and recognition patterns that structure this scene.

After a review of research in this specific area and a re-appraisal of past research extending from Sutherland's (1947) crime behavior system, we lay out the social network analytical strategy that we used to gather and analyze data on this community. The analysis that follows focuses on the key characteristics, structural features and survival of warez hackers. We conclude with a discussion on how such a contemporary and growing phenomenon should be addressed more fully by criminologists.

Hackers and the Warez Scene

The warez scene is distinct from other hacker communities. It is also one of the least researched. Wall (2001), for example, does not address warez hackers in his cybercrime typology. Such hackers would fall loosely into his "cyber trespass" category (the invasion of private space by a hacker) or "cyber theft" category (the theft of intellectual property or online

accounts). The warez hacker is also overlooked in Leeson and Coyne's (2005) typology of "good," "bad," and "greedy" hackers, possibly because financial gain is not an issue for such hackers and consumer attraction for their services makes it difficult to include them in any moralistic category. Nonetheless, Leeson and Coyne's work is important because it emphasizes recognition, which, as provided by peers through hacker forums and magazines, is the incentive for warez activity.

Although research specifically on the warez scene is scarce, some studies do provide an overview of its basic characteristics. The current literature on the warez scene can be divided into three segments: the regulation, the demand and the supply of warez products. We will cover each of these sections separately.

The regulation of the warez scene

Corporate associations have stated that online piracy has cost them billions of dollars (Marshall, 2006). In the case of the music industry, Leman-Langlois argues that many factors (and not just copyright infringement) need to be taken into account to explain the downward financial trends of copyright holders. The number of songs released annually, the sampling habits of online "pirates" and the high turnover in media platforms all need to be factored in when evaluating the industry's sales. According to him, there is, however, "no way to account correctly for industry losses" (Leman-Langlois, 2004). Marshall (2002) takes a similar stand and states that the "battle over copyright is in large part a publicity war" (Marshall, 2002: 7). According to him, the music industry is making use of the public image of artists as well as the empathy felt for honest hard-working individuals in the music industry to change ideas and public opinion about copyright infringement. Big music labels have shifted the argument on online piracy away from themselves toward artists, technicians, and producers who are being hurt by job losses due to online piracy. Like Leman-Langlois, Marshall questions the motivation behind such an approach as well as the term "online piracy" itself.

Leman-Langlois (2004) and Marshall (2002) both state that the threat of copyright infringement is actually much smaller than what the copyright holders claim. Marshall (2006) pushes this point even further by claiming that software producers might actually increase their revenues through the widespread adoption of their pirated software. As the user-base of their program grows, it establishes itself as the standard in an industry, leading to more sales to

clients who need to maintain compatibility with their partners. Marshall cites "several papers [that] outline the possible profitability for software firms in allowing or even promoting piracy […] (Takeyama, 1994; Slive & Bernhardt, 1998; Poddar, 2002)" (Marshall, 2006: p.73). Copyright infringement is also beneficial due to the heightened level of competition it creates. Consumers now have access to a legal and a warez version of products. Since warez is free, copyable and playable on any platform, it is often more appealing than the legal product which is often overpriced and limited through digital rights managements which control how the content can be consumed (Bridy, 2009). This increased competition should in theory stimulate creativity and innovation in the legal market in order to surpass illegal copies of intellectual property.

Not all researchers believe that online piracy has a positive impact on sales. Industry reports by the International Federation of the Phonographic Industry (2011) and the Canadian Intellectual Property Council (2011) are abundantly clear on the negative impact of online piracy. The CIPC report (2011) highlights contradictions in many studies that found that online piracy had no impact on sales. According to it, P2P downloads have reduced revenues and create a strong substitution effect where consumers steal products instead of buying them. Individuals tend to steal products when they can and buy them when they can't steal them. The IFPI (2011) uses Sweden as a case study on how online piracy can be reduced in a country. Through the litigation of a major pirate platform, The Pirate Bay, new legal offerings such as Spotify and strong regulation, the IPRED, Sweden has reduced its online piracy levels and has increased its revenues.

Many academic researchers fall in line with these industry reports. Schultz (2005) reviews some of the past literature and finds that the movie industry lost billions of dollars while a single warez group was responsible for $5 million dollars worth of loss in little more than a year. Schultz (2005) claims that these groups are "so organized and smart that they know every angle of the net […] and are impossible to track" (Schultz, 2005: p.4). Bounie et al. (2006) report important drops in DVD and VHS revenues in France which the industry blames on piracy. Their own study find that piracy has a "strong impact on video rentals and purchases" (Bounie et al, 2006: p.15). According to them, most researchers agree that piracy has negatively affected the revenues of legitimate businesses.

While this may be the case, the debate on the impact of piracy on copyright holders has still not been definitively settled as researchers have yet to build comprehensive models which could factor all the theoretically important variables that affect legitimate sales. Such a research design would require that a representative sample of the population shared with academics their rationale for buying or downloading illegally intellectual property over an extended period of time. It would also need to take into account the characteristics of the industry and of the economy in general such as the number of products released, the marketing budgets, the inflation and the growth of the GDP.

To put an end to these losses, corporations have used a variety of methods. They lobbied governments for new and more aggressive regulations of copyright infringements. They achieved their goal with the adoption of a slew of new laws and treaties including the No Electronic Theft Act, the Digital Millennium Copyright Act, the Family Entertainment And Copyright Act, the WIPO Copyright Treaty and the EU Copyright Directive (Goldman, 2004; Ponte, 2008; Marshall, 2006). Some of these tools appear to be very effective in securing convictions. The NET Act, for example, prohibits copyright infringements for financial gain or the distribution of copyrighted material after a certain threshold (Goldman, 2004). It was responsible for the arrest and conviction of over 80 hackers, including employees of major corporations such as Intel and Microsoft, and members of major hacking groups like PWA and DoD (Goldman, 2004). Each person charged under the NET Act has either been found guilty or has pleaded guilty (Goldman, 2004). Corporations have also relied heavily on digital rights management (DRM) and regional codes to prevent piracy (Ponte, 2008; Bridy, 2009, Marshall, 2006). These tools limit how an individual consumes copyrighted material. They enable copyright holders to control the platforms and timeframe on which content is available. Regulations such as the DMCA have made it illegal to circumvent these DRM and to distribute the tools that would allow an individual to bypass them (Marshall, 2006). However, even with such tight regulations, it is still possible to crack any DRM available (Goode & Cruise, 2006).

Copyright holders have also taken the matter into their own hands by using civil courts to sue copyright infringers (Bridy, 2009). They hired private companies to monitor peer-to-peer (P2P) networks and report the identity of people who have downloaded copyrighted material. They also attacked major P2P network operators such as Napster and Limewire that

provided the means for individuals to exchange copyrighted material (Bridy, 2009). Although the networks themselves were deemed illegal, the technology behind them was not and thus for every network that was shut down, another two have taken its place, each time refining their anti-monitoring skills. Copyright holders have also struck deals with Internet service providers (ISPs) to actively monitor individuals and throttle their internet connection when using P2P protocols, a practice that has since been outlawed by the FCC (Bridy, 2009).

Overall, researchers have come to the conclusion that these strategies have not been very effective and that corporations need to address the underlying causes and processes of piracy (Ponte, 2008; Gopal & Sanders, 2000; Bridy. 2009). Strategies such as attacking warez suppliers, reducing the window between theatre and DVD releases, improving the experience of consumers, and indexing the price of software with the GNP are all alternatives that have been proposed to regulate the warez scene (Ponte, 2008; Bridy, 2009; Gopal & Sanders, 2000).

The demand for warez

The bulk of research on the warez scene focuses on the consumers who download the illegal content provided by hacking groups. Although interesting, there is a great deal of overlap between the different studies. Many of them seek to understand the motivation of consumers through student surveys (Chiang & Assane, 2002; Kini, Ramakrishna & Vijayaraman, 2004; Rahim, Seyal & Rahman, 1999; Sims, Cheng & Teegen, 1996). The results of these studies tend to be specific to their respective samples and cannot be used for general inferences. In some cases, they are also somewhat obvious. For example, it is not surprising to learn that students who have higher technical skills use the Internet heavily or that students with a low standard for ethics are more involved in the illegal downloading of copyrighted products (Hinduja, 2003). It is also not surprising to learn that the speed of the Internet connection and previous involvement in physical piracy[5] have positive associations with levels of online piracy (Hinduja, 2001). Some studies in this area did provide more insightful results. Contrary to popular belief, peer-to-peer networks are not the first choice of

[5] Physical piracy is the act of trading physical media containing warez (ex: an illegal copy of a Windows installation disc).

warez consumers (Schultz, 2005). People are more inclined to download products from chat rooms and news groups which have drawn less attention from law-enforcement agencies and rights holders. The consumers are also not immune to all the regulation efforts described in the previous section. If the perceived risks of pirating content increases, individuals will reduce the frequency of their illegal downloads. There is a sense of guilt associated with the act of pirating, but the easiness of the crime and the benefits outweigh any guilt individuals might feel. Consumers believe that their actions are without consequences are they are defrauding big corporations which are highly profitable. By stealing a movie or a song, they are only marginally affecting the bottom line of these corporations and this alleviates the sense of guilt they might feel. Moreover, consumers enjoy the products they download illegally and therefore concentrate on their pleasure rather than their discomfort at doing that is illegal in most jurisdictions. It is so easy to download intellectual property through P2P systems that consumers do not have time to sit and think about exactly what they are doing. This trivial act is therefore committed almost automatically and integrated into the habits of individuals who become immune to the guilt they may feel. Schultz's (2005) study has one more unique aspect. He compared the time that was needed to download different types of products (movies, games, music, or software) to their price and concluded that people tend to download files with the lowest price-to-time ratio.

The supply of the warez scene

Researchers have focused on two classes of providers of warez: hacking groups and amateurs. Hacking groups are collectives of hackers who dedicate a sizeable portion of their time to the warez scene (Craig, 2005). These are the most prolific pirates and release the quasi-totality of all software and game warez (Goldman, 2004). Amateurs are individuals who randomly upload copyrighted content on peer-to-peer networks (Hinduja, 2007). The difference between the two groups is the level of implication in the warez scene. It is not uncommon for hackers to spend upwards of 40 hours a week working in the warez scene (Craig, 2005; Goode & Cruise, 2006). They usually are more interested by what they can download than what they can offer. They usually upload videos or music files which require little skills to copy and distribute on a peer-to-peer networks. This group, comprised largely of males, does not feel any gilt for their behavior (Hinduja, 2007). Where hackers can be labeled

as professionals, individuals have more moderate computer skills and could easily be defined as hobbyists or enthusiasts (Goldman, 2005).

Hacking groups began with the rise of personal computing and have evolved into huge and international entities. Their members rarely meet in person and use aliases to keep their identities secret (Goode & Cruise, 2006; Craig, 2005). Their main aim is not money, but respect amongst other hackers in the warez scene (Rehn, 2003; Craig, 2005). They compete in a tournament-like setting where the quantity and quality of pirated (or released) products by each group is measured and evaluated. Each time a group releases a new warez, it is considered a challenge to other groups who must either answer back with a release of their own or lose some of their status in the scene (Rehn, 2003). Hackers are motivated by their pride, the thrill of participating in illegality, the belief that data should be free, and their need to belong (Goldman, 2005).

The warez scene is a relatively closed environment with its own rules, customs, and media (Rehn, 2003; Craig, 2005). There is no central place for all the hacking groups to meet. Although the scene consists mainly of hacking groups, some independent individuals are also allowed to participate (Goldman, 2005). These independents may be collectors, downloaders, or enthusiasts who collect abandonware (old software no longer available for sale). There is a strong moral sense in this scene (Craig, 2005; Rehn, 2003; Goldman, 2005). Monetary retribution for the work in the warez scene is frowned upon. Hacking groups often encourage people to buy the products that they initially offered to them through illegal means. In this sense, the warez is considered as a try-before-buying option for consumers. This neutralization process seems to be effective with hackers who show very little or no guilt for their deviance (Goode & Cruise, 2006; Craig, 2005).

Approaching recognition and social organization in the warez scene

Looking back at the literature discussed in the first part of this paper, we realized that the regulation of the warez scene and the consumers of warez have been the main focus of researchers. This is not surprising considering the data that is needed for these two types of research. It is much easier to gather information on new regulations and the behavior of consumers than to find warez hackers willing to share their knowledge. With the recent arrests of major groups such as DoD and PWA (Goldman, 2004), hackers have become even more

secretive. The end result is that researchers have gathered much more knowledge about the context and the setting in which the warez scene evolves than on the hackers responsible for the deviance they should be focusing on.

Researchers who invested the time and energy to befriend warez hackers have been able to harvest individual experiences on how the scene works. This has left us with a collection of stories that have been stitched together by researchers as well as they could. We have discussed previously how important the social factor is for the warez hackers. Their motivation to participate in this tournament-style setting is to get recognized by others for the deeds they accomplish (Rehn, 2003). Given that the social relations are at the root of the scene, a map of the social organization and the distribution of recognition inside the warez scene would greatly improve the understanding of the warez scene and its hackers. Producing such a map will be the main objective of this paper. This Rosetta Stone of social interactions in the warez scene will enable us to understand exactly how recognition and status social is distributed and why some groups manage to survive for years while the vast majority completely disappears after a few weeks. In order to achieve this goal, we draw from two existing frameworks: Sutherland's crime behavior system and Boase and Wellman's work on network individualism.

The Warez Scene as a Crime Behavior System

Past research on specific collective crime settings have traditionally followed what Sutherland referred to as a crime behavior system. Sutherland (1947) dismissed general explanations of crime and emphasized that each crime system must be approached in terms of its uniqueness and specific characteristics. Doing this, he suggested, requires describing three principal features: 1) the integrated unit that represents the "group way of life" between participants; 2) the causal factors and processes that are the source of such common behavior; and 3) the content of the setting that defines a common identity amongst participants. "Ultimately," Sutherland argued, "a behavior system should be defined as a way of life which grows out of a unified causal process" (Sutherland, 1947: 219).

While the crime behavior system does apply to the warez scene, the virtual setting in which this community thrives calls for important nuances to be made when assessing interactions between participants. As with crime behavior systems that emerge from market

settings, interactions between demand and supply in the warez scene are collective, ongoing, and consensual. However, more than ever, the internet offers a largely unregulated environment in which illicit transactions can take place and evolve to reach a large number of people. Another important distinction is that the primary motivation for warez hackers is recognition, and not financial gain. Yet, as with most crime behavior systems, this search for recognition creates a competitive setting in which warez hackers are constantly developing new skills and methods to supply challenging new products to consumers. This results in intensive interaction, which, in turn, serves to ensure that the norms and values of the community are respected. For example, hackers who seek financial benefits are quickly identified and expelled from the community. That such competition and internal checks occur within the Internet environment suggests that warez hackers have to be able to adjust to interactions in a highly decentralized and self-organizing setting (Pastor-Satorras and Vespignani, 2004).

This unregulated and ambitious chase for recognition and the need to constantly cultivate the necessary acumen to survive in the milieu requires that warez hackers remain in (virtual) close contact through a high traffic communication network. But this communication network is radically different than other deviant or criminal networks that embedded participants who were in physical interaction with each other. The Internet distinction is best captured by Boase and Wellman's idea of networked individualism. Boase and Wellman (2006) recognize the community feature of Internet interactions, but stressed that this new communal frontier is largely governed by networked individualism. What Boase and Wellman are referring to is that while individuals are increasingly coming together in Internet communities, the speed, ease, and relational transiency with which this is possible makes this an individualized phenomenon, one in which the individual (and not the group or network) is at the center of his own world.

In order to recreate the map of the social interactions in the warez scene, we will focus on three specific questions. Following Sutherland's (1947) theory, we will first present the general characteristics of the hacker groups. The competitive, decentralized and unregulated features of the scene would suggest that the hacker groups could be compared to the early actors that emerged in illegal drug markets: a fair number of small, agile and transitory groups that have a very limited impact on the market.

Following Boase & Wellman's (2006) theory, we will then present the social organization of the warez scene. Networked individualism defines the new characteristics of personal relationships. Based on these attributes, we thus hypothesize that: 1) hacker groups are involved in many networks that are segmented into clusters or cells, making the collective structure dense (within clusters) but minimally connected to each other (between clusters); 2) relations between the groups are ephemeral; 3) hacker groups tend to connect with other groups that have different profiles than theirs; and 4) most relations between hacker groups are weak.

We then merge these first two sets of analysis to understand how recognition—the driving force of the warez scene—is distributed amongst hacker groups. Past research (Craig, 2005; Rehn, 2003) has led us to surmise that those groups that produce quality warez over extended periods of time should receive the most recognition from others. Our final analyses address such achievement through a systematic investigation of networking and production features of the community at hand.

Data and Methodology

The fact that hacking activities are conducted on the Internet offers both challenges and opportunities for empirical research. On one hand, the Internet provides a shield of anonymity, making it difficult to identify an individual. On the other hand, the convergence of activities on the Internet helps us understand the collective scene. The advent of modern search (or index) engines has facilitated the data gathering process. While mainstream engines such as Google or Yahoo are known to millions of people, underground specialized indices are often more useful for researching Internet-mediated social networks. We discovered that warez hackers had created unique search engines that stored an abundance of information on the copyrighted material they cracked. While it may seem strange that hackers would build such an incriminating directory, the rationale behind it is quite straightforward. Participants in the warez scene live by their own rules. One of these rules stipulates that no one is allowed to distribute a file that has already been hacked by someone else (a "hacker copyright" of sorts; see Craig, 2005). For example, if Group A cracked and distributed Windows XP, no one else would be permitted to distribute this software or create a second version of the crack. Group A will therefore be recognized as the first who cracked and distributed the software. Because of

the importance placed on such recognition, hackers need a way to establish whether a product they intend to crack is already being distributed by another group. The indices we came across during our search for a data gathering technique do just that—they credit a copyright break to the proper hacker group and, with such information available to all online, hackers can no longer mistakenly release a duplicate product.

With no central convergence setting in place, the social organization of the warez scene cannot be studied to a full extent through the use of interviews or observations that gather information on a small set of hackers. It was necessary for us to adopt an approach that integrated new data gathering techniques that optimize the navigation of these Internet interactions across a wide international geographical and virtual scope.

Hacking the hackers

We started the data gathering segment of this research by gaining access to these indices. For each cracked file, we were able to obtain its release date, the name of the hacker group responsible for releasing the file, the type of file (e.g., television shows and movies, "XXX" video, software package, or computer games), the size of the file, and the number of times it had been downloaded. The information also included a direct download link to the "NFO" file associated with the release. NFO files are text files that carry an .nfo extension (hence the name) and are attached to every type of cracked material distributed online by warez hackers. The text on NFO files is usually divided into four sections: 1) nominal information on the copyrighted material (i.e., release date, type of movie/game/software, release type, and platform), 2) a detailed description of the product (e.g., the storyline of a movie, a review of a game), 3) information about the hacker group (the group's name, announcements, and disclaimers), and 4) the salutations or "greetz" made by the hacker group to other groups. Distributing warez software is illegal in many jurisdictions[6] and such open greeting between co-participants is one of the main features distinguishing hackers from other offenders, who are more likely to avoid advertising their criminal activities.

Once we determined what information was available and where it could be accessed, retrieval was simple. While there are many competing indexes on the web, we chose

[6] While the legislation regarding the trading of copyrighted material varies across countries, it is safe to say that in most countries today, there are laws that address hacker actions (see Sterling, 2008).

http://www.nfohump.com as our source for four reasons. First, it offered a direct link for downloading NFO files, a feature offered by few others. Second, each product had its own web page with all the details listed and organized in a way that simplified the process of harvesting the data. Third, the reputation of its nfohump index is well established (TopSite, 2010). Finally, it is also one of the most complete in terms of information access.[7]

In order to extract the data from the index, we used a specialized software package called Web Scraper Plus, which downloads web pages and then stores the pertinent information in a spreadsheet. We obtained details on 100,000 different products which were released between 2003 and 2009. The NFO files associated with these pirated products were downloaded using our own custom program.

At that point we had a very rich spreadsheet which we used to build a database that recorded the activities of each hacker group. This new database had information on 3,164 hacker groups active between 2003 and 2009[8]. It contained the name of the group, the date of its first and last hack (which we took as the group's "life span"[9]), the number of files it distributed, the total size of the files,[10] and the total download count for all files.[11] We calculated the average file size and download count for each release[12] and for each group. We then inferred the "productivity" of the group by dividing the number of days the group was active by the number of releases.

Our database included twenty-two different types of files which, in order to simplify analyses, we categorized into five product groups: computer (PC) games, console games, software, videos, and XXX videos. This allowed us to assess the level of specialization for each hacker group by examining the number of categories in which it was active.

---

[7] Another index, http://www.blueforge.net only offered 60% of the pirated material we could access on http://www.nfohump.com.

[8] The present study is only representative of the warez scene for the years going from 2003 to 2009. The size, density and interactions between its members may have changed since.

[9] The life span was obtained by counting the number of days between the first and last release. This measure is only an estimate since the group could very well have been active before or after those dates.

[10] We were not able to gather information on the total size of files for seven hacker groups.

[11] The index provided a column titled *hits* which indicated the number of times the file was downloaded. However after July 2007 all the NFO files had a hits count of 0. (We were unable to get an explanation of this from the people in charge of the index.) This reduced the number of hacker groups examined for this variable to 2,645.

[12] "Release" is the term used by hackers to refer to a released product

In order to keep track of the value of each product, we used our own custom program that queried an online merchant website (Amazon.com) and obtained the price for each item. The success rate of this operation was around 80%.[13] This gave us the total value of the copyrighted material distributed by each group, as well as the most and least expensive product they distributed.[14] We also calculated the average price of the copyrighted material distributed for each group which, when multiplied by the number of downloads, offers a general indication of the overall impact each group had on the software industry.

To understand the networks behind the production of this material, we then looked at the content of the NFO files we had downloaded[15]. As mentioned earlier, the NFO files also contain greetings or "greetz." These consist of a list of group names, usually located at the bottom of the NFO file. We used these greetings as a proxy for measuring the level of reputation surrounding groups within the warez scene. The more greetz received, the higher a hacker group's reputation. These greetz were interpreted as a straightforward indicator of indegree centrality, a social network measure that accounts for the number of contacts directed toward a node in a given network. However, there are caveats about using this kind of variable as a proxy for influence within the network. An important limitation is that we do not know whether we are measuring *all* the influence that a group is exerting. Our decision to use these greetz as the basis for this study's main variable is justified by the observation that, although groups can greet anyone they wish, they are selective in that they do not greet everyone. NFO files are truly works of art: bound by the file format's limited set of usable characters, their authors still manage to create impressive images. Crafting an NFO file is a painstakingly long and complex task and if greetings are inserted, it is likely for important reasons because each character counts—literally—when it comes to NFOs. Somewhere in the process of making the NFO file, a decision is made to greet some particular groups for personal and professional reasons, and particularly for increasing one's own exposure.

[13] This reduced the number of hackers groups examined for this variable to 2783.
[14] The price measured here reflects the value of the product at the time of the study. The value of older products will be lower today because of the time that has elapsed between their release and the time of the study.
[15] We managed to recover over 700 email addresses of hacker groups in the NFO files which will be used in future studies. Supplying a public email address increases the risks of being discovered, but is also a quick and easy way to recruit new members and network with other groups.

The social network analysis framework

In more traditional research on criminal behavior systems, researchers would interview key participants in these systems or examine crime data to get a basic understanding of the underlying structure of the criminal system in place (Sutherland, 1947). Using our data gathering methodology, we were able to assemble a comprehensive dataset on the warez scene. To make sense of this data, we used social network analysis to study the positioning and influence of different participants. The underlying principle of SNA is to derive the structure of a network as well as the position of each of its participants from their relational ties (Wasserman & Galaskiewicz, 1994: 4). This is precisely the type of questions that our hypotheses address.

For the present study, we accounted only for the presence or absence of a link between hacker groups (a directed binary matrix in social network terms). Each hacker group is a node and each greeting in an NFO file is a vector between two nodes (or actors). We created a network matrix of who greeted who – a square matrix that indicates a link with a *1* and the absence of a link with a *0*. We then used Ucinet 6 (Borgatti, Everett and Freeman 2002) to derive network variables for each group and for the network as a whole. Network variables included basic density and centrality measures (indegree, outdegree, and betweenness centrality). These are the measures most commonly found in SNA research. Density is defined as the level of cohesion within a social network and is measured by dividing the number of direct ties (or dyads) observed over the maximum number of direct ties that are possible in the network. It is thus a measure of the connectedness of actors on a network level. We also examined density at a local level with the clustering coefficient, which measures the number of direct ties between a single node's direct contacts—the clustering coefficient is essentially a measure of personal network density within a network (Watts, 1999). It is a good indicator of the presence of sub-groups or cliques in a network. Indegree and outdegree centrality measures account for the direction of direct ties around each node and indicate, respectively, the number of incoming and outgoing contacts (Freeman, 1979). Betweenness centrality measures the extent to which a node mediates between other nodes by its position along the geodesics (shortest paths between two nodes) within the network. The more often a node is located along geodesics, the higher its betweenness centrality, making the node a broker within the network

(Freeman, 1979). Brokers play a very important role in networks because they control the flow of information. They decide which information they release and which information they retain.

Characteristics of the Warez Scene Social Network

Table 1 provides the descriptive statistics for the hacker group characteristics. Hacker groups that are part of the warez scene are generally ephemeral: half do not survive beyond two months (median = 55 days). Some, however, are able to survive for years, and as we will show, survival is related to greater recognition.

Table 1: Characteristics of the warez scene

	N	Min	Max	Mean	Median	St. Dev.
Life span (days)	3164	1.00	2,051	329.1	55.0	510.50
Nb of releases	3164	1.00	4,948	31.6	3.0	140.90
Productivity	3164	0.08	796	27.1	5.5	64.10
Size of all releases (in GB)	3157	1.00	2,887	34.0	3.9	129.80
Average size of releases (in MB)	3157	1.00	23,500	1,495.4	862.5	1,619.10
Total nb of downloads (in millions)	2645	3.00	16,101	105.4	2.1	0.66
Avg nb of downloads per release (in millions)	2645	1.00	100	4.9	0.4	15.00
Total price of releases (per group)	2783	1.00	28,097	376.5	44.0	1,351.20
Highest price of release	2783	1.00	1,240	51.2	20.0	114.40
Average price of release	2783	1.00	799	22.1	11.0	49.90
Degree of specialisation	3164	1 = 92.5%	2 = 6.6%	3 = 0.7%	4 = 0.2%	5 = 0.0%

The number of group releases is low (median=3 releases). At first glance, this confirms that a large portion of groups are short lived. However, many groups produce little over a long period of time, largely because of the level of difficulty associated with producing a release. As Craig (2005) described, releasing and distributing a product in the warez scene requires the coordinated work of many people. The productivity variable (the number of days a group was active divided by the number of releases) might be distorted by the high number of groups that survive for only one day and consequently have a productivity of only one item. Nonetheless, the minimum (0.08, days by releases) and maximum (796, days by releases) lifespans indicate that although some groups manage to produce more than one release per day, others manage to survive for more than two years without a single release. This demonstrates that a hacker group does not need to produce at a high rate to survive in this scene. One explanation might

be that if a group releases a very popular or hard-to-crack file, their recognition for that feat alone ensures their survival for many months to follow.

When examining what hackers offer for downloading, it is clear that most files have a low monetary value (median = $11). Even when we combine all the releases of a group, the median is less than $50. This suggests that the warez scene is primarily used to distribute low cost products, though one can also find expensive commercial software (maximum price of release = $1,240).

Groups tend to specialize as a majority of groups only release one type of warez. A few have branched out in multiple categories, but data suggest that groups prefer to spawn a new specialized subgroup rather than compete on many fronts. This is another demonstration of the intense competition at the core of the warez scene.

The Social Organization of the Warez Scene

Table 2 provides the descriptive statistics for the network variables constructed to determine recognition among groups. Indegree and outdegree centralization for the overall network is low (both 6%), indicating that no actor or actors significantly dominate the network. This finding is consistent with the democratic or decentralized structure of the Internet. Greetz appear to be quite balanced—each group has, on average, six groups with which they make contact and six groups that contact them. However, the maximum values for these indegree and outdegree centrality measures are telling in that some groups greet (or are greeted by) up to 150 other groups.

Table 2: Network features of the warez scene

	Minimum	Maximum	Mean	St. Dev.
Betweenness (normalized)	0.000	3.763	0.067	0.212
OutDegree	0.000	150.000	6.210	11.162
OutDegree (normalized)	0.000	6.628	0.274	0.493
InDegree	0.000	155.000	6.210	9.957
InDegree (normalized)	0.000	6.849	0.274	0.440
Betweenness centralization index				3.70%
Outdegree centralization				6.36%
Indegree centralization				6.58%
Density				0.0027
Clustering coefficient				0.0920

The density of the network is also low (0.3%). However, the clustering coefficient is thirty-four times higher (9%) than the density of the overall network, suggesting that although the network is dispersed, there is a tendency toward localized group or clique formation. These local cliques are relatively small when compared with the stock count of the overall sample (n = 3,164 groups) and the flow count of this sample (400 to 600 groups active per day). Thus, groups have a social network of friends or business associates, but that circle is fairly limited.

In many social networks, brokers play a central role (Burt 1992, 2005; Morselli 2009). In the warez scene, this is not the case. Betweenness centralization is low (3.70%), especially when compared with degree centralization. It can thus be assumed that, at least when it comes to greetz, groups tend to contact people directly rather than indirectly, so intermediaries within this setting lose their strategic relevance. There is, however, a considerable range between the minimum and maximum scores for betweenness centrality at the actor level, suggesting that some groups are more prominent brokers—and, of course, their presence may be obfuscated by the mass number of short-term groups.

Recognition and Survival in the Warez Scene

Table 3 provides the correlation matrix between the descriptive features of hacker groups and the recognition indicator (indegree centrality). Although there is considerable diversity, almost all variables are correlated with this measure. The lifespan of the group has the strongest relationship with indegree centrality. Consequently, the longer a group survives, the more likely it is that it will be recognized by other groups (and vice-versa). The number of files a group releases is also correlated with indegree centrality, making higher output a key correlate of a group's reputation.

Table 3: Pearson correlation matrix of warez scene variables.

	1	2	3	4	5	6	7	8	9	10	11	12	13
InDegree (1)	1.000												
Life span (2)	**0.428	1.000											
Nb of rips (3)	**0.377	**0.392	1.000										
Average size of rips (4)	**0.065	**0.075	0.002	1.000									
Average nb of downloads per rips (5)	**0.056	**0.202	0.031	-0.023	1.000								
Highest price of rips (6)	**0.100	**0.301	**0.108	-0.005	**0.092	1.000							
Known public email (7)	**0.216	**0.291	**0.198	0.032	-0.031	**0.112	1.000						
Diversification (8)	**0.127	**0.287	**0.152	**0.060	**0.058	**0.171	**0.110	1.000					
Specialty: Videos (9)	-0.030	-0.023	0.021	**0.431	**-0.115	**-0.267	0.022	**-0.063	1.000				
Speciality: PC Games (10)	0.005	0.021	-0.024	**-0.578	**0.180	0.006	-0.016	*0.043	**-0.499	1.000			
Speciality: Console games (11)	*0.038	-0.031	**-0.052	**-0.050	**0.116	-0.020	-0.029	-0.001	**-0.460	**-0.187	1.000		
Speciality: Software (12)	**-0.052	0.032	-0.025	-0.015	0.022	**0.544	-0.020	*0.038	**-0.314	**-0.128	**-0.118	1.000	
Speciality: XXX videos (13)	**0.056	0.027	**0.101	**0.100	**-0.238	-0.006	**0.047	0.024	**-0.276	**-0.112	**-0.104	**-0.071	1.000

** $p < 0.01$

* $p < 0.05$

Efforts to improve networking are also linked to a group's recognition—indegree centrality is correlated with a group's public email address, which allows these groups to receive feedback, recruit new members, and publicize the fact that they are not afraid of being targeted or arrested. Such openness is viewed positively within the warez scene and hacker groups who network this way tend to greet each other more often.

Although specialization is the norm with regard to the products offered for downloading, the few groups that do diversify across multiple fronts are also more likely to be greeted. Their diversification may attract the attention of other hacker groups, which leads to greater recognition. The type of files distributed does not affect a group's recognition. This is somewhat surprising in light of the fact that much less expertise is needed to crack videos than software. We would have expected that those groups that succeed in cracking more difficult products would be recognized accordingly.

Discussion

Our results demonstrate that: 1) hacker groups do not have an extended lifespan; 2) the number of releases they produce is not very large; 3) the products they offer are of low value; and 4) groups tend to specialize in one particular commodity. These findings confirm our initial hypotheses that hacker groups would be numerous, agile, transitory and have a limited footprint on the market. A typical group usually releases a few warez in a limited timeframe before vanishing. This makes for a very dynamic market where alliances shift constantly and where hackers have to find new partners regularly. This ensures the dissipation of the warez culture and the most up-to-date technique amongst all its members. This in turn reinforces the group way of life as described by Sutherland (1947). The strong group way of life might also explain the limited success in regulating the warez scene. Hackers form a cohesive front that is hard to penetrate. Moreover, since the scene is not depending on a single group for most of its releases, it becomes very hard for law-enforcement agencies and right-holders to control the supply of the warez.

Regarding the structure of the scene itself, our results show that the structure of the warez scene is consistent with the context in which it has developed—the Internet: 1) hacker groups are dispersed all over the web and the world; 2) none is at the core of the network and removing any (or even a good number of) hacker groups from this scene would not affect the

overall structure; and 3) the scene is as resilient and redundant as the Internet itself and hacker groups are considerably dispersed, with some level of local clustering. We were thus able to confirm three of our initial hypotheses regarding the social organization of the warez scene. With a clustering level much higher than the overall density of the network, we have confirmed that hackers do aggregate in smaller groups that are not well connected with each other. We have also shown that relations between the groups are ephemeral. With such a low average life span, groups see their links with others disappear as rapidly as they are created. In a tournament-style setting, the demise of a group has a negative impact on the reputation of its members and such hackers often have to change their nickname in order to start fresh and disassociate themselves to their past failures. This means that hackers cannot count on their old relations when building a new group. We believe that this ongoing cycle has a weakening effect on the quality of relations between the hackers. Why would they invest their time and energy in a relation that is bound to disappear in a time span that could be less than a few weeks? We were unable to confirm or deny our third hypothesis regarding the homophily of the network. Further research will be needed to determine if groups greet those that distribute the same type of product more than those that do not.

Regarding the correlation between the group way of life and the level of recognition received (indegree), our results show that there is an important level of stratification that separates successful from unsuccessful hacker groups. The key variable is group lifespan, and the selection effect within the scene seems merciless with a virtual world Matthew Effect (Merton 1968) firmly in place. Indeed, success begets success. The more a group produces, the more that group prospers. This evolution increases their ability to test themselves on new and more challenging material. Groups who fail to obtain a significant level of recognition fade away relatively quickly—this is the fate of most groups. Thus, whereas no central actor may be identified, there are a few clear survivors in this decentralized setting. However, there is still some hope for short-lived groups, insofar as members often move on and become members of those exceptional groups who prosper. This confirms past research findings that suggested that recognition was offered to those that could release quality warez over extended periods of time. Our study extends these factors to include the networking of groups (outdegree and presence of a public email address) as well as the diversification degree. Recognition is thus not distributed randomly within this community. It is rather earned by its

most capable members. This is a powerful motivation for smaller and younger groups; it is only be persevering that they will achieve a higher social status in the scene.

The warez scene is a community that is still very much in its early stage as a crime behaviour system. The limited life span of hacker groups is a good indication of the competitiveness of the scene as well as the lack of experience of most of its participants. Such groups have yet to internalize the steps needed to produce warez on a regular basis. The low number of releases distributed by each group is another example of the inexperience of warez hackers. The fact that new groups emerge on a monthly basis (and replace those that have disappeared) is a sign of a thriving pool of available participants who are able to enter the warez scene. Participants in the scene are thus eager to learn and are not afraid of starting over with new team members and former competitors.

The vast majority of warez groups are only releasing one type of product which can be interpreted as either an indication of the competitiveness of the scene as specialization in a single medium allows for maximum efficiency and a more optimal performance or as a personal preference for a particular type of medium.

As competitive as the warez scene may be, its participants still need to interact with each other. The dispersed and decentralized features of this scene are consistent with its inherent competitiveness. No actor is able to harness the network from a central position. The hackers' characteristics and the network features show however that some hacker groups have distinctively higher scores than others. These are the groups that could be labelled role models in this particular crime behaviour system.

The last analytical section shed some light on the factors that may distinguish a group's role model status. A combination of factors distinguishes role model groups from others. The mixture of performance and audacity is the principal force underlying the success of a group in the warez scene. For those who succeed, it is a matter of great pride; for those who do not, it is this ultimate goal that keeps them in active in the warez scene and motivated to start new groups and continuously learn to crack and distribute more warez content.

Conclusion

Inhabited by hacker groups who spend countless hours in front of their computers each day, the warez scene brings together every piece of copyrighted material that has been cracked

and distributed online. We described the group way of life of these hackers and the emergence of a contemporary crime behavior system in the Internet world. While we analyzed a comprehensive set of data on this system, there are some important limits that must be considered.

First, websites created by and for hackers rarely detail their sources of information or indicate how they gather their data. This could lead to poorly sourced data or false information. We limited this problem by investigating NFO Hump, the index that hosts information on warez hackers. We made sure that it was a trusted source for the warez scene and had been around for several years. It was thus as reliable a source as possible.

Second, we did not gather information on communications between hacker groups per se. It would have been theoretically possible to survey the hacker groups to gather information on such relationships, but such a task would have been daunting. We addressed this problem by using the greetings found in the NFO files as indicators for such interactions.

Third, this study did not take into account the personal relationships of hackers due to a lack of data. This missing variable would be very valuable to researchers since past professional relations surely impact on the target of greetz. This should be the focus of future research.

Finally, the results are based on a network matrix that contains all the greetings for a six year period. Collapsing this data in a single matrix affects the findings in that the links are diluted in a bigger pool (or network). Further research will present the same data on a month-to-month basis in order to refine this study's analysis.

This first study of the warez scene also offers some ideas on how to control suppliers in this area. By targeting the role models in the scene, as indicated by a group's performance level, law-enforcement officials could effectively disrupt the dynamics of the warez scene and weaken the reinforcement of criminal behavior hackers currently provide each other. As most experiences in addressing impunity in a criminal market illustrate, the recognition that is so eagerly sought after by suppliers loses its appeal once exposure becomes a problem.

This study provides a framework for empirical research on hackers and their world. Although knowledge of this phenomenon is increasing, systematic data on the warez and other hacker scenes remains sparse. Past research has relied disproportionally on studies based on college students and their experiences, basic typologies, and website traffic analysis. The

strengths of the present framework are threefold and provide useful guidelines for those who plan to study hackers. First, the Internet is the largest source of data any researcher could hope for. Its open and decentralized structure offers open access to countless forms of information and it is time that criminologists begin to explore the many channels available in this new world. Second, researchers must not hesitate to adopt hackers' tools and mindset. All the data used in this research was gathered and analyzed using publicly available software, but custom programs were also created. These programs were based on techniques adopted by hackers in order to access data that would otherwise be extremely tedious to gather. Finally, the social features of hacking remain centrally important. Although hackers are often alone with their computers, they nevertheless belong to a larger community. The high volume of people involved in such activities and the need for participants to stay up-to-date with the latest tricks and releases make the warez scene an interactive setting that extends far beyond the mere supplier-consumer relationship.

The hacker community within the warez scene reflects both old and new concerns for criminology. While the scene is conducive to analysis using Sutherland's framework and may thus be compared to crime behavior systems both past and present, its scope, context, structure, and mass appeal make it a new and thriving phenomenon that has attracted the attention of a growing mass of consumers.

CHAPITRE 6 – REPUTATION IN A DARK NETWORK OF ONLINE CRIMINALS

Auteurs:
David Décary-Hétu
Benoit Dupont

Publication :
Décary-Hétu, D. & B. Dupont. (2013). "Reputation In A Dark Network Of Online Criminals." *Global Crime*. 14(2-3): 175-196.

Abstract

This paper focuses on criminals who could easily be labelled as entrepreneurs and who deal in compromised computer systems. Known as botmasters, these individuals use their technical skills to take over and control personal, business and governmental computers. These networks of hijacked computers are known in the security industry as botnets. With this massive computing power, these criminals can send large amounts of spam, attack web servers or steal financial data – all for a fee. As entrepreneurs, the botmasters' main goal is to achieve the highest level of success possible. In their case, this achievement can be measured in the illegitimate revenues their earn from the leasing of their botnet. Based on evidence gathered in literature on legitimate and illegitimate markets, this paper sets to understand how reputation could relate to criminal achievement as well as what factors impact a heightened level of reputation in a criminal market.

Keywords

Reputation; Criminal achievement; Online criminal markets; Social Networks

Introduction

Recent research has highlighted the level of organization of today's cybercriminals (Holt, 2012). These online crime market participants have created web platforms where they can virtually meet, discuss, exchange and buy and sell illicit goods and services. These online illicit markets are very popular (over 20,000 profiles in our case study) and provide an easy way to find co-offenders or to get up-to-date best practices regarding criminal activities.

This paper will focus on a single online web forum where participants discussed and bought and sold illicit goods and services related to botnets. Botnets are networks of infected computers which can be used to launch denial of service attacks, steal personal information or send spam (Rajab et al., 2006). As with any criminal setting (Reuter, 1983), there is a high level of competition on these forums and participants are often victimized by their peers (Franklin et al., 2007). In order to increase the market's fluidity and efficiency, many forums have adopted recognition scales which enable participants to rate each other's reliability publicly. This encourages good behavior and reduces the risks associated with business transactions in these environments. This paper will examine exactly how recognition is distributed in a single online criminal market and whether certain pattern emerges regarding the accumulation of reputation. A discussion will follow regarding the possible tactics that law-enforcement agencies could use to disrupt such markets.

The first section of this paper reviews the rise and need for online criminal markets. The second section presents the general phenomenon which we will be focusing on, the botnets. We will highlight their role as crime facilitators in the new online crime setting. The third section will detail the inherent risks associated with the participation in online illicit forums and how reputation can be used to reduced friction and conflicts. We will then build a framework that will explain the role of reputation using three components: personal characteristics, behavior and social networking. Our results prove that recognition is not distributed randomly among participants in an online criminal market. Many of the proposed tactics to disrupt such markets would be difficult to implement, with the exception of the slander attack (Franklin et al., 2007) which would stand the best chance to effectively limit the fluidity of markets.

From online crime to online criminal markets

Older generations of cybercriminals, known as hackers, were mostly motivated by fame, peer recognition and a desire to learn more and test the limits (Taylor, 2000). To this end, they tended to attack highly visible targets which would attract the most media attention. This trend was personified by Mafiaboy who took down news websites and online merchants such as Yahoo!, Amazon and Dell (Calce & Silverman, 2008). These kinds of attacks were easy to carry out as the victims and guardians did not have a good understanding of the threats they were facing as well as the methods to protect their systems against them.

More recently, hackers have come to realize the extent of their power and rather than show off to their peers, they have been more and more taking advantage of the criminal opportunities that the Internet provides. This is reflected in a recent research which shows that criminals now use the cyberspace to commit banking fraud, extortion through denial of service attacks, intellectual property fraud as well as identity fraud (Wall, 2007). This transition has been facilitated by the diffusion of technical knowledge and tools that are required to commit these types of crimes (Gold, 2011). The Internet has always been celebrated for its ability to foster discussions and exchanges (Hansen, 2008); it is therefore not surprising to see that criminals are also taking advantage of these features to maximize their criminal opportunities.

To do so, criminals have moved to online platforms such as online discussion forums and the Internet Relay Chat (IRC), an online synchronous instant messaging system. There, newcomers (known as *n00bs*) are able to ask technical questions to more experienced criminals who may help them or mock them for their lack of skills (Nycyk, 2010). Given the relative anonymity of these settings, this securely enhances the level of cooperation and efficiency in the criminal underworld as best practices rapidly spread among a large population (Wang et al., 2012). While important, the diffusion of information is not the only role that online platforms fill; over time, they have also been used to host criminal markets where illicit goods and services can be bought and sold.

Holt & Lampke (2010) provide a detailed analysis of the inner working of such markets. Participants first register for an account and then create a new discussion thread where they state what they are looking to buy or sale. They also usually include detailed

information on how they wish to be contacted and how the payments should be made. In Holt & Lampke's (2010) study, criminals offered to sell both tangible and intangible assets such as credit and banking card information, malware and fake credit cards. The banking information sold sometimes includes all of the account holder information (name, address, zip code, social security numbers, mother maiden name, etc.), allowing the purchaser to commit banking fraud and identity theft. Participants also offer services to their fellow criminals (Olimann, 2008). These services include cashiers services to empty bank accounts, drops to receive packages paid with stolen credit cards, spamming services and denial of service capabilities (Choo, 2007). These business-to-business services allow unskilled criminals to extend the scope of their reach through specialized services. A criminal may therefore threaten to take down an online gambling website unless he is paid a certain amount of money. If his demands are not met, he can use his access to online illicit markets to hire the necessary help and put his threat into execution. At no time does he need to have the technical skills associated with a denial of service attack as the online criminal ecosystem is there to give him all the services he needs.

This type of online illicit market was foreseen by Mann & Sutton (1998) and has also been the focus of other researchers such as Thomas & Martin (2006). They focus on IRC chat rooms where participants also buy and sell credit and banking information as well as hardware. Thomas & Martin (2006) highlight the complete disregard for secrecy on these platforms and the relative impunity into which criminal behavior occurs. The channels where advertisements of criminals goods and services are posted can be found using simple keywords in any given search engine. Transactions, however, often occur in private messages or through encrypted instant messaging.

Online illicit markets are very active. In a single case study, Franklin et al. (2007) find that hundreds of new credit card information on average are made available every day. The same can be said of online bank account logins and social security numbers as fresh information is always available for sale. The authors evaluate that a single channel was responsible for the theft of over 37M$ (2007). Hundreds of new accounts are created every day but the churn rate is especially high as the majority of participants stay active for less than 40 minutes. These participants do communicate regularly with each other (Motoyama et al., 2011) and tend to register accounts in more than one market.

Botnets as crime facilitators

As we mentioned in the previous section, many business-to-business services are available in online illicit markets. The criminals that offer these services rely on the botnets they control to meet the needs of their customers. Botnets are "networks of infected end-hosts, called bots, that are under the control of a human operator, commonly known as a botmaster" (Rajab et al., 2006). Botnets can be built from scratch by hackers who use computer worms, software vulnerabilities and/or social engineering to trick their victim into installing a software that will allow them to remotely control a computer (Ianelli, 2005). Already infected computers can also be bought in illicit markets for under $0.10 per computer. To control their botnets, botmasters use command and control (C&C) centers which can either be hosted in IRC chat rooms or in web servers. Infected computers periodically connect to these C&C to receive their orders. Although it would be possible for a single person to create his own botnet control program, it is far easier to download or purchase one online. These software suites allow almost anyone, even unskilled computer users, to operate a botnet through a graphical interface that monitors the growth of the network and sends out orders (Cooke et al., 2005).

Botnet are especially valuable to online criminals because of their versatility and efficiency. Large botnets, with thousands or tens of thousands of computers, can easily saturate the Internet connection of a website, blocking legitimate users from accessing it - a distributed denial of service attack (Ianelli, 2005). They can also be used to monitor the legitimate users of zombie computers and steal any personal or financial information through a key logger. Bächer et al. (2005) also highlight many other uses such as sending spam. Each infected machine can be used to send thousands if not more emails and to gather new email addresses that can be targeted by hackers. Online polls and games can also be manipulated as they usually only check that each IP address has voted once. Finally, botnets can be used to artificially increase the traffic of certain websites which contain ads. The ad companies pay the owner of these websites proportionally to the number of views and the number of clicks each ad receives. Using botnets, it is possible to make it look as if thousands of individuals had visited a page and clicked on the ad. This creates a very interesting stream of revenue for hackers and/or the people hiring them.

To fight and prevent botnets and illicit online markets, Holt & Lampke (2010) and Chu et al. (2010) propose that law enforcement agencies infiltrate web forums and chat rooms to identify the key players and build up cases against them. Sting operations could be launched against specific individuals to disrupt the most successful criminal enterprises (Chu et al., 2010). Reverse sting operations where fake financial information is released or where fake servers are the targets of distributed denial of service attacks (DDOS) could be used to further identify key players. To disrupt the markets, market reduction approaches such as those suggested by Sutton (1998), slander attacks and Sybil attacks (Chu et al., 2010) could be implemented. In these types of operations, law enforcement create fake profiles with high reputation which later default on their obligations. Alternatively, fake profiles can also be used to tarnish the reputation of the most honest and successful market participants. This increases friction and reduces the necessary trust for these platforms to operate.

If online criminal markets have fostered as they have over the past few years, it is in great part due to the rise of botnets and the fact that botnets have facilitated crimes. Botnets offer a steady supply of services that others can rent as they wish. They are also an important source of stolen personal and financial information that can be bought in online criminal forums (Bächer et al., 2005). Without botnets, the efficiency of this underground economy would be much lower. Moreover, botnets have also vastly reduced the technical skills needed to become a hacker (Chu et al., 2010). Botnet software can be downloaded online and provides individuals with a graphic user interface that enables almost anyone to launch, spread and control a botnet. Participants unwilling to spend the time and energy to develop their own botnet may also simply rent botnets and ask their owners to manage the different tasks they need to perform (ddos attacks, information theft, ad fraud; see Ollmann, 2008).

The risks and mitigation of risks in online criminal markets

Although online criminal markets facilitate transactions between criminals, they are still affected by many of the same flaws that limit the fluidity and efficiency of traditional criminal communities. Market participants are seen by their peers as easy targets for many reasons (Holt & Lampke, 2010). First, they have money or valuable data that can be stolen. Second, given the relative anonymity of online markets, it is very easy for participants to hide their true identity and to create new profiles once they have committed a scam on one of their

peers. This in effect eliminates any potential negative consequence that would result from a theft. Third, participants are unable to contact law enforcement agencies or guardians that could help them to identify the author of the theft or the scam and to obtain some sort of reparation. Some markets are run by administrators who are in charge of monitoring the users' activity and to take action against scammers and rippers. Unfortunately, these administrators can also be the source of victimization as described by Franklin et al. (2007) who demonstrated that the credit card number validation services that administrators offered was actually a computer program that stole the credit card data and returned a pre-determined message to the user.

For all of these reasons, online criminal markets tend to function like lemon markets where it is impossible to identify reliable business partners and good products before making a transaction (Akerlof, 1970). This pushes the good participants out of the markets and lowers the price of the goods for sale. This is reflected in the price of the stolen financial information which is sold at a steep discount considering the amount of available credit on each credit card that is sold (Holt, 2012).

To enhance the security of the markets, some administrators have decided to award official positions to some of the participants. The profiles of these individual then includes their official title such as *verified vendor* or *verified seller* and indicates that some level of vetting was done on that particular participant (Holt, 2012). The fact that these positions are for sale however tend to limit the trust that is and should be put into these titles. Rather than rely on the market administrators, some platforms have adopted recognition scales similar to those found on popular websites like Yahoo! and Amazon (Motoyama et al., 2011). Each participant is then able to rate the reputation (or reliability) of others and the results of these evaluations can then be displayed next to each individual's nickname. The rationale behind this form of peer recognition is that those with higher levels of reputation will be better business partners and can be more trustworthy. Reputation is therefore used as the key to limiting the degree of victimization on specific online illicit markets which have adopted recognition scales.

These systems have been the focus of a limited number of papers such as Monsma et al.'s (2010) who collected data from an online discussion forum to understand how criminals network with each other. Their hypothesis is that resources, reputation and status all affect the shape and size of personal networks. The findings indicate that all three factors affect one's success in creating a more elaborate and richer network of contacts. This should in turn be translated into higher illegal revenues. Motoyama et al. (2011) also used data from online forums to understand how public ratings (reputation) impact criminals' level of business activity. In their analysis, the individuals with higher ratings receive more private messages, thus indicating a greater level of illicit activities. In this case, the rating system is apparently seen as a method for ascertaining a possible partner's reliability. Pushing this conclusion further, Mell (2012) build a theoretical model to understand the relation between activity and reputation. In this paper, the role of reputation is stressed in the context of online criminal markets where it is difficult to assess the trustworthiness of others as well as the quality of the goods they are selling. Mell's (2012) model focuses on the work of discussion forum administrators, who are tasked with the evaluation and rating of each of the forum members, using past transactions and activity levels as guides. The administrators' job is to root out scammers to increase market fluidity. Mell (2012) finds that if administrators do their job properly, it is possible theoretically to have an efficient market where stolen data can be bought and sold without problems. This opens the door to possible disruption operations by law-enforcement agencies that could pressure administrators into making false ratings of users.

Online markets are not the first to take advantage of the notion of reputation to increase fluidity and efficiency. In the real world, the role of reputation was highlighted in a few ethnographies that focus on offenders. Steffensmeier's (2005) *The Fence* relates the day-to-day life of a stolen goods reseller (also known as fence) that deals in stolen goods. In the book, Steffensmeier details how Sam Goodman, the main character in his study, worked extensively to build a reputation for fairness among the thief community. To do so, Sam had to network with local thieves and behave in a way that showed his respect for their profession. It is of the utmost importance that fences build such a reputation in order to keep the flow of stolen goods coming. According to the author, a bad reputation only increases the risks of being snitched on

or of losing suppliers. Bad reputation is also a cause of concern for many other fringes of society. Bourgois (2002) spent five years of his life with drug dealers in the Spanish part of Harlem. During that time, he came to understand the value of a bad reputation as his subjects were consistently precluded from integrating into the mainstream society and were forced to become criminals in order to support themselves. In this case, bad reputation was built on a bias about the ethnicity and socioeconomic status of Bourgois' (2002) subjects. The explicit violence described in Bourgois' (2002) book is a vivid reminder of the consequences of having a bad reputation and the racism that still affects many segments of the population.

More specific information on criminal reputation can be found in past research papers that focus on organized crime in the United States. According to these studies, recognition is not distributed evenly among offenders. As criminal enterprises are usually short-lived, there is little incentive for most criminals to invest in a reputation that may yield dividends in a distant and uncertain future (Gambetta, 2009). More stable organizations such as the Mafia or the Hells Angels have however established solid reputations from the outset first and this has helped to reduce their costs later on. This is basically Reuter's (1983) idea of the Mafia as a paper tiger. The Mafia first had to build a reputation for violence, which was expensive in human and financial resources. Once this reputation was established, the Mafia could discretely reduce their investments in those resources and still enjoy the benefits of their reputation for violence without the associated costs. A strong reputation is therefore a sign of higher profitability and higher earnings for criminals.

The components of reputation

While we have come to understand the value of reputation, we have yet to fully understand how some individuals accumulate more recognition than others, especially in an online context. Partial answers to this problem can be found in the papers we have mentioned above. The hints they provide can be categorized in three classes that we labeled personal characteristics, networking and behaviour. The importance of who you are (i.e. personal characteristics) is highlighted in Bourgois' (2002) drug dealers. Their bad reputation in the mainstream population was caused by their origin, style and socioeconomic status. Who you know (i.e. networking) is also important to make sure that a reputation spreads and to raise one's profile by associating with the right kind of individuals. Steffensmeier (2005)

highlighted this by demonstrating that strong relationships with suppliers ensure a steady flow of stolen goods for fences. Other papers have also shown that mentioning the right name to the right people could alter one's reputation and increase criminal opportunities. Glückler & Armbrüster's (2003) also highlight the need for networking in a market. Contacts can spread the word about the reputation and quality of consulting firms, raising the chances of landing new contracts. Individuals are often afraid of the unknown and common acquaintances can help to reduce uncertainty between possible partners. Such bonds are usually built over long periods of time and through shared experiences. The final class of predictors of reputation refers to what you do (i.e. behaviour). Williams & Barrett (2000) have demonstrated that reputation evolves through time and is affected by behaviour. Companies that made generous contributions to charity saw their reputation level increase. Steffensmeier (2005) also raised this point by emphasizing the willingness of Sam Goodman to deal fairly with thieves. Of course, this behaviour was not altruistic as we explained before but it still allowed him to maintain a high level of reputation with his partners. A last example of the importance of behaviour can be seen in the Mafia. As Reuter (1983) has shown, it used violence to build a strong reputation that later scared others into submission. The aggressive behaviour of the mafia is an integral part of its reputation.

Building on this research, the starting hypothesis of this paper is that reputation varies with the personal characteristics, the networking and the behaviour of offenders. The aim of this paper will be to validate this hypothesis empirically by studying criminals in the context of an online forum where stolen credit and banking data is bought and sold. Our goal will therefore be to understand how reputation is formed in an online criminal network. Understanding the mechanisms according to which reputation is built is even more important in illegitimate than legitimate markets, as criminals cannot advertise their goods and services. They must thus rely on word of mouth to ensure that their business keeps growing (Gambetta, 1993). As criminal markets require frequent interactions between many suppliers, brokers, and buyers, a good reputation will ensure a greater pool of possible co-offenders with whom to cooperate (Steffensmeier & Ulmer, 2005).

While a good reputation may be desirable due to its positive impact on financial gains, it is also a means to an end in itself in the criminal underground. Goode & Cruise (2006)

demonstrate that peer recognition is an important motivation for software crackers who distribute products online illegally. While the technical challenge of cracking the protection scheme of games and software is their prime motivation, the desire for social status is evident in many crackers who can then use this reputation to join more established hacking groups. The same need for reputation can be found in Poulsen's (2011) book on the credit card thieves' community, where a single person, Max Butler, managed to take over a sizeable portion of the market for stolen credit data out of sheer vanity. His goal was to fix the exchange market where stolen information was sold. For many individuals in the criminal underground and law-enforcement agencies, his online nickname was famous and that enabled him to gather impressive illegitimate revenues. The fact that this reputation also attracted a great deal of attention from law-enforcement agencies may have reduced the benefits of being a famous hacker.

Obviously, this paper will focus on a single online criminal market, which will limit the generalization of the results and conclusions. The mechanisms influencing a criminal reputation may and should be different on and off the Internet. As this is one of the first papers to focus directly on criminal reputation, it makes sense to begin investigating this field of research in an online criminal setting. Indeed, the availability of all public discussions and relations between members of the community provides researchers with a comprehensive understanding of a criminal market. It also ensures access to unbiased data that was not contaminated by the researcher's actions. The fact that online forums have adopted official recognition indices facilitates the evaluation of reputation in such a context and removes much of the subjectivity that would arise from a formal assessment of each actor's prestige. This reinforces our belief than online communities of criminals are good starting places to build an understanding of reputation in the criminal underground.

Data

This paper focuses on a single online criminal market where botmasters and customers met to discuss, buy and sell botnet-related services. This market was hosted on a web forum where each messages were divided in threads. Each thread usually focused on a single topic and included messages by up to a few hundreds participants. This forum was selected by using Google Search and searching for the *forum* and keywords related to botnets. We created a

custom program that downloaded one by one each of the HTML page containing the discussion threads and extracted the content of the messages in a database. In addition to the content of the message, this database included the author of the message, the timestamp of the message, the thread in which it was posted as well as the order in which the message was posted. Our custom program also downloaded each of the profile information of every participant in the market which included a username (or nickname), the date of registration, the date of the last visit, the date of birth, the local time, the number of times the user had changed his public username, the total number of messages posted online, the number of individuals referred to the forums, the number of user groups he was a member of, a list of awards given by the forum administrators, as well as a reputation score. Most of these variables are self-explanatory except for two: user groups and awards. There were 8 user groups active in this specific botnet forum. Members could decide on their own to join any of these exclusive user groups; they first had to be invited by a member or an administrator of that user group. Some user groups would accept donations to facilitate one's application to the group. Membership in these groups was seen as a social distinction by participants. Awards were given by the forum administrators to select members who had performed certain tasks or had reached a certain status. There were over 50 different types of awards. Some may highlight a member's entrepreneurial sense (the *Businessman* award) while others may celebrate a member's design skills (the *Graphic Masters* awards).

In total, we gathered data on 20,270 profiles who were active on the forum between February 3rd, 2007 and November 26th, 2011 and who posted 248,634 public messages in English (the only language of the forum). Given the inherent hostility of the online market (Franklin et al., 2007), participants adopted a method we described earlier to reduce risks and increase market fluidity: the reputation index. Members who had reached a certain level of trust and reputation in the online community as well as those who paid a predetermined fee were granted by the forum administrators the right to give and/or take reputation points from other users. This was fairly easily done through an online form which was always only a click or two away. Users could choose the number of points they wished to add and/or remove and write a reason motivating their action. Each participant began their career on the forum with a total of 0 points and earned (or lost) points as time went by. In the case of the forum we

studied, the system was based exclusively on peer recognition, meaning that administrators had no say in the reputation of participants. Only members could increase or decrease the reputation of one of their own. Administrators were proud of this free market of recognition (i.e. never modifying the reputation score of users) and only interfered in blatant cases of abuses. This quantitative evaluation of reputation is very different than what was used in other research (see for example Holt, 2012)) which took a more qualitative approach to reputation and included peer reviews in threads as well as reviews by administrators. Given the size of the data analyzed, it would have been impossible for us to manually code each of the product reviews and comments made on the individuals. As the market had a formal and easy to use mechanism for disseminating the reputation of participants (the recognition scale), we felt that it would not be necessary to include such evaluations in our top-level view of the botnet forum. While these comments may increase the reliability of each participant's reputation, the recognition index was used enough times (over 200,000 times) to convince us that it was a well-known and popular way of warning others about scammers or of rewarding good behavior on the forum.

Given the limited size of the sample (only one forum), it will not be possible to generalize the results of this study to other online illicit markets, even those centered around botnets. What this paper lacks in term of generalizability can be compensated by the depth of the data analyzed. Every message and every participant of the forum will be included in our quantitative analysis (see below), providing us with a rare global image of the recognition scale of an online illicit market. Numerous references can be found online about the forum we used for this paper proving the relevance of this online forum in the criminal ecosystem. While it may not be representative of all markets, it is a part of this ecosystem and future research may improve on this paper by studying other forums, therefore developing our understanding of this new breed of criminals. Registration on this forum was open to anyone with a valid email address. Administrators therefore did not screen potential market participants which increases the chance of finding scammers or more inexperienced users in this forum. Those individuals would not have access to the more elite and exclusive online marketplaces. Still, illicit goods and services were traded on this forum by many participants and our analysis will reflect the level of involvement in the criminal ecosystem of these individuals.

Methodology

To understand the mechanisms according to which recognition is distributed in an online criminal market, this paper will use a multi-level predictive model, which uses both static and dynamic variables. In this first part of the methodology section, we will detail the operationalization of the variables. In the second part, we will present the multi-level predictive model designed for this research.

Operationalization of variables and descriptive statistics

To build the multi-level predictive model, a series of variables had to be created. The *number of days spent on the forum* was calculated by counting the number of days between registration and the last day of visit to the forum. The *origin* was estimated by comparing the local time of the participant (as disclosed by them) with the researcher's local time. This enabled us to make an educated guess as to where the criminal was located in the world. We created five categories that included America, Oceania, Europe/Africa/Asia, Asia and Unknown. This somewhat crude way to identify the origin of individuals meant that Asia had to be separated in two categories as some of its time zones are also used in Europe and Africa. It was therefore impossible to separate the two from each other. The limited reliability of this metric will be taken into account when we interpret the results.

To gain a more thorough understanding of the messages posted on the forum, we opted for the use of specialized software called SentiStrength, which has been used in the past to estimate the sentiments (both positive and negative) of messages. The program has been evaluated in peer-reviewed academic articles and has proven its ability to measure the sentiments of messages (Thelwall et al., 2010). The software gives scores to each message on a scale of 1 to 5 for its *positive sentiment* and on a scale of -1 to -5 for its *negative sentiment*. Each message receives both a positive and negative score as it can contain diverging sentiments (ex: "I love myself but I hate you"). On the SentiStrength scale, scores of 1 and -1 indicate neutral messages. To facilitate the analyses, we subtracted 1 from all positive sentiment scores and added 1 to all negative sentiment scores. This left us with scales which ranged from 0 to 4 and from -4 to 0. We then calculated a total score for each member both on the positive and on the negative scales. A random sample of messages was tested manually by the researchers to ensure that the results provided by SentiStrength were indeed accurate.

We also measured the social capital of forum members through two metrics: the *ego network size* and Burt's *constraint* (Burt, 1992). The ego network size refers to each individual's (the ego) personal network and counts the number of people who were in direct contact with that person. Burt's constraint is a measure of the structural holes in the personal network of each person. It measures the extent to which an individual's contacts know each other. A low constraint measure indicates that an individual's contacts are seldom connected and must therefore use the individual to interact with one another. This enhances one's power in a network. To build these networks of ties, we used the public messages posted on the forum. There, messages were divided into discussion threads, which centered around one subject usually. In each of these threads, a person was considered to be tied to all the individuals who had posted a message before him. In the advent that a person posted multiple messages in the same thread, we only counted the ties which were created since the last message.

Table 1: Example of message listing in a thread

MESSAGE RANK	NAME
8	Peter
7	Mike
6	Donald
5	Mike
4	Jeff
3	Holly
2	Mike
1	James

Table 1 provides an example of a thread where six individuals (James, Mike, Holly, Jeff, Donald and Peter) post eight messages in the order presented in the first column. In this case, Peter would be tied to all five other individuals who posted in the forum before him

(James, Mike, Holly, Jeff and Donald). The same would go for Donald who would be tied to Mike, Jeff, Holly and James. Mike, however, would have a different pattern as he has posted three messages in the same thread. In this case, Mike would be tied to James with his first message, to Jeff and Holly with his second message and to Donald with his third message. This somewhat complicated the data-gathering process but increased the quality of the data and enabled us to measure more precisely the ties between individuals.

In the results section, we will first present descriptive analyses which include minimums, maximums, means and medians for the variables we created (origin, positive sentiment, negative sentiment, ego network size and constraint) as well as those taken directly from the database (reputation points, number of days spent on the forum, age, number of messages posted, number of awards, number of nickname changes, number of memberships in user groups and number of people referred to the forum).

Multi-level model

This paper aims to incorporate both static and dynamic variables in a single model that predicts the distribution of recognition amongst a population of members of an online forum dedicated to botnets. To achieve this goal, we employed hierarchical linear modeling (HLM) also known as multi-level modeling (Raudenbush et al., 2004). This method allowed us to take into account the variances within the same individuals over time (level 1) as well as between individuals (level 2). The HLM software version 7 was used for our analyses (Raudenbush et al., 2004).

Fischer et al. (2008) describe how multi-level modeling works. HLM begins with a regression equation for each individual in the population, the level 1 of the multi-level model. This regression measures the probability that an event occurred during a given period of time. In this case, we estimated the probability that an individual had received or lost reputation points during any given month based on the following dynamic statistics: number of days spent on the forum, age, number of messages posted, number of awards received, number of positive sentiment points, number of negative sentiment points, ego network size and constraint. A value of each variable was calculated for each individual and for each month over a period of 27 months, which ranged from October 2009 to December 2011. These

variables are known as time-varying observations. The level 1 regression was thereafter recalculated taking into account the level 2 or time-invariant variables. In this case, these include: the number of nickname changes, the number of memberships in groups, the number of people referred and the origin. The value of these variables was calculated for each individual but did not change over time[16]. The combination of these two regressions output a regression coefficient for each variable which enabled us to evaluate its impact (*Y* coefficient) and relative size when compared to other variables (*T* coefficient). A *T* coefficient equal to or greater than 1.96 indicates that the relation between an independent and a dependent variable is statistically significant.

Five hierarchical linear models are presented in the results section. For each one, the dependent variable is the number of reputation points received or lost each month. This metric was recoded as -1/0/1 depending on whether the member lost, did not receive or gained reputation points each month respectively. We opted for the analytical strategy to facilitate interpretation of the results and because of the large number of cases where no recognition, both positive and negative, was given. This transformation will therefore allow us to normalize the distribution of our dependent variable. In doing so, it is true we lose some sensitivity in our results as an individual who would receive more positive than negative recognition within a month would be classified in the positive category (1) despite the fact that some of his behaviour induced others into giving him a negative recognition. To measure the impact of this loss of sensitivity, we calculated the distribution of all possible scenarios:

1) Received positive recognition: 13.1%
2) Received both positive and negative recognition (more positive than negative): 2.1%
3) Received as much positive as negative recognition: 0.3%
4) Did not receive recognition: 81.9%
5) Received positive and negative recognition (more negative than positive): 0.8%
6) Received negative recognition: 1.8%

[16] Some variables presented as static did change over time but we were unable to pinpoint the exact moment of these changes and therefore had to include them as static variables in our model.

This distribution indicates that there is indeed a bias in our analysis, particularly in the case of the negative category (-1) where a third of the sample has accumulated positive and negative recognition. This limit, however, is not as problematic as it seems. Indeed, the forum participants generally had access only the total reputation score of individuals rather than details of all the recognition. In this context, the majority of participants in the forum were witnesses of the final result of all these recognition transactions. Our methodology thus reproduces what regular forum members saw, the sum total of all the recognition.

A linear regression model was chosen for these analyses given the distribution of recognition amongst the population. Model 1 presents a base model without any independent variables. Model 2 and model 3 present the impact of level 1 (time-varying) and level 2 (time-invariant) variables distinctly and respectively. Model 4 includes all independent variables in the same model. Finally, model 5 is a parsimonious model (Model 5) that only incorporates statistically significant variables.

Results

Table 2 presents the descriptive statistics of the dependent and independent variables in our predictive model.

Table 2: Descriptive statistics for level 1 and level 2 variables

	Minimum	Maximum	Mean	Median
Dependent variable				
Reputation	-729.00	2297.00	21.94	0.00
Level 1				
Nb of days spent on forum	1.00	1698.00	376.57	324.00
Age	12.00	101.00	24.27	21.00
Nb of messages posted	1.00	21393.00	454.59	63.00
Nb of awards	0.00	16.00	0.19	0.00
Nb of points for positive sentiments	0.00	2465.00	18.12	4.00
Nb of points for negative sentiments	-2559.00	0.00	-17.33	-3.00
Ego network size	0.00	5679.00	225.58	52.00
Burt's constraint	0.00	1.23	0.23	0.16
Level 2				
Nb of nickname changes	0.00	127.00	1.56	0.00
Nb of memberships in groups	0.00	8.00	0.23	0.00
Nb of people referred	0.00	358.00	0.42	0.00
ORIGIN: America	15.33%			
ORIGIN: Oceania	1.31%			
ORIGIN: Europe, Africa, Asia	55.19%			
ORIGIN: ASIA	20.24%			
ORIGIN: UNKNOWN	7.92%			

Forum members have an average of 21.94 reputation points indicating that, overall, reputation tends to be more positive than negative. Over half of members do not however have a reputation score (Median = 0.00) and the distribution shows great variability with a low of -729 and a high of 2297.

Members maintain a presence on the forum for a considerable amount of time (Mean = 376.57 days). The median is fairly close to the mean at 324 days, indicating that once members join this forum, they tend to maintain their involvement over long periods of time. This differs from previous research on cybercrime, which found that individuals did not

remain active for more than a few weeks or months (Décary-Hétu et al., 2012). Members are on average 24 years old (Minimum = 12; Maximum = 101). This metric may not be totally reliable as individuals entered their age in their profile themselves and were never asked to validate this information. Our analysis will take this fact into account when interpreting the results.

Forum members tend to post hundreds of messages (Mean = 454.59) with power users posting up to 21,393 messages. This denotes a strong sense of belonging in this community, as individuals feel compelled to participate and post messages. A select few members are rewarded for their work with an award from the administrators. Less than one in five individuals manage to receive such an award. Points for positive and negative sentiments are distributed almost evenly (Means of 18.12 and -17.33 respectively) in the population. This stresses the neutral nature of the community. If the forum had been an overly conflictual setting, it would have showcased much higher negative than positive sentiments.

Unsurprisingly, the ego social networks of forum members are fairly large at 225.58 contacts on average with a median of 52. These numbers are broad and likely inflated estimates of the pool of resources and potential co-offenders each botmaster has access to. They still highlight the social nature of this community and the ease with which each person can be contacted. Individuals are for the most part unconstrained in their personal network (Mean = 0.23) indicating that members tend to build their network of contacts in such a way as to stay indispensable to others.

As for level 2 (time-invariant) variables, forum members rarely change their nickname (Median = 0), strengthening the idea that hackers value their nickname and online persona. Only a select few individuals are allowed into user groups (Mean = 0.23). As the HLM will demonstrate however, membership is an efficient gateway to a higher reputation. Given the open nature of the botnet forum (no referrals are needed to join), users seldom refer new members (Mean = 0.42; Median = 0), although the maximum of 358 shows that some members thought it may be beneficial to do so. Finally, more than half of the population comes from Europe, Africa or Asia. Asia by itself also accounts for 20.24% of users while

America comes third with 15.33%. Less than 8% of members indicate that they are from time zones outside of these zones.

Table 3: Predictive model of reputation points in an online botnet forum

	Model 1		Model 2		Model 3		Model 4		Model 5	
	Y	T	Y	T	Y	T	Y	T	Y	T
(Constant)	0.108	63.647	0.107	63.608	0.099	78.574	0.099	78.551	0.099	78.556
Level 1										
Nb of days spent on forum			0.000	14.966			0.000	14.966	0.000	14.966
Age			-0.012	-5.544			-0.012	-5.544	-0.012	-5.544
Nb of messages posted			0.003	3.694			0.003	3.694	0.003	3.694
Nb of awards			0.206	26.596			0.206	26.596	0.206	26.596
Nb of points for positive sentiments			0.003	2.801			0.003	2.801	0.003	2.801
Nb of points for negative sentiments			0.003	3.288			0.003	3.288	0.003	3.288
Ego network size			0.000	13.180			0.000	13.180	0.000	13.180
Burt's constraint			0.053	11.417			0.053	11.417	0.053	11.417
Level 2										
Nb of nickname changes					0.001	3.323	0.001	3.318	0.001	3.318
Nb of memberships in groups					0.261	40.299	0.261	40.308	0.261	40.320
Nb of people referred					0.002	2.208	0.002	2.211	0.002	2.211
ORIGIN: Oceania					n.s.		n.s.			
ORIGIN: Europe, Africa, Asia					-0.038	-9.112	-0.038	-9.115	-0.037	-9.469
ORIGIN: Asia					-0.031	-5.962	-0.031	-5.977	-0.031	-6.089
ORIGIN: Other					-0.018	-2.510	-0.012	-2.514	-0.018	-2.523
σ^2_μ	0.04243		0.04257		0.02239		0.02251		0.02251	
σ^2_ε	0.11575		0.11397		0.11563		0.11386		0.11386	
Statistics										
Deviance	211657.994		207950.559		202665.547		198963.232		198954.362	
Chi-square	124829.144		126785.849		73198.709		74337.386		74337.794	
DL	20238		20238		20232.000		20231		20232	
P	< 0.001		< 0.001		< 0.001		< 0.001		< 0.001	

Model5-Model4: $\chi 2 = 0.408$ dl = 1

Level 1 and level 2 variables are all part of the multi-level models presented in Table 3 and predict the probability that a member receives or loses reputation points during any given month. A T value equal or higher than 1.96 indicates that the result is significant ($p > 0.05$). Model 1 is the base model, which establishes the maximal variance of each level.

Model 2 only integrates level 1 variables that are significant predictors of reputation. The number of awards, the number of days spent on the forum, the ego network size and Burt's constraint are the four most important variables (T=26.596, T=14.966, T=13.180 and T=11.417, respectively). Age is the only negatively correlated variable (Y = -0.012), which indicates that younger members tend to receive more reputation points. This model is significant ($\chi 2 = 126785.849$; $p < 0.001$) but the explained variance is very low (see Table 4).

Table 4: Variance explained by each level of the multi-level models[17]

	R^2_2	R^2_1
Model 2	0.00	0.01
Model 3	0.47	0.13
Model 4	0.47	0.14
Model 5	0.47	0.14

Model 3 removes level 1 (time-variant) variables and incorporates level 2 (time-invariant) variables. This model is much more appropriate to explain the variance in the dependent variable ($R^2_2 = 0.47$) and is significant ($\chi 2 = 73198.709$; $p < 0.001$). The Oceania origin is the only non-significant variable and the number of memberships in user groups is by far the most important factor (T=40.299). Americans receive more reputation points than others as all other origins have negative regression coefficients. All other variables are positively correlated to reputation points.

[17] It may be surprising to notice that the explained variance of the level 1 variables actually increases when they are removed and replaced with level 2 variables in the Model 3. This indicates that the static variables (level 2) actually have a wide distribution at the dynamic level (level 1). To illustrate this results, we could use the example of a multilevel model that would explain the grades of students in a class and in a school. In this case, the characteristics of classes in a single school would be so different that they would contaminate the other level.

Model 4 combines all level 1 and level 2 variables in the same model with an explained variance for level 1 of 0.14 and of 0.47 for level 2 (see Table 4). That model is also significant ($\chi 2 = 74337.386$; $p < 0.001$). The number of memberships in user groups is still the most important factor (T=40.308) but level 1 variables (number of awards, number of days spent on the forum, ego network size and constraint) hold the next four ranks (T=26.596, T=14.966, T=13.180 and T=11.417, respectively). Only one variable is not significant and that is the Oceania origin.

The last model, Model 5, is a parsimonious model which only incorporates statistically significant variables: 8 level 1 variables and 6 level 2 variables. This model is significant ($\chi 2 = 74337.794$; $p < 0.001$) and only differs marginally from the complete Model 4 (Model5-Model4: $\chi 2 = 0.408$; DF = 1). The explained variance for Model 4 and Model 5 is identical at 0.14 for level 1 variables and 0.47 for level 2 variables (see Table 4). The low explained variance of level 1 variables could be an artefact of the dataset as less than half of members actually received reputation points, and each only for a few months of the sample. This relatively low occurrence of the predicted variable reduces the explained variance of level 1 variables and increases the apparent importance of level 2 variables. Still, the significance of Model 5 allows us to dig more deeply into the meaning of the correlation of each independent variable.

The number of days spent on the forum increases one's reputation points (Y=0.000; T=14.966). Craig (2005) has found that more experienced members play an important role in other hacking communities as they are sought for their advice and expertise. The same could be said of members in this online forum. Younger members also receive more points than elders (Y=-0.012; T=-5.544). This ageism could be a consequence of the hacking mentality where older people are seen as out of touch and unable to understand new technologies. Young individuals may also have more free time to spend on the forum, giving them more opportunities to interact with others and to garner reputation points. These results may be skewed by the self-reporting of this metric and our inability to validate the real age of forum members.

Active users who post more messages raise the number of reputation points they will receive from others (Y=0.003; T=3.694). By posting often and regularly, users enhance their public profile and reputation in their community. This is viewed favourably in the botnet scene as it displays one's sense of belonging and involvement in the community. Awards are also very important (Y=0.206; T=26.596) and members who earn or purchase them attract more reputation points than others. Receiving an award highlights a special trait of a member and it draws the public eye to specific members. This reveals the presence of a criminal star system but also that administrators who are in charge of handing out awards can influence the reputation level of members.

Positive and negative sentiments play a more marginal role than awards but both contribute to one's reputation (Y=0.003/T=2.801 and Y=0.003; T=3.288, respectively). Negative sentiments play a marginally more important role than positive sentiments (T=3.288 versus T=2.801). It may be surprising to see that both positive and negative sentiments are positively correlated with the dependent variable. This indicates however that when negative sentiments are closer to 0 (less negative on the scale of -4 to 0), they increase one's reputation.

Finally, both social network metrics are positively correlated to the reputation points (Y=0.000/T=13.180 and Y=0.053/T=11.417, respectively). A larger personal network increases access to resources and possible partners, which enhances one's reputation in the community. Detection costs are associated with such visible positions but the short-term benefits are clear in this multi-level model. Burt's constraint indicates that members who participate in closer-knit subgroups where individuals are all connected receive more points. These individuals could be playing the system by exchanging positive evaluations. In this scenario, users would all agree to give reputation points to each other. This would enhance everyone's profile without having to do any actual work. Their close and strong relationship may also increase the flow of information, giving them more reasons to give points to each other.

The level 2 (time-invariant) variables provide a different but interesting understanding of the notion of criminal reputation. The number of username changes is positively correlated with the reputation points (Y=0.001; T=3.318). Changing one's public nickname may help to

attenuate the effect of a bad reputation as a new online persona is a chance to start anew in the community. It may prove difficult for members to determine if a particular member was known under a different alias in the past.

Membership in user groups is the most important factor for predicting who will receive reputation points (Y=0.261; T=40.320). These exclusive clubs seem to raise the profile of their members just as private clubs in legitimate networks may increase one's profile in a business circle. Referring people is also important, as those that were referred may feel compelled to give reputation points back to the person who introduced them to the online forum. This result is interesting as anyone can register on the forum without needing to introduce a member. Referrals are therefore optional and only serve as a public display of connection between two individuals.

Discussion

The HLM model presented in this paper demonstrates that recognition is not distributed randomly in an online community of botnet enthusiasts. On the contrary, many factors affect each individual's capacity to attract praise and respect from others. The three most important factors are the number of awards received, the number of days spent on the forum and the size of the ego network. This confirms our initial hypothesis that stated that reputation is built on personal characteristics (age, number of awards, number of nickname changes, number of memberships in groups and origin) networking (ego network size, Burt's constraint and number of people referred) and behaviour (number of days spent on forum, number of messages posted and number of sentiment points). All three set of variables were significantly correlated to the reputation points.

Gambetta (2009) mentioned that only long-lasting criminal enterprises seek and gather a criminal reputation. This statement is corroborated by our data, as the number of days spent on the forum is a predictor of the level of reputation. The individuals who intend to remain active for longer periods act in a way that attracts the attention and respect of others, increasing their recognition scale. This reputation can then be used to convince others to build business relationships with them at lower costs. This confirms past research by Thomas & Martin (2006) who found that participants want long-term customers as it reduces risks.

Even though the reputation index is entirely based on peer recognition and even though administrators openly refuse to interfere with the granting of reputation points, this model demonstrates that administrators play a major role in the distribution of recognition. By allowing specific members to become members of user groups or by handing out awards, they have a lasting impact on each individual's reputation. Administrators clearly play an important role in the forum and are some of the most respected members on the forum. When they identify a member as important by taking the time to recognize their implication, others follow suit and grant these individuals reputation points that could then be used to increase one's illegitimate revenues. This suggests the presence of a criminal star system where administrators crown the next up-and-comers as they see fit. This approach by the administrators is one that is less hands-on compared to what was found in past research (Holt & Lampke, 2010). This represents an improvement in the security of the market as removing the administrators would not necessarily disrupt the daily working of the forum. Administrators in this case can be compared to the brokers in Morselli's (2009) papers, individuals who facilitate crimes and who hide behind the scenes. These brokers prefer to play their role indirectly by using more visible individuals to do their bidding while they keep their true involvement to themselves. In the case of our botnet forum, administrators officially play a very small role but as we have demonstrated, their impact on the success of criminals is very real.

Members' behaviour on the forum is still very important, as our content analysis of the sentiment of messages demonstrated. Surprisingly, in this criminal community, individuals who received more reputation points posted more positive messages. Individuals who are positive in their public messages increase their reputation points and those that are negative lower their number of receiving points. One may have expected this forum to value snarky and condescending remarks and to reward the members who insult unworthy and unskilled participants. This is not the case in the present study. This could be explained by the importance of the market in this criminal setting. Members participate in the forum to find suppliers or buyers for their illegitimate businesses. There is a high level of mistrust and doubt between members given the number of scammers and fraudsters in their field of work. To convince others of their trustworthiness, members must send consistent and repetitive signals

that they are reliable and can deliver on their promises. Members must also face heavy competition, as the barrier to entry into the botnet industry is fairly low. Their best option for winning over possible business partners and co-offenders is to appear positive and open in their public messages. This confirms past findings from Motoyama et al. (2011) and Monsma et al. (2010) which highlighted the need to network with others in order to increase one's performance. Social networking is correlated with a higher status and a better reputation in their studies. Nurturing positive roles with others in the community therefore appears as a necessary step to maintain one's status and to potentially increase one's business success. While these research focused on the presence or absence of ties, our study takes a different approach by evaluating the quality of the ties themselves through our SentiStrength measure. This proves that positive ties have an impact on reputation just that it is not just who you know that is important but what your relation with that person is.

These findings lead us to a new question that we have yet to address, the strength of reputation. Knowing how reputation is built is one thing; understanding how to maintain this reputation and/or destroy it is another. Given the importance of reputation in criminal markets, competitors and law-enforcement agencies may very well try to destabilize online markets by abusing their recognition system. We already presented three classes of attacks in this paper: the identification of key players (Chu et al., 2010), the Sybil and the slander attacks (Franklin et al., 2007).

Our results demonstrate that recognition systems could be used to easily identify key players in online illicit markets. As recognition is not distributed randomly and is associated with specific profiles of behavior, networking and personal characteristics, it could be used as a proxy of involvement in a criminal market and therefore be used to determine which participants should be removed from a community. Given the large size of the population active at one point or another in the market (over 20,000 profiles), adopting this technique may necessitate large investments of money and manpower in order to detect, identify and remove specific individuals. While studying the participants with the highest level of reputation may be useful to gather intelligence on the participants that are most involved in the community, removing any number of them would be a challenge for law-enforcement agencies.

In our specific case study, attacks that would focus on creating fake profiles with a high level of reputation (the Sybil attack) would also be hard to implement. The main factors responsible for reputation are user group membership and awards. Both of these require that users maintain and prove involvement in the botnet community for extended periods of time. The next series of factors include experience (number of days on the forum) as well as social networking. Both of these also require investments from participants over a certain period of time. Seniority on the forum cannot be faked. Social bonds, for their part, need to be developed and sustained over extended periods of time through shared experiences and transactions. These factors all demonstrate the impossibility for outsiders to quickly build a strong reputation on the forum. Reputation is based on character and behaviour and needs to be reinforced repetitively over time. These mechanisms ensure that only those who deserve a good reputation actually get one. In such a hostile environment, very few signals allow botmasters to judge the trustworthiness of others. As reputation is one of the only tools available to do so, it is not surprising to see such protection around it. Reputation therefore appears as a strong indicator of someone's character and trustworthiness in the botmasters' forum and something that cannot easily be faked.

We find that slander attacks where random and false accusations are made against participants with high levels of reputation would be the easiest to implement and the approach with the highest chance of success. Posting accusing public messages and contacting administrators to complain about the behavior of participants could be achieved rapidly and easily and repeated through time very efficiently. While these accusations may not stick, they may create a reasonable doubt in the other participant's mind. Unfortunately, members with high levels of reputation could always rely on the status that comes with their experience and extended social network to offset any attempt to destroy their reputation. Given the relatively low impact of user behaviour on the forum, it appears that accusations and bad behaviour on the forum have little impact on an actor's reputation and that once a good reputation is established, it tends to maintain itself over time.

Conclusion

Our results should be of great interest to researchers working on the concepts of achievement in criminal markets and criminal careers. Past research has demonstrated that just

like reputation, criminal achievement is not distributed randomly amongst the criminal population. On the contrary, a limited set of factors has been repeatedly identified as the predictor of higher illegitimate earnings and/or lower rates of detection by law-enforcement agencies: criminal mentors (Bouchard & Nguyen, 2009), the number of contacts (Nguyen & Bouchard, 2011), the structure of personal networks (Morselli et al., 2006), experience and skills (McCarthy & Hagan, 2001), low self-control (Morselli & Tremblay, 2004) and enrolment in criminal organizations (Tremblay et al., 2009). Criminal achievement and reputation share many contributing factors that suggest a link between the two concepts. It is very possible that criminal reputation could increase one's illegitimate revenues (and vice-versa). Further research should be conducted to better understand the relationship between the two concepts. Reputation could also be a motivation for criminals to continue their criminal career. As Goode & Cruise (2006) demonstrated, hackers strive to build their public reputation in their peer community and understanding how criminals achieve high levels of reputation could help understand why some criminals desist while others continue to commit crimes. The link between criminal achievement and reputation could be very helpful in answering this question.

This paper focused on the recognition index of an online botnet community. Our work was facilitated by the fact that such an index exists and that a complete copy of the forum could be easily downloaded for detailed analysis. Obtaining such comprehensive datasets on other illegitimate markets such as the drug market may prove to be much more difficult. This would require researchers to build and distribute surveys to as many participants as possible and to include questions on each participant's reputation in the market. While feasible, we would suggest that further studies be completed on online communities where access to data is much less cumbersome. The knowledge and experience from these papers would serve as the basis for extended work on criminal achievement in criminal markets with fewer ties to the Internet.

Further studies should look into a more diverse range of criminal markets such as carding and identity theft. These markets also use online message boards and chat rooms to build connections between participants and to alleviate the inherent frictions of such environments. The methodology of this paper could be directly applied to other research and

the results compared to determine if the distribution of recognition is unique to the botnet community or if bigger trends can be extracted from our dataset.

Finally, we would encourage further research into the value of recognition indices in online communities. This formal representation offers a view of each member's reputation that may be different from informal reputation. There may at times be discrepancies between what individuals think of someone and what they are ready to openly say about them. It would be very interesting to use qualitative analysis of conversations and surveys to measure precisely the reliability of recognition indices for measuring the prestige of criminals in an underground forum. Given the popularity and adoption rate of this tool, it appears as though these indices are in a position of strength but as is always the case, qualitative data may enable us to better understand how prestige is allocated in this community. It would also be interesting to further investigate the trends and patterns of accumulation of reputation. Our model did not include a measure of the reputation level of individuals in the previous months which could have contributed to the later levels of reputation. Indeed, it is possible that individuals received recognition because of their already high level of reputation. It would be the equivalent of paying your respects to the most notorious actors in the market. In this particular case, group-based trajectory analysis as described by Nagin (1999) may prove to be an interesting research model.

In the discussion part of this paper, we purposefully neglected to mention Glenny's (2011) work on the DarkMarket carding forum. DarkMarket was in the second part of the 2000s the largest English-speaking carding forum and had at its peak over 2,000 members, each vetted individually to ensure that they were experienced cybercriminals. The FBI used an undercover agent to infiltrate the forum and to eventually earn the trust of its administrators. The operation was a total success as the FBI managed to gain control of the master server on the forum, allowing it to identify many of the top members of the forum. This lead to the arrest of over 60 individuals and the prevention of tens of millions of dollars in fraud. To achieve such a high impact on the carding community, the FBI had to assign one of its special agents to this case full-time and to make sure that he logged on the carding forum every day for hours. This was done to raise the profile of this undercover agent and to create ties with the forum administrators. As time went by, the agent saw an opportunity to move up in the

administration and to become a part of the team running the forum. This provided him with an unprecedented access to the raw data on the forum. Overall, the investigation took two years and the special agent on the case had to convince his superiors of the importance and relevance of this operation. Such an operation would unquestionably reap much better results that the techniques that were presented in this paper. It is doubtful however that such an investigation could be launched against many targets. The number of special agents to could go undercover in such forums is very limited and each time a new investigation is launched, each special agent would need to devote his full attention to the case, every single day, for months if not years. This would require major sacrifices on their part, something that not everyone is ready to accept. Furthermore, the details of the police investigation were published in Glenny's (2011) book in extensive details and provided criminals with a detailed portrait of how the FBI works. As many in the carding scene are aware of the demise of Darkmarket and Glenny's (2011) book, there is no way to find out if the technique used by the FBI in the past would still work today. Although the administrators of DarkMarket were very cautious, new generations of administrators will undoubtedly take even more precautions before they accept new members in their team as a consequence of this operation. The success of the DarketMarket operation was a surprise both to the law-enforcement agency and to the cybercriminals. The sheer importance of the resources that had to be invested to make this operation a success limits how often these can launched, even though they have proven their effectiveness without a doubt. Now that the entire criminal underground is divided into a very large number of forums and IRC chat rooms, it would be next to impossible for the FBI to use these techniques to investigate all of their members and this is where Sybil and slander attacks become much more cost-effective, although not as effective.

Just as their legitimate counterparts, participants in illegitimate markets pursue reputation in order to improve their success in a particular field. Many variables explaining how recognition is distributed in legitimate enterprises also apply to the criminal underworld. Papers focusing on the legitimate end of reputation have described in detail the role of networking and behaviour for example. These papers were important guides that led us to better understand the concept of reputation and the selection of variables that needed to be included in our predictive model. This paper is once again a reminder that other fields outside

of criminology have already generated knowledge that could and should be studied by criminologists who are looking for models to understand social behaviour such as recognition and market dynamics. We expect to find similar patterns in other literature such as that on criminal achievement. As forces outside the control of their participants primarily govern markets, the same concepts and principles should apply to both legitimate and illegitimate markets. This crossover between criminal and sociological research appears to be key to the pursuit of the understanding of criminals who are, as we often forget, simple human beings.

CHAPITRE 7 – WALKING THE LINE

Auteurs:
David Décary-Hétu
Yanick Charette

Publication :
À soumettre.

Abstract

Just as their legitimate counterparts, criminal entrepreneurs thrive to increase their performance in difficult environment. Past research has shown that factors such as mentoring, social capital, criminal organizations, experience and skill can impact their illegitimate revenues. This paper seeks to extend this body of research and to understand the role of another resource, reputation, as a correlate of success. Using Glückler & Armbrüster's (2003) concept of networked reputation, we build a survival analysis model with repeated measures to the impact of public, experienced-based and networked reputation on the performance of online offenders who specialize in financial and personal information fraud. Our results demonstrate that the offenders who develop strong reputation both in their close and extended social network enjoy a higher rate of illicit transactions than others. This increase in performance can be further improved by walking the line and breaking from time to time the rules of the markets.

Keywords

Reputation, social networks, criminal performance, edgework

Introduction

In settings where resources of wealth and status are scarce, strong competition between actors is likely to arise. To gain an edge over others, individuals must increase their access to business opportunities and make a better use of them than their counterparts. Such rivalry has recently become more important as traditional illicit markets have begun their transition from the physical world to the Internet. Researchers have highlighted the ever increasing size and importance of online criminal markets where offenders can buy and sell illegal goods and services (UK Card Association, 2012; DIBR, 2010).

In the case of illicit markets, the relative performance (or success) of offenders has been measured in three ways: a lower detection risk (Nguyen & Bouchard, 2011), higher illegitimate revenues (Morselli & Tremblay, 2004) or a higher number of transactions (Décary-Hétu & Leppänen, forthcoming). Independently of the measure used, the same set of variables appear in most of these studies: the presence of a mentor, social networking, skills and experience.

This paper builds upon this past research to improve our understanding of performance in criminal markets. To do so, we revisit the notion of criminal reputation. In the legitimate world, reputation has been cited numerous times as a prerequisite for success (Shapiro, 1983; Stickel, 1992; Yamagishi, 2002). Entities that invest early on in reputation building activities are more likely to succeed in the future and to generate more revenues. Reputation is therefore understood as a resource that increases performance. To broadcast information about one's public image, social networks are of the utmost importance. It is through social interactions that one receives the signs and signals necessary to the diffusion of reputation. To model the dissemination and impact of reputation, Glückler & Armbrüster (2003) have developed the concept of networked reputation which compares the effectiveness of public, experience-based and networked reputation in achieving higher levels of performance. The first type of reputation is measured by the public image of an entity. Experienced-based reputation, as its name implies, focuses on past personal experiences to evaluate the reputation of an entity. Finally, networked reputation is a combination of first-hand experiences as well as referrals by trusted third parties.

To extend our current understanding of performance in the context of illicit markets, this research aims to apply the concept of networked reputation to a criminal setting where offenders specialize in the theft and monetization of stolen financial data. The focus of this paper is on the notion of performance and two of its correlates, reputation and social capital. For this study, performance is measured by the rate of transactions of each offender. This rate varies through time and across individuals which is why we developed a survival analysis model with repeated measures which allows us to model the impact of reputation, social capital and control variables on each transaction. This dynamic model therefore precisely accounts for all the changes that may impact the time that is needed for an offender to reoffend.

The first section of this paper operationalizes the concept of reputation as a resource liable to be used to increase performance in the context of licit and illicit markets. The second section introduces the notion of social capital and its interaction effects with reputation and performance. The third section describes the theoretical framework of this study – Glückler & Armbrüster's (2003) concept of networked reputation. This theory specifies that reputation and social capital play an important role in the distribution of performance in a market and that the information circulated in social networks can help foster business opportunities. Our analyses confirm that Glückler & Armbrüster's findings can be applied in illicit markets. They also demonstrate that by bending the rules slightly and walking the line, some criminals are able to increase their rate of illegal transactions. In this context, we prove that performance is not distributed randomly among the offending population.

Reputation as a resource

Business opportunities are far from being randomly distributed among participants in any given market. Whether we consider legitimate or illicit markets, some actors always manage to outperform others by finding and taking advantage of opportunities. To understand the reasons behind this, some researchers have examined the notion of resources that have the potential to provide a sustain competitive advantage (Hayagreeva, 1994; Gaulthier-Gaillard & Pratlong, 2011). According to this approach originally developed for the business world, each entity can count on a different amount of resources. These resources are either tangible (buildings, employees, products) or intangible. To be considered as a resource, a feature of an

entity must exhibit four specific properties: value, imperfect imitability, nonsubstitutability, and rarity (Deephouse, 2000).

While a broad range of resources may impact the performance of entities, this paper will focus on a single item that has attracted the attention of researchers in both the licit and illicit worlds: reputation. Reputation can be defined as "what is generally said or believed about a person's or thing's character or standing" (Jøsang et al., 2007). Deephouse (2000) demonstrates why reputation should be considered a resource. First, it is valuable as it enables entities to obtain goods and services at a lower cost and to sell their own goods and services at a higher margin. As confidence is higher in entities with a good reputation, the uncertainty associated with any given transaction is reduced, thus allowing for maximal profit. Second, reputation is imperfectly imitable as it takes a long period of time for an entity to build up and spread a good reputation. Moreover, once lost, it takes even longer to repair a reputation (Hall, 1992). It is therefore very difficult to imitate a good reputation according to Deephouse (2000), who also mentions the fact that it is impossible to buy a reputation (Caves, 1980) or to fake its "complex and social nature" (Deephouse, 2000: p1099). Third, reputation should not be substitutable. Barney (1991) highlights the fact that entities will often seek to increase their reputation in various ways while offering guarantees and formal contracts for their products and services. As reputation is sought at the same time as these legal instruments are being offered, Barney (1991) claims that the latter are not a replacement for the former and that reputation should be considered nonsubstitutable. Lastly, reputation is rare as it is not distributed evenly among all participants in a market and as it cannot be summoned at will. As all entities are unable to have as much reputation as they would like, it is therefore rare.

Numerous studies have confirmed the value of a good reputation as a resource stimulating business opportunities (and inversely, the dangers of a bad reputation). This is particularly true of online auction sites such as eBay, Amazon and Yahoo! which all use an automated feedback system to collect data about the reputation of sellers and broadcast that information (Melnik & Alm, 2002; Lee, 1998; Lucking-Reiley et al., 2000). Such studies traditionally measure the final selling price, the number of bids and whether a product was sold or not on these platforms to identify the correlates of success for sellers. Although most factors such as the length of the auction, the quality of the product and the shipping options all

have a variable influence on the closing price of auctions, reputation is the only resource that is consistently mentioned as being positively correlated with higher returns. The most exhaustive study on the subject was done by Snijders & Zijdeman (2004). They developed the most complete model, which indicates that every 10 additional reputation points increase the price of a product by US$0.60, all else being equal.

Reputation can also be viewed as a resource with entities looking to launch initial public offerings (IPOs). Using a reputed and well-known accounting firm sends the signal that a firm is not afraid of scrutiny and that its books are in order (Beatty, 1989). Kotha et al. (2000) further demonstrate that the price of an IPO can be raised when investments are received from reputed venture capital firms, thus giving an aura of legitimacy to firms looking to make an IPO.

While studies on licit markets have been the main focus of researchers looking at reputation as a resource, a few studies have also applied this approach to the case of illegal markets. This is the case of some ethnographic studies on offenders. Anderson's (2000) book on the code of the streets as well as Topalli's et al. (2002) study of drug dealers in St. Louis are consistent with prior research in establishing that a reputation for violence reduces the likelihood of victimization among offenders and therefore increases the performance of actors. The same effect can be seen in Sauvadet's (2006) study of the interaction process of young people from poor areas. He observes that certain forms of assets arouse deference, what he calls the warrior capital. This capital not only consists in the ability to fight, but also in the capacity to argue with others and manage relationships. The accumulation of this capital sends signals of success to others, thus increasing esteem and respect.

The cyber criminology literature has also contributed to corroborating the view of reputation as a resource enhancing performance in illicit markets. Reputed and high-status actors of online illicit markets receive more messages when they offer goods and services online (Motoyama et al., 2011). They are also more credible when they ask for other members to be blamed by the market administrators, giving them a chance to use deterrence and eliminate their competition. The power that comes with a high level of reputation reduces the odds that an actor will act opportunistically with others as this would reduce their reputation

(Mell, 2012). Actors must first invest in their reputation by selling their goods and services at a discount in order to build up their reputation. Once they have established themselves, offenders can create long-term partnerships and charge a premium for their products. The power of reputation is also highlighted in Monsma's et al. (2010) study which explains the attraction of actors with high levels of reputation, which ensure continued access to more opportunities.

Although most illicit markets are left unsupervised, some criminals have found that it was in their best interest to relinquish some of their liberty in exchange for protection. This is the case of some carders, i.e. the individuals who steal and monetize financial data stolen online. These offenders use traditional methods (card skimmers on automated banking machines, complacent employees in restaurants) as well as hacking techniques to steal credit card numbers which can be sold online to other offenders or used to purchase goods illegally. Using a computer simulation, Mell (2012) shows that market administrators who efficiently rank the reputation of participants increase the fluidity of markets and reduce the risks of participants being scammed. Under this supervision, criminals can interact more safely as the recognition index gives them precious information on possible business partners.

Social capital, reputation and performance

Reputation is an important resource for any entity looking to enhance its opportunities and therefore its performance. To maximize the impact of reputation, it is essential that as many people as possible be made aware of other people's reputation. This is where Bourdieu's (1972) concept of social capital comes into play. According to him and others who followed his lead (Coleman, 1988; Granovetter, 1973; Putnam, 1993), social agents build personal networks of contacts to enhance their success. Similar processes have also been observed in the criminal underworld (Morselli & Tremblay, 2004). This strategy allows them to increase the level of trust between them and others (Lai & Siu, 2006). It also enables them to gather information on possible partners by contacting mutual acquaintances (Tremblay, 1993). Using social networks, it is possible to spread information about a person's reputation. Brokers, who often control the flow of information in criminal networks, are particularly good at this and they have been identified in the past as the most active and powerful members of these networks (Morselli, 2009). Without a good network of friends, reputation is rendered useless.

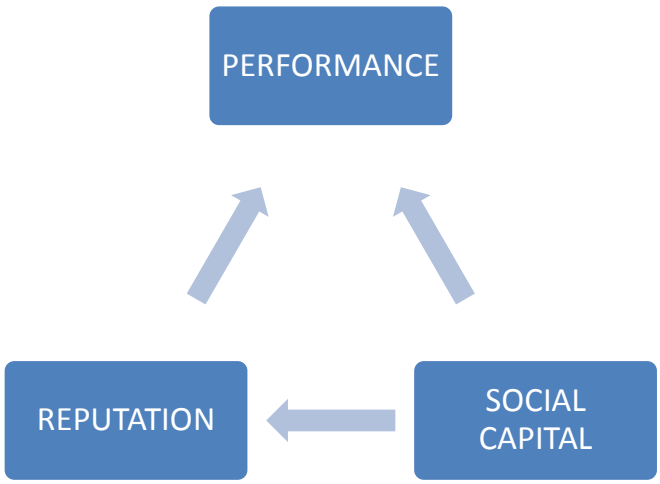
In the context of the Internet, the importance of social capital is somewhat reduced by the automated feedback systems which collect and broadcast information on the reputation of all actors. This provides offenders with a public image of each person but the quality of that information may be somewhat unreliable as its origin is often unknown (Glückler & Armbrüster, 2003). Social capital is therefore needed to spread quality information about individuals from business partner to business partner. Automated systems are a poor man's alternative for those not lucky enough to be able to count on an extended network of contacts.

In addition to extending the value of reputation, social capital is in and of itself another resource that can be used to increase business opportunities. According to Nguyen and Bouchard (2011), a larger number of contacts increases the chances of finding suppliers and buyers and can thus increase one's illegitimate revenues. The quality of contacts is also important as was demonstrated by Morselli et al. (2006). In their study, they highlight the role of mentors in the development of offenders. Having such a tutor helps one learn the tricks of the trade as well as bridge over to new social networks. The structure of each person's personal network is also very important as non-redundant contacts provide criminals with brokerage opportunities to bridge the structural holes between market actors (Morselli et al., 2006; Morselli & Tremblay, 2004). By playing the middleman between two offenders, an individual ensures that others will always need them and raises their value in a criminal market. This was the case of Mr. Nice, an international drug dealer who saw his power in the drug trade diminish when his business partners began to contact each other directly instead of going through him (Morselli, 2001).

Networked reputation as a ladder to success

As we have seen so far, reputation and social capital can both be considered as resources which have an impact on business opportunities and performance. There is also an interaction effect between reputation and social capital, whereby social capital can help heighten the impact of reputation on performance. Figure 1 summarizes these findings.

Figure 1: Diagram of the relation between performance, reputation and social capital



Glückler & Armbrüster (2003) have developed a model which presents this interaction between performance, reputation and social capital in a context that is surprisingly very similar to criminal markets, the consulting market. Similarly to criminal markets, the consulting industry has a very low barrier to entry, as anyone can set up a business and offer their services. In both cases, market insecurity arises from the impossibility of determining the quality of a service (or good) that is up for sale beforehand. Past contracts of consulting firms are usually confidential and protected by non-disclosure agreements. Clients looking to hire a consulting firm thus have very little information to work with in order to evaluate potential service providers. The same can be said of criminals, who often do not have any information on their partners in crime or the products they sell. Glückler & Armbrüster (2003) mention that uncertainty in the consulting market is also heightened by the fact that no institution or professional order regulates the work of consultants. In this very competitive setting, new actors are constantly appearing and the expected life span of consulting firms is fairly limited. The same dynamics also apply to some criminal settings (Reuter, 1983; Décary-Hétu et al., 2012).

In the market of consulting firms, prospective clients must take on multiple risks. They take a performance risk as they are unable to ascertain the level of service they will receive beforehand. They must also take a relational risk as the consulting firm may use the

information disclosed under one contract in subsequent contracts. If two firms competing with each other hire the same consulting firm successively, consultants may be tempted to use information from the first company to better their performance with the second company. While moral codes do exist, it is impossible to make sure they are enforced. Clients, in this case, have to take high levels of risk when dealing with consultants. The same holds true for many criminal markets. It is, for example, very difficult to evaluate the quality of a protection service beforehand as is evaluating the effectiveness of a bribe. Offenders may lead their clients to believe that they were instrumental in the granting of a work permit when all they did was submit the paperwork and wait for the administration to do its work. Furthermore, offenders must always be careful with the information they share as it may be used against them in court or in later dealings (Reuter, 1983).

To reduce risks and uncertainty, Glückler & Armbrüster (2003) suggest that clients should focus on the reputation of consulting firms. There are three types of reputation: public reputation, experienced-based reputation and networked reputation. Public reputation is the general perception the community has of the performance of a consulting firm. It paints an overall picture of all the active firms in a market but the information provided is of poor quality and from unknown sources. As for experienced-based reputation, it is solely based on previous transactions between a client and the consulting firms it has worked with in the past. Clients may, in some cases, decide to look for a firm to hire among the pool of past consultants. Such a behavior implies that clients base their decision on their impression (e.g. reputation) of the past performance of consulting firms they have worked with. In this case, the information used to make a decision is of high quality as it is based on first-hand knowledge. It is however highly limited as clients restrict themselves to firms they have worked with in the past. These known firms may not be the most efficient at solving the new problems they might be facing. Glückler & Armbrüster's (2003) position is that both propositions are suboptimal and that clients should adopt a third strategy based on networked reputation.

In this scenario, clients contact friends and business relations and investigate the first-hand reputation of consulting firms in the circle of their social network. This allows the client to build a reputation profile of all the firms they have worked with in the past and of all the

firms their contacts have worked with in the past. This provides high-quality information on more consulting firms, thus enabling the client to make more efficient decisions. Glückler & Armbrüster (2003) believe that using public reputation is better than not using reputation at all. Experienced-based reputation is more reliable but limits the number of possible firms to work with. Networked-based reputation provides the best balance between risks and return on investment.

This theoretical framework perfectly explains the dynamic relationship between performance, reputation and social capital. According to Glückler & Armbrüster (2003), consulting firms that manage to take advantage of networked reputation achieve the best performance in their industry. Given the similarities between the consulting market and many illicit markets, this paper will apply Glückler & Armbrüster's (2003) framework to a criminal setting, the carding scene (explained in further detail below). As our understanding of how reputation affects performance in the illicit world is still very limited, this study will make it possible to better understand the role and impact of reputation and social capital on performance.

According to Glückler & Armbrüster (2003), the three types of reputation should differentially affect the probability of making a transaction in the future. Having a good public reputation should yield better results than having a bad public reputation. These effects should however be more limited than those found with experienced-based reputation and networked-based reputation.

Methods

Data

The data for this paper comes from an online marketplace where offenders, known as carders, meet to buy and sell stolen financial data. In this community, criminals mostly specialize into one of two crafts: the theft of financial data or the monetization of financial data. The former consists in acquiring data through online and offline methods including credit card skimmers that copy the magnetic stripe of credit cards, computer viruses and social engineering to trick people into providing their own information in online forms. The latter

involves turning this information into cash by printing fake credit cards, finding mules willing to receive wire transfers and making illegitimate purchases online.

Over the past two decades, the Internet has vastly extended criminal opportunities by facilitating the interactions between these two groups of offenders. Ordinary online forum software which is often used to host discussions about sports or movies has been adapted as criminal marketplaces where criminals can meet anonymously and secretly. Such platforms allow users to post both public and private messages and learn more about one another by looking at personal profiles. Transactions usually begin when a member posts publicly a message containing a detailed description of what they have to offer or what they are looking for. Others can then contact them through a private message on the forum or an external instant messaging system to negotiate a deal.

Each platform has its own administrators who are tasked with elaborating rules of conduct and enforcing them. Several marketplaces have historically competed for a larger share of online illegal trades. Administrators usually take a percentage of all sales by offering a validation and/or escrow service for which they charge their members. Marketplaces with more transactions therefore have the potential to generate higher profits for their administrators. To cripple their competition, marketplace administrators have sought to hack one another's platforms to steal confidential data and publicly humiliate other administrators. In a few instances, such attacks have been successful and led to the online distribution of entire copies of online forums. These images contained all private and public messages as well as all member profiles. Some of the above-mentioned research (Monsma et al., 2002) has taken advantage of these databases to better understand these criminal markets; a similar approach will be adopted in this paper.

We downloaded a copy of an entire online forum which was active between 2007 and 2009. This dataset includes all public and private messages as well as all the member profiles. The initial population of 18,834 profiles published 858,744 public messages and 501,913 private messages. Many changes occurred during the three years of activity of the forum. One of them was the introduction of a public reputation measure. This recognition scale allowed members to rate each other's reliability in the same way that eBay buyers can rate the sellers

of goods. As this paper focuses on the link between reputation and performance, we restricted our sample to a window of 85 days from August 25th, 2009 to November 18th, 2009, the period when the reputation measure was active.

Past research on criminal performance has in the past used illegal revenues and/or the risks of arrests to evaluate the relative performance of offenders (Morselli et al., 2006). Our dataset did not contain unfortunately an evaluation of each participant's revenues nor were there any indication that anyone was arrested because of their dealings in the forum. To circumvent this problem, we decided to look at the transactions each member conducted rather than the amount of money made through illicit transactions. The detection of such transactions was automated by analyzing private messages to identify those containing a number preceded or followed by either "$", "dollar", "dolar", "€" or "euro" (ex: "$14" or "14 dollar" or "30€"). This enabled us to quickly identify messages that led to a transaction as members used private messages to negotiate the price of stolen financial data. Even if we cannot know for sure whether this transaction actually occurred, this could be considered as a good proxy measure of the existence of a transaction. Among the total population of our observation period, 1,773 members either sent or received a private message which contained an amount in euros or dollars. As all other members were not directly involved in illegal trades on the forum (n=14,841), they were removed from the sample. If two individuals exchanged more than one message containing an amount of money within 48 hours, all but one message were removed so as not to artificially inflate the number of transactions between individuals. These messages were mostly bargaining exchanges in which users bargained for the best possible price and sent counter-offers to each other. The transactions we identified were not directional, meaning that we did not know who was selling and who was buying the stolen financial data. All that was known was that the individual was involved in an illegal trade.

Measure

More than the occurrence or frequency of transactions, the time (number of days) between each transaction is a more precise measure of carders' criminal performance and will be the dependent variable of our model. It is not only the fact that one or several transactions were made that measures efficiency but, above all, the time between each transaction. This

ability to quickly find criminal opportunities best represents criminal performance as it demonstrates one's access to the ressources necessary to offending. During our window period, 3,409 transactions occurred on the forum; they were made by 1,773 members, with an average of 1.92 transactions per individual (SD = 2.04). Of those transactions, 50.3% (n = 1716) were followed by another one in the future, 50.3 days later (SD = 102.09; n = 1716) on average.

To explain the time elapsed between two transactions, we created a number of independent variables. As we have seen earlier, the levels of reputation mentioned by Glückler & Armbrüster (2003) have a major impact on the success of transactions. All three types of reputation were therefore included in the model as independent variables. Public reputation was operationalized using the recognition scale introduced by the administrators of the carding forum. In this system, each participant could award other members reputation points for things they had done on the forum. This scale was only positive, meaning that users could only give points to others and not take them away. This metric provided us with a good idea of the public profile of each individual. The average accumulated public reputation was 1.57 points (SD = 6.59; n=3,409) at the time of transaction. Experienced-based reputation was measured by looking at whether two members making a transaction had been involved in a deal before. In 10.3% (n=352) of transactions, the two individuals had been involved in a transaction with each other in the past. This metric was dichotomous meaning that for each transaction, a 1 meant that the two partners had dealt together in the past. Lastly, networked reputation refers to friends of friends who had a previous transaction with the other participant in the transaction. On the forum, members could ask others to become their cyber-friend just as one would do on Facebook. Using this list of friendships, networked reputation indicates whether the two members involved in the transaction had a friend in common who had already made a transaction with the other participant in the transaction. In the case where individuals had dealt together in the past and also had a friend in common, we only kept the strongest bond between the two which is the direct connection. In 8.3% (n=283) of transactions, the other participant had already dealt with a common friend. This metric was dichotomous meaning that for each transaction, a 1 meant that the two partners had a friend in common who had dealt with them in the past.

While administrators did not play a role in the evaluation of reputation, they did impact reputation by issuing warnings and bans on the forum. Members could report to these regulators the behavior of participants who had broken the platform rules. After reviewing the complaint, administrators could issue a warning to a member telling them that a particular behavior was not acceptable. If a member accumulated too many warnings, they could then be banned from the forum. The number of warnings accumulated between each transaction was measured for each member. At the time of each transaction, individuals had accumulated 1.2 warnings (SD=2.1) on average. Furthermore, 318 (9.3%) transactions involved an individual who was eventually banned from the forum.

The behavior of each member was also measured by the number of prior transactions and the number of discussions they had started. Measuring the number of discussions launched by each individual provides an estimate of their involvement in the world of carding. Such discussions are generally started by someone who is looking to buy or sell an illegal good or service. We also controlled for the number of days since the creation of the forum (M=891.91; SD=26.63). As we moved forward in time, the chance that a transaction would take place in the future was reduced because of the limited time frame ahead.

Lastly, social network analyses were used to better understand the activities of participants and how these fit into the whole network of interactions. The social network metrics selected were based on all the private messages exchanged between members. Their evolution in time was measured during the accumulation period. Three measures were used to describe the structure of the network: degree centrality, betweenness centrality and ego network constraint. The centrality of degree represents the number of contacts of each participant. The pattern of ties originating from or sent to a network member is usually a reliable indicator of this person's prestige or status as it helps to recognize people with sought-after expertise (Wasserman & Faust, 1994). Individuals at the time of their transaction had an average degree centrality of 134.2 (SD=287.50). This implies a fairly large number of past contacts and highlights the extent of the degree of social interactions between the participants. Degree centrality has been criticized for underestimating the value of actors who have fewer direct ties but are nevertheless influential because of their ability to harness these ties more strategically in order to unite network members (Moxley & Moxley, 1974; Freeman, 1977).

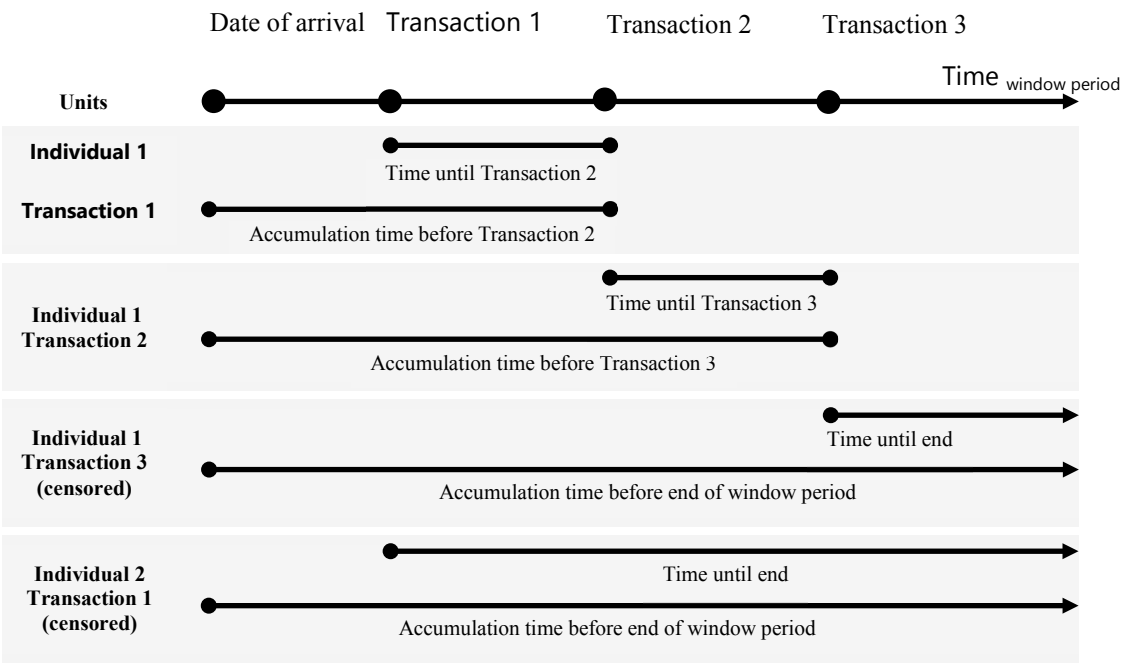
To address this concern, we also used the betweenness centrality metric which measures the extent to which a node is located on the shortest path between other disconnected nodes within the network. The more often a node is located between other actors, the higher its betweenness centrality, making it a broker within the network. The position of broker has been associated with the notion of power in networks, since these individuals control the flow of information between the different actors (Morselli, 2009; Prell et al., 2008; Toral et al., 2009). Both betweenness and degree centrality take into account the network as a whole rather than the smaller circle of ties around each actor. Burt (1992) has shown that these local networks, known as ego networks, are also very important to understand the structure of a network. Ego network constraint evaluates the extent to which the ties of an actor know each other. If all their ties are connected, the actor's importance is reduced as they are no longer needed for transactions to occur between their ties. This feature of networks was also reported by Morselli (2001), who studied the evolution of the personal network of a drug dealer, Mr. Nice, finding that the importance of this dealer was considerably reduced as he became redundant in his own network. The average ego network constraint at the time of transactions was 0.21 (SD=0.30). This indicates that the personal networks of actors were mostly unconstrained, increasing their power and leeway.

The goal of this paper is to better understand the role and impact of reputation and social capital on performance. Once again, according to Glückler & Armbrüster (2003), the three types of reputation should differentially affect the probability of making a transaction in the future. Having a good public reputation should yield better results than having a bad public reputation. These effects should however be more limited than those found with experienced-based reputation and networked-based reputation. We will begin our results section with six survival curves which were generated with the Kaplan-Meier estimator (1958) and compared using the Mante-Cox log rank method (Mantel, 1966) with pooled overall comparison. This will enable us to understand how much time it takes the different categories of carders (with/without public reputation, with/without experience-based reputation and with/without networked reputation) to transact again. Each group will be compared with each other.

Following these survival curves, we will present a multivariate recurrent event survival analysis predicting the probability that a subsequent transaction will occur during the next day

in a carding community. This model uses the number of days between two transactions as a dependent variable and was performed using a Cox proportional hazard model with robust estimation (Anderson & Gill, 1982; Therneau & Grambsch, 2000). This model estimates the likelihood of an event occurring in the future, modeling for right censored data that adjusts the variance estimator for correlation within subjects for recurrent events.

Figure 2: Diagram of the operationalization of the sample and concepts



As show in Figure 2, our model first measures all of the independent variables at the time of the first transaction as well as the time it took to happen since the arrival of the participant on the forum. The independent variables are used to explain the probability that a transaction will occur during the next day. At the time of the second transaction, a measure is taken of all independent variables since the arrival of the member on the forum. These updated values are used to explain the probability that a second transaction will happen. This process is repeated for all subsequent transactions.

Our results section will end with a third and last analysis which focuses on the carders themselves and not the transactions. For this purpose, the data was aggregated at the individual

level to give a wider perspective to results in terms of individual performance (N=1,773). Our goal was to understand the different strategies that carders could use to maximize their performance. To do so, carders were classified into 4 categories: (1) individuals who had no strategy at all (n=806; 45.5%), (2) individuals who had at least one reputation point during their life span but no warnings (n=228; 12.9%), (3) individuals who had at least one warning but no reputation points (n=503; 28.4%) and (4) individuals who had at least one warning and one reputation point (n=236; 13.3%). We compared each of these categories in regards to their total number of transactions per individual (M=1.92; SD=2.04), the number of days they remained active on the forum (M=6.85 months; SE=4.54) and their productivity measured in the number of transactions per month (+=0.55; SD=0.97). It may seem as counterintuitive to investigate whether receiving warnings may be beneficial to offenders. In this case, however, members received warnings when they behaved too aggressively. This type of behaviour may have increased their sales on the short term while hurting their chance of conducting business on the long term. These analyses will enable us to better understand the short and long term effects of warnings on performance.

Standardized coefficients (β) were calculated using Z score transformed variables. Since the assumption of homogeneity of variance was violated (Levene's $p<0.05$), non-parametric ranking procedures were preferred (Kruskal & Wallis, 1952) for the comparison between categories for continuous variables. Multiple comparison tests were also carried out using Dunn's (1964) procedure on ranks with the Bonferroni correction. All analyses were performed using R 2.14.2 (R Core Team, 2012) and survival package 2.36-14 (Therneau, 2012).

Results

Glückler & Armbrüster's (2003) position is that reputation, whether public, experienced-based or networked, influences the performance of businesses in the legitimate world. Figure 3 shows survival curves for the time until a subsequent transaction occurs for each of the different types of reputation. Time until the next transaction is shorter for members who have at least one point of public reputation (solid grey line; Mdn=38.0; SE=7.22) than for those who have no reputation points (grey dotted line; Mdn=221.0; SE=22.94; Mandel-Cox $Chi^2(1)=67.16$; $p<0.001$). Fifteen days after a transaction, 38.0% of those who had at least one

public reputation point had made another transaction, while only 25.8% of those with no points had another transaction at that time. This is a first indication that public reputation does play a role in the selection of business partners and that participants in this community should strive to increase their own public reputation.

Figure 3: Survival curves of time until the next transaction

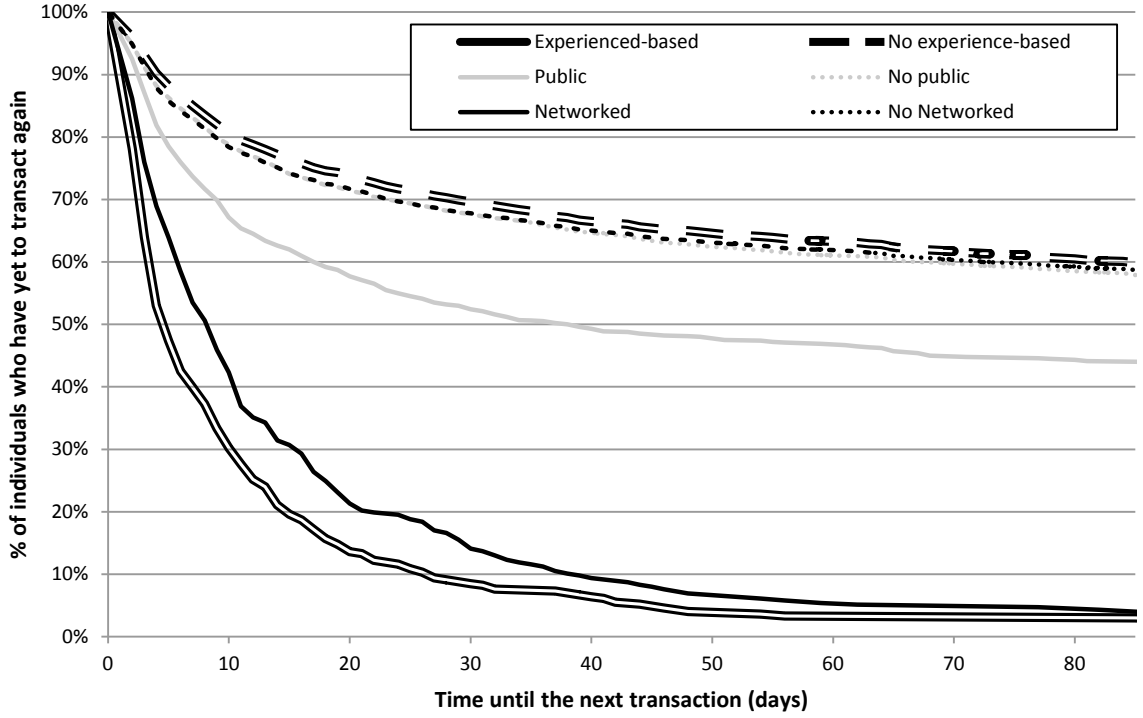


Figure 3 also presents the time until a subsequent transaction for individuals who have dealt with each other in the past (double line; Mdn = 5.0; SE=0.37) and those who have not (double dotted line; Mdn = 278.0; SE = 20.07). Fifteen days after a transaction, 80.4% of those who had already made a transaction with the other member involved had made another transaction, while only 23.5% of those who did not have this history had made another transaction at that time. This impact of experienced-based reputation showcases even more prominently the effect of reputation on criminal performance. As such, two individuals who have dealt together in the past will likely make a transaction again much sooner in the future (Mandel-Cox $Chi^2(1)=1059.71$; $p<0.001$).

The same effect also applies to networked reputation. The black solid line represents the number of days until the next transaction when the members involved have a friend in common who was involved in a transaction with one of them in the past. For this group, the median time lapse until the next transaction is 9.0 days (SE=0.73). The black dotted line represents the number of days for those who did not have a friend in common, with a median period of 251.0 days (SE=20.06). Fifteen days after a transaction, 69.3% of those who had already made a transaction with a common friend had made another transaction, while only 25.8% of those who did not have this type of indirect relationship had made another transaction at this time. Once again, the time elapsed before another transaction is much shorter when friends of friends are involved in a deal (Mandel-Cox $Chi^2(1)=606.69$; $p<0.001$).

There is a significant difference between the three reputation types as regards the time before a new transaction occurs (Mandel-Cox $Chi^2(2)=470.52$; $p<0.001$). The most efficient type of reputation to reduce the time between transactions is experienced-based reputation. This reputation type is significantly more effective than public reputation (Mandel-Cox $Chi^2(1)=367.45$; $p<0.001$) or network reputation (Mandel-Cox $Chi^2(1)=11.28$; $p=0.001$). Using recommendations from friends to select business partners is the second-best reputation type and is more effective than public reputation (Mandel-Cox $Chi^2(1)=226.01$; $p<0.001$). Lastly, public reputation does provide an improvement over no reputation at all, but that enhancement is much less effective in increasing the rate of transactions. Since these observations are not independent (some transactions could involve individuals who possessed public, experienced-based and networked reputation at the same time) and since other variables must be taken into consideration, those results must be interpreted with caution and a multivariate analysis is now proposed.

Table 1: Multivariate recurrent event survival analysis predicting time before a subsequent transaction occurs in a carding community

Reputation model					
	B	exp(B)	Robust SE	β	p
Public reputation	0.01	1.01	0.00	2.82	0.005
Networked reputation	1.00	2.72	0.08	13.14	0.000
Experienced-based reputation	1.56	4.74	0.07	23.61	0.000
Likelihood ratio test=795 on 3 df, p=0 n= 3409, number of events= 1716					
Full model					
	B	exp(B)	Robust SE	β	p
Public reputation	0.02	1.02	0.00	0.11	0.000
Networked reputation	0.31	1.36	0.08	0.09	0.000
Experienced-based reputation	0.72	2.05	0.07	0.22	0.000
Years elapsed since forum started	-4.38	0.01	0.37	-0.32	0.000
Nb of previous transactions (/100)	0.19	1.20	0.07	0.17	0.011
Nb of discussions initiated (/100)	-0.02	0.98	0.07	-0.01	0.750
Nb of warning received	0.03	1.03	0.01	0.06	0.009
Banned from the forum	0.17	1.18	0.08	0.05	0.044
Ego network constraint	-6.87	0.00	0.84	-2.03	0.000
Degree centrality (/100)	0.13	1.14	0.02	0.38	0.000
Betweenness centrality (/1,000,000)	-0.60	0.55	0.00	-0.36	0.000
Likelihood ratio test=2500 on 11 df, p=0 n= 3404, number of events= 1711 (5 observations deleted due to missing values)					

Table 1 shows a multivariate recurrent event survival analysis, performed using a Cox proportional hazard model with robust estimation explaining the likelihood of another transaction taking place in the future. The first model only includes the different types of reputation as predictors. In this model, experienced-based reputation increases the rate of

transactions the most (β=23.61; p<0.001), followed by networked reputation (β=13.14; p<0.001) and public reputation (β=2.82; p=0.005).

The second survival analysis model offers a slightly different interpretation of the impact of reputation on criminal performance. Experienced-based reputation has once again the strongest effect of all reputations on criminal performance (β = 0.22; p < 0.001). Its impact is more important than that of public reputation (β = 0.11; p < 0.001). The presence of a past transaction with the other party involved increases the chance of a future transaction occurring by 2.05 times (Exp(B)=2.05). Interestingly, in the multivariate model, networked reputation has a smaller impact on success in the criminal world (β = 0.09 p < 0.001) than public and experienced-based reputation. This difference with the first model can be explained by the fact that networked reputation shares some common variance with the network measures: ego network constraint (r=-.19; p<0.001), degree centrality (r=.29; p<0.001) and betweenness centrality (r=.12; p<0.001). When those measures are included in the model, they make it possible to better explain the probability of a future transaction.

All three social network measures (degree centrality, betweenness centrality and ego network constraint) have a significant influence on the time elapsed before a future transaction, although they are not always positively correlated with criminal success. These factors of the models have the most explanatory power (respectively β=0.38; β=-0.36; β=-2.03). The number of contacts increases criminal success as it provides access to more criminal opportunities (B=0.13; SE=0.00; p < 0.001). An increase of 100 contacts in the direct network improves by a factor of 1.14 the probability of making a transaction in the future (Exp(B)=1.14). Betweenness, on the contrary, reduces the success of offenders in this criminal setting (B=-0.60; SE=0.00; p < 0.001). This is surprising as past research has found that brokers, the individuals with high levels of betweenness, usually outperformed others in criminal networks (Morselli, 2009). The fact that this platform exists in a virtual context, the Internet, may have played a role in this result. Lastly, constraint is negatively correlated with criminal performance (B=-6.87; SE=0.84; p < 0.001). This is consistent with previous research (Morselli, 2001) which stated that being redundant in a network reduced performance. In this case, the members with lower constraint are indispensable as the people around them need them to contact one another.

The number of past transactions is a good indicator of transactions to come as it significantly increases the probability of a future transaction taking place (B = 0.19; SE=0.07; p=0.011). A hundred more transactions in the past increases by 1.20 times the probability of making a transaction in the future (Exp(B) = 1.20). The number of discussions previously started has no influence on future transactions (B=-0.02; SE=0.07; p = 0.750).

The model shows that the number of warnings is positively correlated with performance (B=0.03; SE=0.01; p = 0.009). This is counterintuitive as one would not expect that receiving a disciplinary action would increase the success of carders. Each warning increases by 1.03 times the probability of making a future transaction (Exp(B)=1.03). Even members who were eventually banned performed better than the others (B=0.17; SE=0.08; p = 0.044). This came as a surprise but further analysis of these results will help to understand how actors who misbehaved on the platform managed to increase their rate of transactions.

The survival analysis predictive models presented so far used transactions as the unit of analysis. As specified in the Methodology section, we also ran a third set of analysis at the individual level to gain a better understanding of the career of carders during the observation period according to length of life span on the forum, level of activity and efficiency. Carders were classified into 4 categories: (1) individuals who had no strategy at all (n=806; 45.5%), (2) individuals who had at least one reputation point during their life span but no warnings (n=228; 12.9%), (3) individuals who had at least one warning but no reputation points (n=503; 28.4%) and (4) individuals who had at least one warning and one reputation point (n=236; 13.3%). Each of these categories were compared to each other.

Table 2 presents the results of a one-way analysis of variance by ranks between the strategies used and the number of transactions during the window period, the duration of the activity and the number of transactions per month. The data shows that members who built up a reputation but who also, from time to time, used unethical techniques for which they were warned, managed to outperform others in the market (Kruskal-Wallis $\chi^2(3)=232.13$, $p < 0.001$). Post-hoc tests show that breaking the rules of the forum provides an advantage but only when one's reputation can offset past abuses. Having reputation points and warnings at the same time is more correlated with the number of transactions (M=3.21; SD=2.97) than

having no strategy at all (Q=-13.96; p<0.001), reputation alone (Q=-4.34; p<0.001) or warnings (Q=-7.33; p<0.001) alone. Members who only have reputation (M=2.27; SD=2.14) or warnings (M=2.06; SD=2.07) both perform similarly (Q=2.194; p<0.001) and they fare better than those with no strategy at all (respectively Q=-8.395; p<0.001 and Q=-8.001; p<0.001). At the bottom of the food chain, the members with neither warnings nor reputation have a much lower number of transactions than the other groups (M=1.36; SD=1.34).

Table 2: Impact of warnings and reputation on the number of transactions, the life span and the rate of transactions per month

			Number of transactions		Number of months active		Number of transactions per month	
Strategy preferred	n	%	M	SD	M	SD	M	SD
No strategy	806	45.5	1.36	1.34	7.86	4.80	0.40	1.02
Reputation only	228	12.9	2.27	2.14	7.96	5.33	0.54	0.86
Warnings only	503	28.4	2.06	2.07	5.17	3.40	0.65	0.89
Both strategies	236	13.3	3.21	2.97	5.67	3.53	0.85	1.01
Total	1773	100	1.92	2.04	6.82	4.54	0.55	0.97
Kruskal-Wallis Test			$X^2 = 232.13$; df = 3; p < 0.001		$X^2 = 220.87$; df = 3; p < 0.001		$X^2 = 140.91$; df = 3; p < 0.001	

The strategy chosen also is correlated with the length of profile life spans (Kruskal-Wallis $\chi^2(3)=220.87$, $p < 0.001$). While warnings may be beneficial in the short term, they are in no way useful in the long term. Users who have warnings statistically survive for a shorter period on average (M=5.17; SD=3.40) than those who do not, whether or not they have reputation points (with reputation points: M=7.96; SD=5.33; Q=9.21; p<0.001; no reputation points: M=7.86; SD=4.80; Q=10.84; p<0.001). Even members who have both reputation and warnings (M=5.67; SD=3.53) have an expected life span that is shorter than those with neither reputation nor warnings (Q=6.58; p<0.001) or only reputation (Q=4.80; p=0.001). This indicates that members who wish to establish themselves in the trade of stolen financial data

should be careful about what they do on the forum and should abide by the rules of the marketplace. Otherwise, their career may very well end prematurely.

Lastly, we see a statistical difference in the number of transactions per month according to the types of strategy (Kruskal-Wallis $\chi^2(3)=140.91$, $p < 0.001$). The rate of transactions appears to be highest among members who have warnings alone (M=0.65; SD=0.89) or both warnings and reputation (M=0.85; SD=1.01). Both fare better than members with reputation alone (M=0.54; SD=0.86; respectively Q=-4.26; p<0.001; Q=-5.78; p<0.001) or no strategy at all (M=0.40; SD=1.02; respectively Q=-12.03; p<0.001; Q=-11.89; p<0.001). Once again, this stresses the importance of spamming others (a common cause of warnings) as a marketing tool. Members with reputation are not trailing far behind with an average of 0.54 transactions (SD=0.86) compared to 0.65 (SD=0.89) for members with warnings and 0.85 (SD=1.01) for members with both reputation and warnings. Having only reputation is still better than having no strategy at all (Q=-4.58; p<0.001). The difference here is marginal especially when one compares this metric with the expected life span of members. Although they may be involved in transactions at a slightly lower rate than those with warnings, they stand to earn much more over the long run as their life span is longer by at least two months. In the carding scene, the best strategy to improve criminal performance over extended periods of time appears to be a good reputation. It may be possible to boost one's results by using illegal techniques from time to time but these events should be few and far in between.

Discussion

This paper supports the findings of Glückler & Armbrüster (2003) that reputation can be used to increase performance in a competitive market. Reputation itself can be divided into three categories: public, experienced-based and networked. The most effective strategy for carders is to focus on experienced-based reputation. Public reputation yields lower returns than experienced-based reputation but it is more effective than networked reputation. On this point, our results differ from those of Glückler & Armbrüster (2003) as networked reputation was not the best strategy to enhance performance. Three reasons can explain this difference. First, the predictive model included social networking metrics which may have lowered the importance of networked reputation. In the first model, networked reputation yielded better returns but this effect was countered by the inclusion of degree centrality, betweenness

centrality and ego network constraint in the second model. This highlights the importance of the structure of criminal networks for criminal performance. Second, the operationalization of friendship ties was far from perfect. Indeed, we limited these ties to official friendships on the forum, excluding all other types of friendship. This reduced the importance of these relationships in our analysis and the result was a lower impact for networked reputation. Future research should seek to build better representations of friendship ties to measure networked reputation more accurately.

Lastly, the context of the Internet may have played a role in the differences between Glückler & Armbrüster's (2003) model and ours. The quality of ties online has been questioned in the past (Boase & Wellman, 2006) and it appears that people may not have the same level of trust in their online friends compared to their real life friends. Businessmen may be willing to seek the advice of partners and friends and to act based on that feedback. Carders however may be more hesitant to heed other people's advice as they evolve in a setting that is ripe with uncertainty and risks. This undoubtedly affected the quality of ties and the strength of networked reputation as a predictor of criminal performance. Moreover, carders appeared to put more trust in the collective mind of the market rather than in their own personal ties. Direct ties as measured by degree centrality provided increased benefits whereas indirect ties (betweenness centrality) actually decreased the performance of carders. Public reputation, a representation of the image of a carder by the entire market, was more important than networked reputation based on personal contacts. As trust is low in these dark networks, it is very possible that an opinion spread by many individuals appears to be more trustworthy that the opinion of a single person. This has deep implications as disruption efforts will need to modify the public image of members of the market, a feat that now appears as very challenging.

This research is also ground-breaking for social network scientists who have always looked at brokers as the most successful entrepreneurs in criminal networks. What we have found is that in the context of the Internet, information is much more accessible and public than in the real world. This considerably reduces the amount of control anyone can have over particular pieces of information, from which brokers traditionally derive their power. Even large nation-states such as the United States were unable to prevent the leaking of hundreds of

thousands of diplomatic cables by an Internet activist website a few years ago. Furthermore, contacting other members of an online community is considerably easier than in the real world as well. All members can be reached through public and private messages and each person can be evaluated through their online profile. This also contributes to limit the power of brokers. This indicates that the structure and distribution of power in a virtual criminal community is very different than in a more traditional setting. Here, direct contacts are more important than indirect contacts. What was true for reputation is also true for networking. This implies that participants and law-enforcement agencies should shift their focus from brokers to the more active individuals who regularly engage with a large range of contacts directly. On a more local level however, not much has changed since Burt's (1992) paper on structural holes. Strategic positioning is still essential in order to become successful and participants should strive to remain non-redundant in their own network of contacts. Once friends of friends know each other, there is no need to keep in contact with the original friend and this person therefore loses some of their power. Those who excel at creating firewalls between their contacts will have a much better handle on their future and therefore access to much more criminal opportunities.

Above all, these results highlight the need to understand and study the concept of reputation in criminal markets. This reputation is not a one-dimensional object and needs to be broken down into its different components to be understood. If reputation is able to increase the rate of transactions, it is largely because it reduces the inherent risks and uncertainty of criminal markets. This provides another example of offenders' capacity of adaptation. The carding market presented in this paper showcases their ability to create a new online marketplace where the risks of detection are lower. The side effect of this move to the Internet is the rise in uncertainty but this was countered by the adoption of appropriate tools such as a recognition scale. Offenders thus demonstrate the dynamic nature of their markets and their capacity to innovate.

As we mentioned earlier, our results also raised questions about the positive relationship between warnings, bans and criminal performance. Our multivariate model demonstrated that the members who broke the rules and received warnings from the administrators as well as those who were eventually banned managed to increase their rate of

transactions. This finding was counterintuitive as other participants in the market should have been afraid to deal with members who had been labeled as troublemakers by the administrators. Two reasons might explain this surprising result. First, we noticed that many members received warnings for spamming the forum with messages advertising their services. Participants were therefore bombarded with information about stolen financial data and many may have been tempted to deal with the offending members. As in any market, the most visible players often manage to increase their sales more than others. In this case, spamming others appeared as a valuable marketing tool for criminals. A second explication can be found in Lyng's (2004) edgework theory. According to this theory, many individuals decide to get involved in high-risk activities such as extreme sports and financial markets. These activities take place in risky and uncertain settings. To understand why some individuals would agree to participate in such activities, Lyng (2004) states three explanations: 1) the desire to seek strong emotions; 2) the deep satisfaction of overcoming these strong emotions and; 3) the high returns these activities offer. Not everyone succeeds equally in high-risk settings. A minority of participants has developed over time an expertise that allows them to maneuver more efficiently in this environment.

It appears as though carding is another example of edgework theory (Lyng, 2004). Carders are attracted by the thrill the activity provides and the possibility of making huge profits. Those who manage to outperform others are those who have developed the best strategies to take advantage of the rules of the game. The environment provides certain opportunities that only some individuals know how to take advantage of. Reputation and warnings are opportunities that can help increase the criminal performance of carders but only a limited number of individuals have understood how they could be used as tools to achieve this goal. By combining the two, players grab every available opportunity and manage to outperform others.

Edgework views risks as opportunities but we must be careful not to forget that warnings in this case may lead to banishment. Our analysis of the expected survival rate of carders demonstrates that most individuals who receive warnings have shorter criminal careers on the exchange platform and therefore fail to turn this risk to good account. This is reminiscent of the saying that a bird in hand is worth two in the bush. As such, warnings pose

high risks to carders and they should only be used by those with enough expertise to gain from them.

Edgework theory was first elaborated to explain the behavior of adepts of extreme sports. In later writings, it was adapted to others settings such as financial markets (Smith, 2004) and even crime in general (Morselli et al., 2004). This paper confirms the conclusions of Morselli et al. (2004), who stated that structured recklessness was actually responsible for the good performance of offenders. Taking risks can sometimes be advantageous to economic agents, whether or not they are criminals.

Conclusion

Understanding success in criminal markets is of the utmost importance as it explains why crime attracts so many individuals and why so many criminals persevere in their life of crime for so long in spite of all the negative impacts on their life. As long as criminals believe that a criminal market has the potential to make them rich, they will continue to participate in it and to commit crimes. Understanding what makes some criminals more successful than others allows us to better control these individuals and break the cycle whereby the success of a few criminals encourages many others to follow suit.

The fact that one theory can be applied to both the consulting market and a carding market highlights the similarities between the legitimate and illegitimate worlds, something that has been hinted at numerous times in previous research. In both cases, reputation plays a crucial role in achieving a certain level of success. Past research has shown that personal characteristics, behavior and networking all have an impact on reputation and longitudinal models should be developed in the future to better understand the formation of reputation and its subsequent impact on criminal performance.

One of the most interesting results of this paper concerns the notion of deviance. As we mentioned above, carders looking for that extra edge over others need to bend the rules from time to time. This implies that even criminal markets have rules. The question of whether and how these rules are enforced was not the focus of this paper but it appears as a promising lead for future research. Some scientists seek to find structure where there appears to be none. What we began to outline with this paper is the structure of a criminal community and how its

participants relate to one another. Such markets appear to be chaotic and disorganized environments. Our findings provide the basis for further research and hint that contrary to this traditional belief, there is a hidden structure awaiting to be discovered in other similar criminal markets.

CONCLUSION

L'existence même d'une forme particulière de criminalité sur internet est encore aujourd'hui une source de débats (McGuire, 2007). Certains auteurs se demandent en effet pourquoi et comment une simple innovation technologique pourrait être responsable d'un changement de paradigme en criminologie. Ceux-ci voient la criminalité comme une simple infraction aux normes sociales et le contexte dans lequel un tel acte se produit ne serait que secondaire. Des inventions passées comme l'automobile, le téléphone et la poste semblent leur donner raison a priori; personne n'ose publiquement se proclamer spécialiste des crimes de l'automobile et affirmer que les criminels qui utilisent un véhicule moteur se démarquent de la masse des criminels. Pourquoi l'internet devrait-il alors être différent? Nos résultats nous permettent de fournir une réponse à cette question et de contribuer à ce débat sur l'impact de l'internet sur la criminalité.

Notre thèse générale est que l'impact de l'internet est la transformation du modèle criminel et non la création d'un nouveau modèle. Il est vrai que plusieurs types de crimes ne pourraient exister sans la toile. Nous avons étudié exhaustivement le cas des botnets, ces réseaux d'ordinateurs infectés qui sont utilisés pour envoyer des pourriels et voler des informations personnelles et financières, entre autres. Nous retrouvons aussi dans cette catégorie d'autres crimes comme le déni de service où un criminel inonde de connexions un serveur afin que ses utilisateurs légitimes ne puissent s'y connecter. Bien que ces comportements aient des conséquences bien réelles pour leurs victimes, leur avènement reste secondaire face à la multitude de formes particulières de crimes qui ont été transformées par l'arrivée de l'internet. Ces changements s'observent à six niveaux différents : 1) l'augmentation de la facilité à trouver des co-criminels; 2) l'augmentation de la compétition entre les criminels; 3) l'augmentation du nombre de victimes; 4) la diminution des risques d'arrestation; 5) l'augmentation du taux de réussite des criminels; et 6) les changements dans l'équilibre entre criminels, victimes et protecteurs.

Pour illustrer l'étendue de l'impact de l'internet, nous prendrons comme point de référence le marché de la fraude en Angleterre dans les années 1948 à 1972 (Levi, 2008). Nous avons choisi ce point de comparaison pour deux raisons. Tout d'abord, l'époque étudiée est

antérieure à l'apparition des réseaux informatiques. Les ordinateurs personnels eux-mêmes étaient encore très peu répandus dans les années 1970 et l'internet n'en était qu'à ses premières phases de test. Les chances de contamination des données sont donc ici nulles. Par ailleurs, la fraude est un crime en col blanc qui se rapproche des crimes étudiés dans cette thèse. La motivation principale de ce type de criminels est de faire des profits et ils choisissent pour ce faire des comportements qui ne font pas appel, en général, à la violence. Dans les deux cas, la manipulation des victimes est au centre des activités, qu'il s'agisse de convaincre un utilisateur de cliquer sur un lien pour qu'il installe un virus, de convaincre un individu de fournir ses informations bancaires à l'aide d'un formulaire en ligne ou de convaincre une institution d'ouvrir une ligne de crédit comme dans le cas de Levi (2008).

Le livre de Levi (2008) s'intéresse donc à la fraude par crédit. Pour commettre un tel crime, des individus investissent temps et ressources afin de se bâtir un dossier de crédit. Ils agissent donc dans un premier temps comme n'importe quel homme d'affaires le ferait. Lorsqu'ils estiment avoir une assez bonne cote de crédit, ils empruntent alors au maximum de leurs marges et commandent des produits avec l'argent emprunté. Ils disparaissent ensuite avec les produits et les profits accumulés sans rembourser leurs créditeurs.

Lévi décrit l'évolution de ce type de fraudes au courant des années 1948 à 1972. Au départ, deux types de personnes s'adonnaient à ce genre d'activités. D'un côté, de petits criminels peu organisés et sans grande envergure qui tentaient tant bien que mal de vivre de ces revenus illicites. De l'autre, des hommes d'affaires peu scrupuleux qui saisissaient une opportunité s'offrant à eux ou qui étaient en position difficile et qui ne voyaient d'autres moyens de régler leurs problèmes d'argent. Les hommes d'affaires n'avaient souvent que peu de contacts avec le monde interlope et agissaient seuls. Une certaine proportion d'entre eux avaient, il est vrai, des liens avec le monde criminel, mais ceux-ci étaient faibles et distants. Dans la première tranche de l'étude de Levi, le marché de la fraude par crédit était peu régulé et les chances d'arrestation étaient relativement faibles. Comme la majorité des criminels étaient des hommes d'affaires sans aucun lien avec le monde interlope, ils passaient habituellement sous le radar policier. Le marché était aussi très décentralisé et aucune organisation n'était en mesure de contrôler ce type de fraude.

Voyant certains individus prospérer à travers ce type de criminalité, deux organisations criminelles ont décidé de se lancer dans ce type de fraude à partir des années 1960. Plutôt que faire leurs propres fraudes, ces organisations ont tenté de contrôler les acteurs déjà présents sur le marché ainsi que les nouveaux entrants. Ces deux clans fournissaient alors les prête-noms et les mises de fonds nécessaires au lancement de ce type de fraude. Pour assurer leur mainmise sur ce marché, les organisations criminelles ont utilisé la violence, créant une onde de choc parmi la communauté de fraudeurs habitués à agir de façon indépendante. Cette violence a rapidement fait augmenter la surveillance de la police sur ces organisations qui se sont retrouvées, au bout de quelques années, démantelées suivant l'emprisonnement de leurs têtes dirigeantes.

Levi (2008) tire deux constats de l'étude du marché de la fraude par crédit. Tout d'abord, il est extrêmement difficile de contrôler un marché criminel. Les deux organisations criminelles ont rencontré énormément de résistance de la part des fraudeurs et ceux-ci ont finalement accepté de collaborer avec la police afin de faire cesser les abus. Les têtes dirigeantes étaient donc en partie responsables de leur sort. Par ailleurs, le marché de la fraude par crédit est un milieu extrêmement méfiant où la confiance est pratiquement absente. Ses acteurs agissent régulièrement de manière opportuniste et n'hésitent pas à se voler les uns les autres à la première occasion. Cela augmente le niveau de risque pour les participants qui doivent se surveiller mutuellement. Ceux-ci doivent aussi suivre leur fraude de beaucoup plus près, augmentant ainsi leur exposition et les chances qu'ils laissent des preuves de leur implication. Cette dynamique a finalement pour effet de nuire grandement à l'efficacité du marché. Levi (2008) cite un criminel qui affirme que s'il avait pu trouver des partenaires fiables, il aurait engrangé plusieurs millions de plus.

Ce texte de Levi (2008) nous permet d'établir une base de référence afin de mieux comprendre l'impact de l'internet en fonction des six niveaux présentés précédemment. Cet impact s'observe tout d'abord par la saveur internationale et la facilité accrue avec laquelle les individus peuvent trouver des co-criminels. Nous avons en effet pu constater qu'un même forum de discussion regroupait des acteurs venant de toutes les régions du monde (Décary-Hétu & Dupont, 2012). Il en va de même pour le marché de cardeurs (Décary-Hétu & Charette, à venir) et la scène des warez (Décary-Hétu et al., 2012) bien que ces aspects n'aient

pas été explorés en profondeurs dans ces articles. Dans les trois cas, des plateformes virtuelles (index, forums de discussions) ont remplacé les tavernes d'antan et offrent la possibilité aux criminels de trouver des partenaires d'affaires ou encore des victimes potentielles. Levi (2008) affirme que le manque de personnel fiable est une des plus grandes limites à l'essor du marché de la fraude par crédit. Il était en effet difficile pour les criminels de l'époque de trouver des partenaires fiables en raison du caractère illégal de leurs activités et des risques d'arrestation et d'infiltration. Les criminels devaient alors faire ce qu'ils pouvaient avec les criminels dans leur entourage, entraînant une performance sous-optimale.

L'internet a aussi entraîné une compétition beaucoup plus vive entre criminels. Le cas de la scène des warez illustre le mieux ce phénomène. À leurs débuts (Craig, 2005), les pirates de la scène communiquaient entre eux en se laissant des messages sur les *Bulletin Board System* (BBS). Ceux-ci étaient de simples plates-formes électroniques connectées à une ligne téléphonique. Pour y avoir accès, les pirates devaient téléphoner au numéro de téléphone du BBS à l'aide de leur ordinateur pour obtenir une interface texte leur permettant de visionner les messages laissés par les autres et d'y répondre. Comme toutes les communications se faisaient via les lignes téléphoniques, un pirate désirant se connecter à un BBS situé dans un autre indicatif régional devait payer les frais d'interurbains applicables à l'appel qui était facturé comme une communication régulière. Bien que certains groupes aient été en mesure de contourner ces frais en fraudant les compagnies de téléphone, la majorité des acteurs de la scène n'avaient pas cette capacité et la compétition sur la scène des warez était donc avant tout locale. Les groupes de pirates étaient en compétition avec les autres formations de leur indicatif régional. Avec l'arrivée de l'internet, les frais interurbains ont disparu, permettant ainsi aux meilleurs groupes du monde de s'affronter sur un terrain de jeu égal et de mesurer leur productivité à celle des autres. Sans internet, la scène des warez n'aurait donc pu atteindre le niveau international qu'elle a aujourd'hui; celui-ci a donc permis à de nouvelles compétitions de voir le jour. Dans le cas des marchés de botnets et de cardeurs, l'arrivée des plateformes en ligne a diminué l'asymétrie d'information qui régnait au niveau de l'offre de produits. En magasinant sur les marchés en ligne, les clients peuvent évaluer chacune des offres et sélectionner celle qui les intéresse le plus en fonction du profil du vendeur et de la qualité du produit. La compétition devient donc beaucoup plus forte entre vendeurs. Dans le

cas des fraudeurs du crédit, plusieurs d'entre eux se connaissaient et s'entraidaient au besoin (Levi, 2008). Les relations personnelles étaient beaucoup plus importantes et le faible nombre de fraudeurs assurait à tous une place dans le marché. Les développements récents dans d'autres marchés criminels nous laissent penser que si l'internet avait existé au cours de la période de l'étude de Levi (2008), la compétition aurait été beaucoup plus féroce entre les fraudeurs et ceux-ci auraient alors pu identifier et recruter des partenaires beaucoup plus facilement en consultant leur profil en ligne.

L'internet n'a pas que fourni un accès à un plus grand bassin de criminels potentiels. Il a aussi permis d'augmenter exponentiellement le nombre de victimes potentielles. Que ce soit au bureau, à l'école, à la maison ou encore à l'aide d'un téléphone intelligent, l'accès à l'internet est devenu une commodité qui est utilisée par une majorité de la population du monde développé. Chacune de ces personnes est une cible potentielle et même des ordinateurs personnels peu performants peuvent devenir des actifs importants lorsqu'agrégés en grand nombre. Krebs (2012b) illustre en effet les multiples usages criminels de telles machines. Ceci inclut l'hébergement de contenu illicite pour la scène des warez, l'envoi d'attaques par déni de service pour les botmasters et la surveillance des utilisateurs afin de voler des informations personnelles et financières dans le cas des cardeurs. La valeur des ordinateurs augmente encore davantage lorsqu'il s'agit de machines appartenant à de grandes entreprises et donnant accès aux ressources internes des compagnies. L'internet est donc un outil qui permet aux criminels de trouver et d'attaquer des cibles en plus grand nombre. Ceci pourrait expliquer le grand dynamisme des communautés en lignes étudiées dans nos recherches. Uniquement dans les échantillons analysés dans cette thèse, nous retrouvons des dizaines de milliers d'individus responsables de plusieurs centaines de milliers de crimes. Les possibilités qu'offre l'internet sont impressionnantes et il n'est guère surprenant de constater que la plupart des logiciels et films produits se retrouvent plus tôt que tard sur les serveurs de la scène des warez. Il en va de même pour les botnets qui comptent maintenant des millions d'ordinateurs infectés et pour les cardeurs qui capturent les informations personnelles à coups de millions sur des serveurs gouvernementaux ou de compagnies. Avec l'internet, les fraudeurs du crédit auraient pu créer de fausses entreprises en ligne et abuser des nouveaux services de crédit en ligne afin d'augmenter considérablement les dommages subis. Ils n'auraient par ailleurs plus été limités

géographiquement, une autre limite soulevée par Levi (2008). Contrôler des partenaires dans d'autres quartiers et d'autres villes était excessivement difficile pour les fraudeurs et cela encourageait encore davantage les comportements opportunistes chez les criminels. Finalement, bâtir une entreprise crédible auprès des créanciers nécessitait habituellement la location de bureaux et l'embauche d'employés. Le temps investi dans ces tâches pourrait aujourd'hui être investi dans l'augmentation du nombre de victimes.

Par ailleurs, il est souvent difficile d'identifier avec précision les auteurs d'actes criminels en ligne. Une multitude de services permettent en effet de camoufler le point d'origine des connexions. Nous avons indiqué dans notre revue de littérature l'existence de systèmes de type *fast flux* qui permettent aux botmasters de communiquer de façon anonyme avec les ordinateurs qu'ils ont infectés. Les visiteurs de forums de discussions utilisent aussi des services pour camoufler leur identité et cette pratique est recommandée par les administrateurs des forums. Les pirates du warez se réunissent pour leur part dans des salles de clavardage privées et se cachent derrière leurs serveurs privés. Seuls quelques élus peuvent accéder à ces ressources. Les forces de l'ordre n'ont donc pas encore les outils pour faire face à ce type de crime. C'est pour cette raison qu'il est très rare d'entendre parler d'arrestations chez ce type de criminels; les services de police se contentent bien souvent de démanteler l'infrastructure des pirates plutôt que de tenter de découvrir leur identité. Levi (2008) souligne pour sa part que les fraudeurs se devaient d'être présents dans les locaux de leurs entreprises pour surveiller les activités de la firme et d'être très impliqués dans le suivi de la fraude. Cela les exposait grandement aux frappes policières. Avec les possibilités de télétravail et de télésurveillance qu'offre internet, de tels risques pourraient être aujourd'hui grandement diminués. Pour les personnes ayant les connaissances nécessaires, il serait aussi possible de chiffrer et de sauvegarder à distance les données sensibles reliées aux fraudes. Une comptabilité compromettante n'aurait ainsi plus à être sauvegardée dans les bureaux de l'entreprise.

En plus d'être d'origines nébuleuses, les attaques des criminels d'aujourd'hui ont aussi beaucoup plus de chance de réussir sur internet que dans le monde réel. Les botmasters peuvent attaquer des systèmes informatiques un nombre illimité de fois en utilisant des méthodes variées jusqu'à ce que l'une d'entre elles fonctionne. Les départements de sécurité

se doivent de repousser chaque attaque afin d'être efficaces; les criminels, eux, n'ont qu'à être chanceux ou compétents une seule fois pour atteindre leurs objectifs. Les pirates de la scène des warez peuvent aussi compter sur plusieurs vecteurs d'attaque. Craig (2005) indique à ce sujet que les pirates ont par le passé bâti de faux sites de critiques de jeux afin de recevoir des copies d'évaluation à l'avance et les distribuer illégalement. Ils ont aussi soudoyé des employés des usines d'emballage de Cds et de Dvds afin qu'ils volent des produits avant leur sortie. L'internet permet ici d'identifier et de rejoindre des individus qui seraient potentiellement enclins à participer à ce genre d'entreprises. Les cardeurs, finalement, ont accès à un nombre quasi illimité de numéros de cartes de crédit. Si l'un d'entre eux ne fonctionne pas, ils peuvent demander un échange ou encore en acheter un autre pour quelques dollars. L'information des cartes de crédit peut être copiée en quelques secondes sur une carte clonée. Il est ainsi on ne peut plus aisé pour un criminel de copier plusieurs cartes et de vider des guichets automatiques sans avoir à se soucier des risques d'arrestation étant donné l'impossibilité de surveiller tous les guichets d'une ville à la fois. Levi (2008) souligne pour sa part que les fraudeurs de crédit n'étaient pas en mesure d'optimiser leurs pratiques et que leurs fraudes restaient dans la plupart des cas très simples. Les créditeurs apprenaient rapidement de leurs erreurs et étaient en mesure de partager l'information sur les fraudes passées. Il devenait donc de plus en plus difficile avec les années de réaliser des fraudes ; à l'inverse des criminels de l'internet qui, eux, voient leurs capacités augmenter avec le temps.

L'internet vient ici modifier profondément la relation entre les criminels, les victimes et les protecteurs, les trois piliers de la prévention situationnelle (Clark, 1997). Alors qu'il existait un certain équilibre entre ces trois forces auparavant, l'internet semble vouloir pencher décidément en faveur des criminels dans le contexte virtuel. Ceux-ci ont accès à un plus grand nombre de ressources en raison du bassin de criminels motivés qui fréquentent les marchés criminels en ligne et les groupes de discussion. Les victimes n'ont toujours pas développé les réflexes leur permettant de se protéger adéquatement contre les menaces. Les protecteurs se retrouvent pour leur part contre des adversaires qu'ils n'arrivent pas à identifier et qui sont en mesure de profiter de chacune des brèches pour s'infiltrer dans les systèmes et obtenir accès aux produits et informations qu'ils recherchent. Un tel déséquilibre des opportunités et des risques de victimisation est dû à une innovation technologique en particulier, l'internet. De par

la transformation profonde qu'il apporte aux forces en présence, l'internet a eu et continuera d'avoir un impact profond sur le phénomène criminel mondial.

Ce résultat est en partie une conséquence de la montée en puissance de l'individualisme réseauté présenté au début de cette thèse. Nous avons déjà statué de la pertinence d'appliquer cette théorie aux relations interpersonnelles des pirates informatiques. Les articles présentés dans cette thèse nous permettent d'apporter un meilleur éclairage sur ce sujet. La première caractéristique de l'individualisme réseauté stipule que les personnes entretiennent des relations autant avec des personnes proches qu'éloignées géographiquement (Boase & Wellman, 2006). Notre discussion de l'impact de l'internet sur la criminalité nous a permis de renforcer à nouveau ce point. Les participants des marchés illicites proviennent de tous les continents et rien n'indique dans nos données qu'il existe un quelconque mur qui limite les interactions entre personnes éloignées. Au contraire, les plateformes en ligne ont été adoptées justement pour permettre aux criminels de trouver des partenaires et d'obtenir le meilleur prix possible pour leurs produits et services. Avec l'internet, les communications sont instantanées et les téléphones mobiles permettent maintenant de répondre aux demandes et communications, peu importe où nous nous trouvons. Cela ne fait qu'ajouter à la fluidité des échanges entre criminels ainsi qu'à leur succès. La mondialisation permet en effet d'augmenter ses bénéfices en trouvant le partenaire idéal tout en limitant ses risques en jouant sur les différentes juridictions. Un service de police européen aura en effet beaucoup de difficultés à obtenir un mandat d'arrêt contre un individu d'Asie du Sud-Est responsable de fraude financière en ligne.

Boase & Wellman (2006) affirment par ailleurs que les individus sont aujourd'hui impliqués dans de nombreux réseaux très denses, mais qui ont peu de contacts entre eux. Ce constat est validé en partie par nos données. Dans tous les cas, les criminels sont en contact avec un nombre important d'individus. Les cardeurs comptent en moyenne plus de 130 liens directs, une mesure qui monte à 225 chez les botmasters et à au moins 150 chez les pirates de la scène des warez. La logique veut que ces larges cercles sociaux soient divisés en de nombreux sous-groupes. Il serait en effet impraticable pour les criminels de former des cliques avec autant d'individus. À la différence de Boase & Wellman (2006) cependant, nos études sont mitigées sur la cohésion interne des sous-groupes qui se forment dans les communautés

criminelles. Dans le cas de la scène des warez, le coefficient d'agglomération indique une tendance à l'augmentation des liens forts dans les cliques de la scène. Ceci n'est pas le cas dans nos deux autres études où la contrainte est relativement faible. Le débit d'information potentiel entre acteurs est donc limité et ne permet pas une pleine réalisation de l'individualisme réseauté. Cependant, il se pourrait qu'ici le caractère illicite des réseaux étudiés ait eu un impact sur la qualité des liens. Alors qu'un groupe de loisirs pourra développer des liens forts et redondants, une organisation criminelle sera limitée dans son réseautage de par le contrôle social qui s'exerce sur elle et de par les menaces à sa sécurité qui en découlent. Par ailleurs, nos sources de données n'étaient pas complètes et ne nous permettaient pas d'avoir accès à tous les canaux de communication utilisés par les criminels – surtout pour les botmasters. Il se pourrait donc que le chiffre noir des communications nuise à notre compréhension du phénomène des relations à haut débit dans le monde illicite. Malgré tout, cette multiplication des liens et des groupes devrait garantir aux criminels des chances plus élevées de succès (Morselli, 2009). En ayant accès à des sources d'informations et des contacts aussi diversifiés, les criminels s'assurent de toujours avoir des opportunités criminelles à leur portée et ainsi d'être en mesure de réaliser leur plein potentiel.

Pour ce qui est du côté éphémère des relations, nous avons déjà mentionné que la courte durée de vie des pirates du warez entraînait obligatoirement un renouvellement constant des liens dans la scène. Les deux autres communautés criminelles offrent un portrait similaire avec des durées de vie moyennes d'une année ou moins dans les deux cas. Ceci implique que les criminels ont, en général, de la difficulté à s'établir dans ces marchés compétitifs et que les relations à long terme ne sont pas la norme. Ceci a pour effet d'augmenter l'incertitude et les risques de comportements opportunistes dans les transactions. Dans un tel contexte, la réputation prend alors encore plus d'importance. Nos recherches ont démontré en effet que la réputation, qu'elle soit publique ou réseautée, améliore les chances de transiger à nouveau dans le futur. Ces relations d'affaires sont toutefois minces étant donné que seule une mince proportion de partenaires d'affaires concluront une transaction ensemble à nouveau. Il devient donc important d'utiliser au maximum les possibilités que chaque contact nous apporte. Ce dernier peut être un amplificateur de réputation ou encore une porte d'entrée vers un autre groupe de contacts.

Ce jeu des relations est particulièrement important dans les marchés criminels où les acteurs ont des origines et des profils vastement différents. Notre étude de l'écosystème du carding par exemple nous a permis de comprendre qu'il existait une division du travail bien définie où des individus aux caractéristiques bien particulières remplissent des tâches spécifiques. Les individus en mesure de voler les informations personnelles ou financières ne sont pas nécessairement les mêmes qui fabriquent de fausses cartes de crédit. Le même phénomène s'observe dans la scène des warez où cette division s'opère à l'intérieur des groupes de pirates et non dans la communauté en général. Certains membres agissent comme leaders alors que d'autres brisent les systèmes de protection contre les copies. Les criminels se doivent d'être en mesure d'aller au-delà de leurs préférences personnelles et de l'homophilie afin de performer et de fonctionner dans ce monde interlope. Le marché des botnets étudiés dans cette thèse illustre cette orientation avec des participants venant de tous les continents, incluant l'Océanie. Cette capacité à sortir de sa zone de confort et de former des réseaux avec des individus aux profils différents est une source de force pour les criminels. Ceux-ci peuvent se concentrer sur ce qu'ils font de mieux et utiliser les services spécialisés des autres au besoin. Cette spécialisation des activités augmente la performance et l'efficacité de chaque individu permettant ainsi de meilleures chances de succès des entreprises criminelles.

S'associer avec des personnes qui ne nous ressemblent pas n'est souvent pas un gage de liens forts. Boase & Wellman (2006) affirment que dans le contexte de l'individualisme réseauté, les liens auront tendance à être plus faibles que forts. Cette faiblesse s'observe à deux niveaux. Tout d'abord, les participants ont mis en place des systèmes automatisés de reconnaissance pour se protéger contre les individus aux profils trop opportunistes. Des administrateurs gèrent aussi activement les marchés illicites afin de s'assurer de limiter les conflits entre participants. Il est apparent que de tels systèmes ne seraient pas nécessaires dans une communauté aux liens forts où les relations sont bâties sur la confiance. Par ailleurs, les liens d'affaires entre les individus dans les marchés des botnets et du carding sont des plus limités. Seulement une mince proportion d'entre eux transigent plus d'une fois ensemble et les relations ont tendance à être très éphémères. Dans ce contexte, établir des liens forts est excessivement difficile. Ce qui peut sembler un problème au départ peut toutefois aussi être vu comme un bénéfice par bien des criminels. En étant libres d'agir à leur guise, les criminels ont

dans ces marchés illicites une liberté d'action qui est inégalée. Ils n'ont que peu d'alliances ou de liens avec les autres et ils peuvent ainsi décider beaucoup plus librement de leurs actions.

Ce que nous observons dans les trois communautés de criminels est une transformation et une adaptation des comportements criminels à un nouveau médium, l'internet. Celui-ci fait pencher la balance du pouvoir en faveur des criminels qui voient leurs chances de succès augmenter tout en maintenant ou diminuant les risques d'arrestations. Ceci laisse présager une période d'adaptation possiblement douloureuse pour les victimes, tant chez les particuliers que chez les entreprises. En adoptant l'individualisme réseauté, les criminels arrivent à maximiser les opportunités criminelles tout en limitant leur exposition au risque. Le fait de communiquer et d'interagir avec un grand nombre de personnes permet d'avoir accès à une quantité d'information importante. Si ces personnes évoluent dans des cercles différents et qu'elles ont des profils qui se démarquent les uns des autres, l'information qui circulera sera d'autant plus variée et riche. Bien qu'elle puisse être d'une utilité limitée au niveau individuel, au niveau agrégé, cette information peut être un gage de succès important pour les criminels. Comme la plupart d'entre eux entretiennent des liens faibles, les risques qu'un autre individu puisse utiliser de l'information confidentielle sont plus limités. Un criminel n'aurait que peu de prise sur les autres membres de son milieu en raison de la faible connaissance qu'ils ont l'un de l'autre. L'internet ouvre donc la porte à de nouvelles opportunités pour les criminels.

Les interactions interpersonnelles n'ont pas seulement été transformées en raison de l'individualisme réseauté. Il faut au contraire comprendre le concept de réputation dans le contexte de marchés criminels en ligne pour saisir l'étendue des transformations récentes du milieu. Dans notre article sur la scène des warez, nous avons constaté que la réputation est la principale source de motivation. Les pirates sont impliqués dans un tournoi perpétuel afin de prouver leur valeur à leurs pairs; ils ne peuvent en aucun cas s'asseoir sur leurs réalisations passées et doivent se prouver semaine après semaine. Les groupes qui sont les plus productifs et qui réussissent à survivre le plus longtemps ont plus de réputation que les autres. Le fait d'avoir distribué un produit dispendieux et de s'attaquer à plusieurs types de propriété intellectuelle permet aussi d'augmenter sa réputation.

La performance est aussi corrélée à la réputation chez les botmasters. Dans ce marché, les pirates qui survivent le plus longtemps reçoivent plus de points de réputation que les autres. Les participants ont intérêt à commencer leur carrière le plus tôt possible étant donné que l'âge est inversement corrélé à la réputation. Les relations cordiales sont récompensées tout comme les relations personnelles rapprochées. Un grand nombre de contacts amène plus de réputation. Ces liens sont d'autant plus bénéfiques lorsqu'ils se font au sein de cliques denses. Ce marché est plus centralisé que celui des warez et évolue sous la surveillance d'administrateurs. Ceux-ci ont un impact important sur les réputations des membres en sélectionnant ceux qui reçoivent des mentions et qui sont acceptés dans les clans.

L'importance de la réputation dans l'écosystème d'un marché criminel a été confirmée à l'aide de notre troisième et dernier article. Dans ce forum où les participants pouvaient acheter et vendre des informations financières volées, la réputation est un prédicteur de la performance criminelle. Différents types de réputation ont des impacts différents. Les expériences de première main sont ainsi plus efficaces que les informations publiques. L'expérience passée mesurée à l'aide du nombre de transactions passées est aussi significative tout comme le nombre de contacts. Le rôle de courtier ainsi que le niveau de contrainte nuisent pour leur part à la performance des cardeurs.

Ces trois milieux criminogènes nous donnent l'opportunité de comprendre l'importance de la réputation dans le contexte d'un marché qui était déjà présent dans les réseaux informatiques avant l'internet (le warez), d'un marché qui est apparu avec l'internet (les botnets) et d'un marché qui a fait la transition du monde physique au monde virtuel (le carding). Nous constatons tout d'abord que dans le cas des warez, la motivation principale est la réputation elle-même alors que dans les autres cas, les profits monétaires sont l'objectif recherché par tous. Les pirates issus de la scène des warez auraient la possibilité de monétiser leur travail en vendant des produits de contrefaçon. Avec leurs réseaux de fournisseurs bien rodés, ces pirates ont un accès direct au matériel brut nécessaire à ce genre de fraude. Le fait qu'ils aient toujours baigné dans la mentalité du piratage semble ici jouer un rôle prépondérant dans le rationnel des pirates. Ils s'inspirent en effet des mantras des premiers pirates qui affirmaient que toute l'information doit être libre. Mettre un prix sur cette information devient alors un mur qui empêche sa libre circulation. Les botmasters et les cardeurs ne sont pas liés

par le même historique et peuvent, eux, profiter au maximum de leurs crimes. Ils s'apparentent donc davantage à des mercenaires qui recherchent le bien personnel plutôt que celui de la communauté.

Ces trois formes particulières de crimes se rejoignent cependant dans la place qu'ils accordent à la réputation. Cette dernière se transforme ici en capital virtuel qui permet aux criminels d'atteindre plus efficacement leurs objectifs. Dans le cas de la scène des warez, une bonne réputation permet de recruter les meilleurs membres de la scène. Craig (2005) souligne que les pirates ont tendance à changer régulièrement d'allégeance et une invitation dans un des grands groupes de la scène des warez ne se refuse tout simplement pas. Ce capital enclenche donc un cercle vicieux où les groupes les plus réputés sont en mesure de recruter les collaborateurs les plus efficaces qui leur permettront à leur tour de maintenir voir d'augmenter leur performance et leur réputation. Ceci pourrait expliquer pourquoi tant de groupes naissent et meurent à chaque mois dans la scène. Ils ne seraient tout simplement pas en mesure d'atteindre un seuil critique de réputation qui leur permettrait de survivre.

Dans le cas des botmasters et des cardeurs, bien que ce capital virtuel ne soit pas l'objectif final, il remplit un rôle similaire à celui que nous venons de décrire et peut être utilisé afin de maximiser la performance. En effet, plusieurs signaux utilisés pour juger du caractère d'un individu ne sont tout simplement pas disponibles sur la toile mondiale. Nous sommes habitués à évaluer l'apparence physique, la posture, l'habillement et l'accent d'une personne pour se forger une image de celle-ci. Sur l'internet, tous ces signaux ne sont tout simplement pas disponibles et ne nous sont d'aucune utilité pour déterminer la fiabilité d'un possible partenaire d'affaires. Il en va de même pour plusieurs autres signaux tels que le vocabulaire ou encore les connaissances générales. Ces signaux sont aussi souvent utilisés, mais peuvent être facilement imités lorsque transmis par internet. Un individu peut par exemple prendre le temps de faire les recherches nécessaires sur une sous-culture ou encore imiter une façon de parler beaucoup plus facilement en ligne qu'elle ne le pourrait en personne. Dans ce contexte, les signaux que nous utilisions traditionnellement pour évaluer les individus de notre cercle social sont donc soit inexistants soit facilement manipulables. La réputation devient alors de facto le signal vers lequel les acteurs se tournent afin de juger les individus. Étant donné l'importance des relations interpersonnelles dans le contexte de

marché, une bonne réputation augmentera inévitablement les opportunités et les revenus des personnes impliquées.

Si ce capital virtuel a été adopté par les criminels, c'est en partie en raison de sa capacité à minimiser certaines lacunes de marchés criminels traditionnels comme celui de la fraude par crédit. Nous avons déjà souligné qu'il était excessivement difficile pour les fraudeurs de trouver des partenaires fiables et qu'il existait un manque de confiance total entre les participants du marché. Les systèmes automatisés de reconnaissance étudiés dans cette thèse viennent retirer toute subjectivité dans l'évaluation des individus et amènent des données dures sur lesquelles les acteurs peuvent baser leurs décisions. Choisir le meilleur vendeur de cartes de crédit ou le service de pourriel le plus fiable est beaucoup plus facile lorsque des centaines d'individus ont évalué tous les services disponibles. Le capital virtuel répond à un besoin criant des criminels et ceux-ci sont prêts à faire la transition du monde physique vers le monde virtuel pour pouvoir en profiter.

À la lumière de ces résultats, il est pertinent de se demander pourquoi si peu de gens ne s'investissent pas dans une carrière criminelle en ligne. Nos revues de littératures ont en effet démontré que toute l'information nécessaire pour devenir un criminel performant est disponible dans des forums de discussion en ligne ou encore dans des salles de clavardage IRC. De simples recherches dans le moteur de recherche de Google pointent directement vers ces ressources. Nous avons aussi déterminé que tous les outils sont aussi disponibles en ligne. Dans le cas des logiciels de contrôle de botnets, le prix d'acquisition varie de quelques centaines à quelques milliers de dollars. Dans d'autres cas, la plupart des outils sont gratuits et à code libre. Même le code source de Zeus, le logiciel de contrôle de botnets le plus utilisé, est aujourd'hui disponible gratuitement ayant été publié illégalement par un de ses utilisateurs. Finalement, nous avons aussi pu remarquer qu'en général, les risques d'arrestation reliés aux cybercrimes sont assez minces. Au Canada seulement, nous parlons toujours de l'opération BASIQUE qui a permis l'arrestation de 10 botmasters (Dupont, 2013). Depuis les dernières années cependant, nous attendons toujours une suite à cette opération qui était sans précédent au Canada à l'époque. Il semble donc que les botnets soient des crimes à peu de risques, du moins au Canada.

Nous pouvons proposer quatre raisons qui expliqueraient l'apparente petite taille de la communauté des cybercriminels. Tout d'abord, bien qu'il existe un nombre très important d'opportunités criminelles sur internet, ces opportunités ne sont pas visibles ou connues de tous. Les chercheurs ne font que commencer à explorer cet univers et à comprendre la structure sociale et le modus operandi de ces individus. La plupart des opportunités criminelles se transmettent de bouches à oreilles virtuelles et leur diffusion s'en trouve donc limitée. Les criminels n'ont d'ailleurs pas intérêt à attirer un trop grand nombre de nouvelles recrues afin de ne pas attirer l'attention des forces de l'ordre. Une hausse marquée du nombre de victimes pourrait en effet pousser les services de police à finalement s'attaquer à cette problématique. Par ailleurs, même les individus qui sont mis au fait des opportunités criminelles ne sont possiblement pas au courant d'où trouver les outils et/ou les conseils pour en tirer avantage. Il est vrai que bien des ressources sont disponibles gratuitement, mais leur qualité est de niveau variable et il n'est pas toujours aisé pour des novices informatiques de les appliquer. Ceux-ci auront tendance à laisser plus de traces et ainsi à se mettre davantage en danger. La formation de nouveaux cybercriminels peut donc prendre un certain temps et amener certains individus à abandonner ce type d'activité avant même d'avoir commis un seul crime. Troisièmement, le monde criminel attend toujours de pouvoir compter sur un leader voir même un modèle. Bien des pirates informatiques ont été accusés et condamnés, mais ceux-ci le sont pour des raisons politiques ou encore pour des pertes financières des entreprises – rarement pour leurs gains personnels. Le cas de Kevin Mitnick dont nous avons déjà parlé dans cette thèse illustre bien ce phénomène. Celui-ci a causé des pertes de productivité évaluées en millions de dollars, mais n'a jamais profité financièrement de ses crimes. À l'inverse, des pirates comme Kim Dotcom qui ont profité de leurs actes de piratage pour se faire connaître et lancer des services supposément illicites ne sont pas reconnus pour leurs capacités techniques et sont davantage associés à des profiteurs et des fraudeurs qu'à de vrais cybercriminels. L'arrestation d'un cybercriminel notoire ayant fait fortune à travers ses actes de piratage pourrait contribuer à faire connaître ce type de criminalité et ainsi possiblement diffuser les opportunités qui y sont rattachées. Le cas d'Alberto Gonzalez aux États-Unis aurait pu servir d'exemple étant donné la taille de la fraude (plusieurs dizaines de millions de numéros de cartes de crédit volés), mais sa possible association aux services secrets américains vient ternir sa réputation de pirate informatique criminel et laisse un doute sur la vraie histoire derrière ses actes de piratage. Il a

en effet soulevé lui-même le fait qu'il n'avait agi que pour le compte de ses employeurs qui désiraient qu'il continue ses crimes afin de pouvoir monter des dossiers contre d'autres criminels. Nous nous devons finalement de considérer parmi les hypothèses soulevées ici qu'il existe peut-être un plus grand nombre de cybercriminels que nous le pensons, mais que le chiffre noir associé à ce type de criminalité pourrait nous induire en erreur. Il n'existe en effet que très peu de données sur le phénomène des cybercrimes en raison de la réticence des victimes à porter plainte. Celles-ci peuvent légitimement penser que la police n'agira pas dans leur dossier et qu'il est donc inutile de faire une plainte officielle. Les victimes pourraient aussi avoir peur des répercussions d'une dénonciation à la police. Une banque qui avouerait un acte de piratage pourrait très bien voir ses clients transférer leurs comptes vers une institution en apparence plus sécuritaire. Les victimes peuvent aussi ne jamais se rendre compte qu'elles ont été victimisées et donc ne même pas être en mesure de prendre une décision éclairée sur le fait de faire une plainte ou non. En ne disposant que d'informations fragmentaires, il reste toujours problématique d'évaluer une menace telle que celle des cybercrimes.

Ce que nos trois articles ont tenté de démontrer est que la réputation est un capital virtuel qui peut et doit être utilisé pour comprendre la structure des réseaux ainsi que la position des individus. Nos recherches s'intéressent de près au domaine de l'analyse des réseaux sociaux; il semble maintenant être temps de passer à l'analyse des réseaux articulés autour de la réputation. Plutôt que de nous intéresser aux contacts directs et indirects, l'analyse de la réputation, particulièrement dans un contexte des technologies de l'information, nous semble des plus prometteuses, et ce, à trois niveaux. La réputation permet tout d'abord d'identifier les individus ayant le plus d'influence dans un réseau. Étant donné que la reconnaissance est reçue des autres membres d'une communauté, les personnes ayant le plus de réputation auront tissé de nombreux liens avec d'autres acteurs et seront à même de les rejoindre et de les influencer. Ces individus seraient aussi d'excellentes portes d'entrée pour collecter de l'information, voire même de diffuser de la fausse information cherchant à perturber un réseau. La prestance et l'importance de ces individus assureront une diffusion optimale. Dans un contexte d'enquête, une telle avenue serait très intéressante pour déstabiliser des réseaux criminels et planifier les attaques ciblées.

En plus de pouvoir identifier les personnes les plus influentes, la réputation nous permettrait aussi d'identifier les personnes les plus performantes d'un réseau. Nous avons vu dans notre revue de littérature que les individus ayant une réputation supérieure étaient en mesure d'exiger des prix plus élevés et de compléter un nombre plus grand de transactions. Cela a été confirmé dans notre troisième étude sur le carding qui indique que les individus qui arrivent à maximiser leur réputation bénéficient de plus d'opportunités criminelles que les autres. Ceux-ci profitent donc d'un avantage comparatif sur les autres. Ce n'est pas la première fois qu'un tel résultat est souligné. Décary-Hétu & Leppänen (à venir) ont aussi été en mesure de relier la notion de performance à la réputation dans une étude à venir. Finalement, notre premier article sur la scène des warez établissait une corrélation entre la productivité et la réputation.

Grâce aux systèmes automatisés de reconnaissance implantés dans plusieurs marchés illicites, il est maintenant possible de suivre à la trace l'évolution de la réputation des membres dans le temps. Notre recherche utilisant des analyses de survie à mesures répétées offre un guide pour quiconque aimerait comprendre l'évolution dans le temps de la réputation. Il serait donc possible de combiner des courbes de performance à des courbes de réputation afin de confirmer nos résultats de recherche voulant que la réputation entraine à la hausse le succès des criminels.

Les analyses de réseaux offrent déjà des outils informatiques et des concepts qui permettent de comprendre la structure des réseaux ainsi que la position des individus. Ceux-ci peuvent être déduits il est vrai en utilisant les liens sociaux. Nous proposons ici cependant d'étendre ces liens à la notion de réputation et d'intégrer cette notion aux études qui s'intéressent à la performance et au fonctionnement des réseaux criminels. Dans un milieu où le certain se mélange à l'incertain, la réputation est un des rares signaux auxquels les acteurs peuvent se fier.

Cette thèse est la première étape d'un long programme de recherche qui vise à mieux comprendre la criminalité dans son ensemble. Ce projet n'est ni novateur ni original. Il s'inspire en fait du concept de systèmes de délinquance introduit par Sutherland (1947) il y de cela plusieurs décennies. Bien moins connu que son Chapitre 4 portant sur l'association

différentielle, le Chapitre 13 de Sutherland est le cœur même de son projet de sociologie criminelle à l'américaine (Tremblay, 2011).

Sutherland y propose un guide pour les sociologues de la déviance désireux d'étudier certains types de déviance qui ont atteint une forme relativement développée d'organisation. Sutherland (1947) affirme qu'il est inutile d'utiliser les définitions légales (meurtre au premier degré, introduction par infraction) afin d'étudier la déviance. Celles-ci mélangent dans un même tout plusieurs comportements qui n'ont que des similitudes artificielles ou superficielles. Il faudrait plutôt chercher à identifier les unités sociologiques qui se trouvent derrière cette déviance. Ces systèmes de délinquance (ou unités sociologiques) permettent aux criminels de réduire leurs risques d'arrestation tout en maximisant l'atteinte de leurs objectifs. Ils structurent donc leurs activités afin de maximiser leurs gains et réduire leur risque d'arrestation. La question de l'efficacité du contrôle social tant formel qu'informel se pose donc entièrement ici. Sutherland (1947) est peu loquace lorsque vient le temps de définir ce qu'est un système de délinquance. Il propose tout de même trois caractéristiques qui permettent de les circonscrire : 1) le mode de vie des participants; 2) les traits communs et; 3) le sentiment d'appartenance.

Une des grandes forces de la théorie des systèmes de délinquance est la richesse des analyses qu'elle permet de développer. En effet, il ne s'agit pas ici de se limiter à tel ou tel aspect de la criminalité ou des criminels, mais plutôt d'en décortiquer les moindres subtilités. Les comportements criminels sont évidemment au cœur des analyses. Il est question ici de l'actualisation de la déviance. Un chercheur tentera donc de comprendre et de décrire la déviance qui est en jeu. S'arrêter là n'est cependant pas suffisant. Comme nous le mentionnions plus tôt, un même acte peut avoir plusieurs motifs ou cibles et il faut donc creuser plus loin, d'où l'énoncé de Sutherland (1947) qui indique qu'il faut s'attarder aux «codes, traditions, esprit de corps, relations sociales entre participants directs ainsi que la participation indirecte de plusieurs autres personnes». On reconnaît ici l'influence des associations différentielles qui affirment l'importance du transfert de savoir et des pairs criminels dans l'obtention d'une maturité criminelle. L'organisation sociale derrière les vols de voitures, par exemple, devient essentielle lorsque vient le temps d'analyser le phénomène. En effet, une fois le véhicule volé, le criminel se doit encore de trouver un moyen de

l'échanger contre de l'argent. Ce n'est qu'en faisant affaire avec d'autres criminels qu'il pourra y arriver (Tremblay, 2011). Afin d'entrer en contact avec eux, il devra prouver qu'il connaît les codes et traditions du milieu et qu'il n'est donc pas un agent de police. Il s'installera alors possiblement entre ces deux personnes un esprit de corps qui cimentera leur relation. À ce chapitre, Tremblay (2011) rappelle l'importance de la théorie des scripts de Cornish (1993) qui affirme qu'il est erroné de concevoir un acte criminel comme un évènement et qu'il faut plutôt le conceptualiser comme une histoire où plusieurs personnes et gestes se succèdent dans l'atteinte d'un objectif commun. Sutherland (1947) souhaite donc que la recherche tente d'identifier des systèmes de délinquances en se basant sur des actes criminels, mais sans pour autant laisser de côté le mode de vie de ses participants.

Pour qu'un système de délinquance apparaisse, il ne suffit pas d'avoir un certain nombre de criminels. Il faut aussi que ces criminels possèdent des traits communs au niveau de leurs comportements, de leurs motivations et de leurs cognitions. Un système de délinquance implique une transmission des connaissances entre les participants et cela entraîne une certaine homogénéité entre les membres qui tenteront d'adopter les techniques les plus efficaces. Nous devrions donc nous attendre à observer des actes illicites qui sont similaires et qui se reproduisent à des fréquences similaires. Évidemment, chaque criminel aura sa propre interprétation et sa façon de procéder qui s'adapte mieux à son style. Mais l'étude des systèmes de délinquance devra tenter d'identifier les traits communs qui unissent tous les participants d'un même système. Cela fera ressortir les motivations ainsi qu'encore plus d'informations sur le fonctionnement du système. Ces traits communs devraient aussi être étudiés afin de déterminer les mécanismes de diffusion de l'information dans le système. Il existe donc une boucle qui amène les participants d'un système à tendre vers une homogénéisation de leurs comportements. Le système permet de faire circuler les innovations et permet aux criminels d'évaluer leur efficacité. Ils voudront alors imiter les criminels les plus performants en adoptant les mêmes techniques qu'eux. Cette boucle sans fin ne serait cependant pas aussi forte sans le sentiment d'appartenance des criminels face à leur système.

Les participants à un système de délinquance éprouvent finalement un sentiment d'appartenance à ce système. Lorsque plusieurs participants se rencontrent, ils devraient éprouver un certain sentiment d'appartenance. Sutherland (1947) donne ici l'exemple d'un

fraudeur par chèque et d'un spécialiste de l'escroquerie. Les deux utilisent des techniques similaires et auront donc des intérêts et des façons de fonctionner qui se ressemblent. Ils pourraient donc faire partie d'un même système de délinquance. Un voleur de voiture et un prêteur sur gages n'auraient par contre que très peu de points communs (intérêts, standards) et ne ressentiraient donc aucune connexion entre eux.

Les systèmes de délinquance sont donc des foyers d'innovation et de création de criminalité. Sutherland (1947) mentionne que les fraudeurs dans les cirques se rassemblaient tous les hivers pour s'échanger leurs dernières innovations et ainsi augmenter leur productivité et réduire leur risque d'arrestation. Il existerait un savoir-faire qui serait enseigné dans chacun des systèmes de délinquance. L'objectif de l'étude d'un système de délinquance est donc multiple. Il s'agit tout d'abord de comprendre comment le système en est venu à exister pour ensuite comprendre comment il a évolué dans le temps. Ce faisant, nous pouvons aborder une multitude de questions qui touchent l'entrée des participants dans le système, les techniques qu'ils utilisent, les relations entre eux, etc. Le but ultime est de comprendre comment le système fonctionne. Selon Tremblay (2011), l'objectif de Sutherland serait d'arriver à une compréhension globale de la déviance en analysant un système de délinquance à la fois. Certaines caractéristiques communes pourraient ensuite être extraites de ces analyses afin de révéler la vraie nature de la déviance. Cette approche du bas vers le haut serait l'avenue à privilégier donc dans la recherche de l'explication de la déviance.

Cette thèse n'a fait que gratter la surface de trois systèmes de délinquance. Nous nous sommes intéressés avant tout au concept de réputation et comment celui-ci pouvait avoir un impact sur la performance criminelle. Dans le cas de la scène des warez, deux transformations majeures viennent bouleverser ce que nous pensions savoir de la scène. Tout d'abord, de nombreuses opérations policières ont, au cours des dernières années, mené à l'arrestation de membres très influents de cette communauté. Bien qu'il n'existe pas de leaders chez les pirates du warez, certaines personnes jouent le rôle de modèles pour les autres et leur absence pourrait avoir un impact certain sur la transmission des connaissances et l'organisation sociale de la scène. Par ailleurs, de plus en plus de services juridiques sont offerts pour permettre aux individus d'acheter et de louer à prix raisonnable de la propriété intellectuelle. Les succès de plateformes comme iTunes sont venus réduire l'attrait de la scène des warez pour les

consommateurs. Alors que les pirates jouissaient d'une certaine reconnaissance du public pour les produits qu'ils distribuaient, le fait que les détenteurs des droits ont maintenant mis en place des services qui répondent aux besoins des consommateurs vient diminuer l'importance de la scène des warez. Il sera intéressant d'étudier dans les prochaines années l'impact de ces deux transformations sur ce système de délinquance.

Au niveau des botnets, nous n'avons toujours pas été en mesure d'approfondir la notion de réussite. En effet, nous nous sommes limités à comprendre la distribution de la reconnaissance dans le contexte de cette forme particulière de crime. Des études futures devraient donc s'intéresser à la performance et à la réussite chez ces pirates informatiques. On devrait aussi consacrer plus de temps à mieux comprendre ces individus. Nous en savons toujours très peu sur les botmasters et notre compréhension de ce système de délinquance en souffre actuellement. L'acquisition de connaissances, le réseautage et la performance sont autant de sujets qui méritent plus que jamais notre attention.

Finalement, les cardeurs sont les criminels que nous avons le plus étudié dans cette thèse en lien avec la réputation. Nous ne nous sommes intéressés cependant qu'à une seule plateforme, et ce, pour une période d'observation relativement limitée. De meilleures études pourraient encore inclure plus de marchés d'origines et de langues diverses. Elles devraient aussi inclure des plateformes d'échanges qui sont protégées par des mots de passe et où l'accès est limité. Les criminels qui fréquentent de tels milieux devraient être parmi les plus performants et les plus réputés. En comprenant mieux leur développement et leurs façons d'opérer, nous serions alors en mesure de prévoir les tendances à long terme de ce type de criminalité. Le projet d'étude des systèmes de délinquance a débuté il y a de cela plusieurs décennies. Comme l'a si bien dit l'écrivain et poète Ralph W. Emerson, "Life is a journey, not a destination". Nous continuerons donc notre programme de recherche portant sur les systèmes de délinquance en espérant que notre chemin soit aussi fructueux que celui des auteurs qui nous ont précédés.

RÉFÉRENCES

ACC. (2011). “Card Fraud.” *Crime Profile Series Of The Australian Crime Commission*.

Akerlof, G. A. (1970). “The Market For Lemons: Quality Uncertainty And The Market Mechanism.” *The Quarterly Journal Of Economics*. 84(3): 488-500.

Alleyne, B. (2010). “Sociology Of Hackers Revisited.” *The Sociological Review*. 1-35.

Andersen, P. & R. Gill. (1982). “Cox's Regression Model For Counting Processes, A Large Sample Study.” *Annals of Statistics*. 10:1100-1120.

Anderson, E. (2000). *Code Of The Street*. New York, USA: W. W. Norton & Company.

Bächer, P. & T. Holz & M. Kotter & G. Wicherski. (2005). “Tracking Botnets: Using Honeynets To Learn More About Bots.” Retrieved on March 1st, 2013 from: http://www.honeynet.org/papers/bots/.

Banday, M. T. & J. A. Qadri & N. A. Shah. (2009). “Study Of Botnets And Their Threats To Internet Security.” *Sprouts: Working Papers On Information Systems*. 9(24): 2-12.

Barney, J. (1991). “Firm Resources And Sustained Competitive Advantage.” *Journal of Management*. 17: 99–120.

Beare, M. (2002). “Organized Corporate Criminality – Tobacco Smuggling Between Canada and The US.” *Crime, Law & Social Change*. 37: 225-243.

Beatty, R. P. (1989). “Reputation And The Pricing Of Initial Public Offerings.” *The Accounting Review*. 64(4): 693–709.

Becker, H. S. (1963). *Outsiders : Studies in the sociology of deviance*. New York, USA: Free Press.

Bergiel, B. J. & E. B. Bergiel & P. W. Balsmeier. (2008). ”Internet Cross Border Crime: A Growing Problem.” *Journal Of Website Promotion*. 3(3-4): 133-142.

Bhattacharjee, R. & A. Goel. (2005). “Avoiding Ballot Stuffing In eBay-Like Reputation Systems.” *Workshop On Economics Of Peer-To-Peer Systems*. Philadelphie, Pensylvannie.

Block-Lieb, S. (2002). “e-Reputation: Building Trust In Electronic Commerce.” *Louisiana Law Review*. 62: 1199–1219.

Boase, J. & B. Wellman. (2006). *Personal Relationships: On And Off The Internet*. DANS Vangelisti, A. L. & D. Perlman. (2006). *The Cambridge Handbook Of Personal Relationships*. Cambridge, UK: Cambridge University Press.

Bolton, G. E. & E. Katok & A. Ockenfels. (2004). “How Effective Are Electronic Reputation Mechanisms? An Experimental Investigation.” *Management Science*. 50(11): 1587–1602.

Boot, A. W. A. & S. I. Greenbaum & A. V. Thakor. (2006). “Reputation and Discretion in Financial Contracting.” *The American Economic Review*. 83(5): 1165–1183.

Borgaonkar, R. (2010). “An Analysis of the Asprox Botnet.” *Fourth International Conference On Emerging Threats*. Venise, Italie.

Borgatti, S.P., Everett, M.G. and Freeman, L.C. (2002). *Ucinet for Windows: Software for Social Network Analysis*. Harvard, USA: Analytic Technologies.

Bouchard, M. & H. Nguyen. (2009). “Is It Who You Know, Or How Many That Counts? Criminal Networks and Cost Avoidance In A Sample Of Young Offenders.” *Justice Quarterly*. 27(1): 130-158.

Bounie, D. & M. Bourreau & P. Waelbroeck. (2006). "Piracy and The Demand For Films: An Analysis Of Piracy Behavior In French Universities." *Review Of Economic Research On Copyright Issues*. 3(2): 15-27.

Bourdieu, P. (1972). *Outline Of A Theory Of Practice.* Cambridge, UK: Cambridge University Press.

Bourgois, P. I. (2002). “In Search Of Respect: Selling Crack In El Barrio.” Boston, USA: *Cambridge University Press*.

Boyd, M. (2008). *Botnets – An In-Dept Analysis*. Récupéré le 10 novembre 2011 au: http://www.scribd.com/doc/103915441/Botnets-an-in-Depth-Analysis.

Brenner, S. (2007). *Cyber Crime: Re-thinking Crime Control Strategies*. Dans Jewkes, Y. (Ed.). *Crime Online.* Portland, USA: Willan Publishing.

Bridy, A. (2009). “Why Pirates (Still) Won't Behave: Regulating P2P in the Decade After Napster.” *Rutgers Law Journal*. 565: 594-97.

Burt, R. S. (1992). *Structural Holes*. Cambridge, UK : Cambridge University Press.

Burt, R. S. (2005). *Brokerage and Closure: An Introduction to Social Capital*. Oxford, UK: Oxford University Press.

Burt, R. S. (2010). *Structural Holes In Virtual Worlds*. Papier de travail. University of Chicago, Booth School of Business. Chicago, USA.

Cadel, P. (2010). “Le marché de l’e-réputation: du positionnement fonctionnel aux enjeux technologiques.” *Les cahiers du numérique*. 6(4): 111–121.

Calce, M. & C. Silverman. (2008). *Mafiaboy : How I Cracked The Internet And Why It’s Still Broken*. Toronto, Canada: Viking Canada.

Camerer, C. & K. Weigelt. (1988). “Experimental Tests Of A Sequential Equilibrium Reputation Model.” *Econometrica*. 56(1): 1–36.

Campbell-Kelly, M (2009). “*Historical Reflections - The Rise, Fall, And Resurrection Of Software As A Service*.” Communications of the ACM. 52(5): 28–30.

Cárdenas, A. A. & S. Radosavac & J. Grossklags & J. Chuang & C. J. Hoofnagle. (2009). “An Economic Map Of Cybercrime.” *Working paper for the 37th Research Conference on Communication, Information and Internet Policy*. Arlington, VA.

Caves, R. E. (1980). “Industrial Organization, Corporate Strategy And Structure.” *Journal of Economic Literature.* 18: 64–92.

Charest, M. (2007). “Classe sociale et réussite criminelle.” Masters Thesis presented at the School of Criminology, University of Montreal.

Charette, Y. (2012). “La perception du prestige des occupations illicites par des criminels : une perspective sur les capitaux criminels.” Masters Thesis presented at the School of Criminology, University Of Montreal.

Chen, M. & J. P. Singh. (2001). “Computing And Using Reputations For Internet Ratings.” *Proceedings of the 3rd ACM conference on Electronic Commerce*. Tampa, USA.

Chen, T. M. & J.-M. Robert. (2005). *The Evolution of Viruses and Worms*. Dans Chen, W. W. S. (Ed.). *Statistical Methods In Computer Security*. New York, USA: CRC Press.

Chiang, E. & D. Assane. (2002). “Software Copyright Infringement Amongst College Students.” *Applied Economics*. 34(2): 157-166.

Choo, K. R. (2007). “Zombies And Botnets. Trends And Issues In Crime And Criminal Justice.” Retrieved on March 1st, 2013 from: http://www.aic.gov.au/en/publications/current%20series/tandi/321-340/tandi333/view%20paper.aspx.

Chu, B. & T. J. Holt & G. J. Ahn. (2010). “Examining The Creation, Distribution, And Function Of Malware On-Line.” Retrieved March 1st, 2013 from: http://www.ncjrs.gov./pdffiles1/nij/grants/230111.pdf.

CIPC. (2011). “The True Price Of Peer To Peer File-Sharing.” Récupéré le 3 janvier 2012 au:: http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Release_P2P_File-sharing_fr_110228.pdf.

Clark, R. V. (1997). *Situational Crime Prevention : Successful Case Studies 2nd edition.* Albany, USA: Harrow And Heston.

Coleman, J.S. (1988). "Social Capital In The Creation Of Human Capital." *American Journal of Sociology* (94: *Supplement: Organizations and Institutions: Sociological and Economic Approaches to the Analysis of Social Structure*). S95-S120.

Cooke, E. & F. Jahanian & D. McPherson. (2005). "The Zombie Roundup: Understanding, Detecting, And Disrupting Botnets." SRUTI '05 Workshop Proceedings. Berkeley, USA.

Cornish, D. (1994). *The Procedural Analysis Of Offending And Its Relevance For Situational Prevention*. Dans Clarke, R. V. *Crime Prevention Studies Volume 3*. NY, USA: Criminal Justice Press.

Craig, P. (2005). *Software Piracy Exposed*. Rockland, USA: Syngress.

Crandall, J. R. & Z. Su & S. F. Wu & F. T. Chong. (2005). "On Deriving Unknown Vulnerabilities From Zero-Day Polymorphic And Metamorphic Worm Exploits." *Proceedings Of The 12th ACM Conference On Computer And Communications Security*. New York, USA.

De Oliveira, K. C. (2008). *Botconomics: Mastering The Underground Economy Of Botnets.* Récupéré le 10 novembre 2011 au : http://www.cert.uy/documentos/pdf/botconomics.pdf.

Décary-Hétu, D. & A. Leppänen. (Forthcoming). "Criminals And Signals." Under review by the *Security Journal*.

Décary-Hétu, D. & B. Dupont. (2012). "The Social Network Of Hackers." *Global Crime*. 13(3): 160-175.

Décary-Hétu, D. & C. Morselli & S. Leman-Langlois (2012). "Welcome to the Scene: A Study of Social Organization and Recognition among Warez Hackers." *Journal Of Research On Crime And Delinquency*. 49: 359-382.

Densely, J. A. (2012). "The Organisation Of London's Street Gangs." *Global Crime.* 13(1): 42–64.

Deephouse, D. L. (2000). "Media Reputation as a Strategic Resource : An Integration of Mass Communication and Resource-Based Theories." *Journal Of Management.* 26(6): 1091–1112.

Demetriou, C. and A. Silke. (2003). "A Criminological Internet Sting: Experimental Evidence of Illegal and Deviant Visits to a Website Trap." *British Journal of Criminology*. 43: 213-222.

Di Gennaro, C. & W. H. Dutton. (2007). "Reconfiguring Friendships : Social Relationships And The Internet." *Information, Communication & Society*. 10(5): 591-618.

DIBR. (2010). "2010 Data Breach Investigations Report." Récupéré le 4 juillet 2012 au: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.

Doctorow, C. (2007). *Botnet Turf Wars*. Récupéré le 10 novembre 2011 au: http://boingboing.net/2007/05/14/botnet_turf_wars.html.

Dunham, K. (2008*). Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet*. Boca Raton, USA: Auerbach Publications.

Dunn, O. .J. (1961). “Multiple Comparisons Among Means.” *Journal Of The American Statistics Association*. *56: 52*–64.

Dupont, B. (2013), “Nouvelles technologies et crime désorganisé : incursion au cœur d’un réseau de pirates informatiques.“ *Sécurité & Stratégie*. 11 : 25-37.

Eck, J. (1993). “The Threat Of Crime Displacement.” *Problem Solving Quarterly.* 6(3): 1-2.

Emler, N. (2000). “La réputation sociale“. In S. Moscovici (Ed.), *Psychologie sociale des relations à autrui*. Paris, FR: *Nathan*.

Erbschloe, M. (2010). *Economic consequences*. Dans Ghosh, S. & E. Turrini. (Ed). *Cybercrimes: A Multidisciplinary Analysis.* Berlin, Allemagne: Springer.

Fallmann, H. & G. Wondracek & C. Platzer. (2010). “Covertly Probing Underground Economy Marketplaces.” *Proceedings Of The 7th International Conference On Detection Of Intrusions And Malware, And Vulnerability Assessment*. Bonn, Allemagne.

Farrington, D. P. (1986). “Age And Crime.” *Crime And Justice*. 7: 189-250.

Fischer, S. N. & M. Shinn & P. Shrout & S. Tsemberis. (2008). “Homelesness, Mental Illness, And Criminal Activity: Examining Patterns Over Time.” *American Journal Of Community Psychology*. 42: 251-265.

Ford, R. & S. Gordon. (2006). “Cent, Five Cent, Ten Cent, Dollar: Hitting Botnets Where It Really Hurts.” *Proceedings Of The Workshop On New Security Paradigms.* New York, USA.

Franklin, J. & V. Paxson. (2007). “An Inquiry Into The Nature And Causes Of The Wealth Of Internet Miscreants.” *Proceedings Of The Conference On Computer And Communications Security*. Alexandria, USA.

Freeman, L. C. (1977). “A Set Of Measures Of Centrality Based Upon Betweenness.” *Sociometry*. 40: 35–41.

Freeman, L. C. (1979). “Centrality In Social Networks: Conceptual Clarification.” *Social Network*. 1: 215:239.

Freeman, R. B. (1999). “The Economics Of Crime.” IN Ashenfelter, O. & D. Card. (1999). *Handbook Of Labor Economics, Volume 3*. Amsterdam, NL: North Holland.

Freiberg, A. (1997). “Regulating Markets For Stolen Property.” *Australian & New Zealand Journal Of Criminology.* 30: 237-258.

Friedman, E. J. & P. Resnick. (2001). “The Social Cost Of Cheap Pseudonyms.” *Journal of Economics & Management Strategy*. 10(2): 173–199.

Gambetta, D. (1993). “The Sicilian Mafia: The Business of Private Protection." MA, USA: *Harvard University Press*.

Gambetta, D. (2009). *Codes Of The Underworld: How Criminals Communicate.* New Jersey, USA: Princeton University Press.

Gaultier-Gaillard, S. & F. Pratlong. (2011). "Le risque de réputation : le cas du secteur bancaire." *Management & Avenir.* 8(48): 272–288.

Gendreau, P. & T. Little & C. Goggin. (1996). "A Meta-Analysis Of The Predictors Of Adult Offender Recidivism: What Works!" *Criminology.* 34(4): 575-607.

Glenny, M. (2011). *DarkMarket: How Hackers Became the New Mafia*. Toronto, CA: House Of Anansi Press.

Glückler, J. & T. Armbrüster. (2003). "Bridging Uncertainty In Management Consulting: The Mechanisms Of Trust And Networked Reputation." *Organization Studies*. 24(2): 269-297.

Gold, S. (2011). "Understanding The Hacker Psyche." Network Security. 2011(12): 15-17.

Goldman, E. (2004). *Warez Trading And Criminal Copyright Infringement*. Récupéré en ligne le 11 novembre 2010 au : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487163.

Goldman, E. (2005). "The Challenges of Regulating Warez Trading." *Social Science Computer Review*. 23(1): 24-28.

Goode, S. & S. Cruise. (2006). "What Motivates Software Crackers?" *Journal Of Business Ethics*. 65: 173-201.

Google. (2010). *Programme pilote*. Récupéré le 1er novembre 2012 au: http://www.google.com/chromeos/pilot-program.html.

Google. (2011). *Statistiques d'utilisation d'internet*. Récupéré le 10 novembre 2011 au : http://www.google.com/publicdata?ds=wb-wdi&met=it_net_user_p2&idim=country:CAN&dl=en&hl=en&q=internet+usage#met=it_net_user_p2&idim=country:CAN&tdim=true.

Gopal, R. D. & L. Sanders. (2000). "Global Software Piracy: You Can't Get Blood Out Of A Turnip." *Communications of the ACM*. 43(9): 83–89.

Gordon, S. (1994). "The Generic Virus Writer." *Presentation At The 4th International Virus Bulletin Conference*. Jersey, Angleterre.

Goudey, H. (2004). "Watch The Money Go Round, Watch The Malware Go Round." *Virus Bulletin Conference*. Chicago, USA.

Grabosky, P. (2007). *Electronic Crime*. Upper Saddle River, USA : Prentice Hall.

Granovetter, M.S. (1993). "The Strength Of Weak Ties." *American Journal of Sociology*. 78:6: 1360-1380.

Gutmann, P. (2007). "The Commercial Malware Industry." *DEFCON*. Las Vegas, USA.

Hackerspaces. (2011). Récupéré le 10 novembre 2011 au: http://hackerspaces.org/wiki/Hackerspaces.

Hagan, J. & B. McCarthy. (1997). *Mean Streets: Youth Crime And Homelessness*. Cambridge, UK: Cambridge University Press.

Hall, R. (1992). "The Strategic Analysis Of Intangible Resources." *Strategic Management Journal*. 13: 135–144.

Hanneman, R. A. & M. Riddle. (2005). "Introduction To Social Network Methods." Récupéré le 10 novembre 2012 au : http://faculty.ucr.edu/~hanneman/nettext/.

Hansen, D. E. (2008). "Knowledge Transfer In Online Learning Environments." Journal Of Marketing Education. 30(2): 93-105.

Herbig, P. & J. Milewicz. (1993). "The Relationship Of Reputation And Credibility To Brand Success." *Journal of Consumer Marketing.* 10(3): 18–24.

Herley, C. & D. Florencio. (2009) "Nobody Sells Gold For The Price Of Silver: Dishonesty, Uncertainty And The Underground Economy." Téléchargé le 4 juillet 2012 au: http://research.microsoft.com/pubs/80034/nobodysellsgoldforthepriceofsilver.pdf.

Hilley, S. (2006). "Case Analysis Of The Shadowcrew Carding Gang." *Computer Fraud & Security*. 2: 5.

Hinduja, S. (2001). "Correlates of Internet Software Piracy." *Journal of Contemporary Criminal Justice*. 17(4): 369-382.

Hinduja, S. (2003). "Trends And Patterns Among Online Software Pirates." *Ethics and Information Technology*. 5: 49-61.

Hinduja, S. (2007). "Neutralization Theory And Online Software Piracy: An Empirical Analysis." *Ethics and Information Technology*. 9(3): 187-204.

Holstege, S. (2010). "Western Union $94M Settlement Broadens Border States' Investigative Powers." Récupéré le 4 mai 2013 au : http://www.azcentral.com/news/articles/2010/02/11/20100211smuggling-money-western-union-arizona.html?nclick_check=1#ixzz2TzQITft2.

Holt, T. J. (2007). "Subcultural Evolution: Examining The Influence Of On- And Off- Line Experiences On Deviant Subcultures." *Deviant Behavior*. 28(2): 171-198.

Holt, T. J. (2008). *Lone Hacks Or Group Cracks: Examining The Social Organization Of Computer Hackers*. DANS Schmalleger, F. & M. Pittaro. (Ed.). *Crimes Of The Internet*. Upper Saddle River, USA: Prentice Hall.

Holt, T. J. & E. Lampke. (2010). "Exploring Stolen Data Markets Online: Products and Market Forces." *Criminal Justice Studies*. 23(1): 33-50.

Holt, T. J. & K. R. Blevins & N. Burkert. (2010). "Considering The Pedophile Subculture Online." *Sexual Abuse: A Journal Of Research And Treatment*. 22(1): 3-24.

Holt, T. J. (2012). "Exploring The Social Organization And Structure Of Stolen Data Markets." Social Science Computer Review. DOI: 10.1177/0894439312452998.

Holz, T. & M. Engelberth & F. Freiling. (2008). "Learning More About The Underground Economy: A Case-Study Of Keyloggers And Dropzones." *Lecture Notes In Computer Science*. 5789: 1-18.

Homans, G. C. (1958). "Social Behavior As Exchange." *American Journal Of Sociology*. 63(6), 597–606.

Houser, D. & J. Wooders. (2006). "Reputations In Auctions: Theory, And Evidence From eBay." *Journal Of Economics & Management Strategy*. 15(2): 353–369.

Ianelli, N. & A. Hackworth. (2005). "Botnets As A Vehicle For Online Crime." Pittsburgh, PA: CERT Coordination Center.

IFPI. 2011. "IFPI Digital Music Report 2011: Music at the Touch of a Button." Récupéré le 14 septembre 2011 au: http://www.ifpi.org/content/library/DMR2011.pdf.

Jarvenpaa, S. L. & N. Tractinsky & M. Vitale. (2000). "Consumer Trust In An Internet Store." *Information Technology And Management*. 1: 45–71.

Jordan, T. & P. Taylor. (1998). "A Sociology Of Hackers." *Sociological Review*. 46(4): 757-780.

Jøsang, A. & R. Ismail & C. Boyd. (2007). "A Survey Of Trust And Reputation Systems For Online Service Provision." *Decision Support Systems*. 43(2): 618–644.

Kaplan, E. L. & P. Meier. (1958). "Nonparametric Estimation From Incomplete Observations." *Journal Of American Statistics.* 53:457–481.

Khsetri, N. (2010). *The Golbal Cybercrime Industry: Economic, Institutional And Strategic Perspectives.* Berlin, Allemagne: Springer-Verlag.

Kini, R. & H. V. Ramakrishna & B. S. Vijayaraman. (2004). "Shaping of Moral Intensity Regarding Software Piracy: A Comparison between Thailand and U.S. Students." *Journal of Business Ethics*. 49: 91–104.

Kleinknecht, S. W. (2003). *Hacking Hackers: Ethnographic Insights into the Hacker Subculture-Definition, Ideology and Argot.* Mémoire de maitrise. Department Of Sociology, McMaster University.

Kotha, S. & S. Rajgopal & V. Rindova. (2000). “Reputation Building And Performance: An Empirical Analysis Of The Top-50 Pure Internet Firms.” *European Management Journal*. 19(6): 571–586.

Krebs, B. (2006a). *Bringing Botnets Out Of The Shadows*. Récupéré le 10 novembre 2011 au: http://www.washingtonpost.com/wp-dyn/content/article/2006/03/21/AR2006032100279.html.

Krebs, B. (2006b). *Invasion Of The Computer Snatchers*. Récupéré le 10 novembre 2011 au: http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html.

Krebs, B. (2010a). *Accused Mariposa Botnet Operators Sought Jobs At Spanish Security Firm*. Récupéré le 10 novembre 2011 au: http://krebsonsecurity.com/2010/05/accused-mariposa-botnet-operators-sought-jobs-at-spanish-security-firm/.

Krebs, B. (2010b). *Alleged Mariposa Botnet Author Nabbed*. Récupéré le 10 novembre 2011 au: http://krebsonsecurity.com/2010/07/alleged-mariposa-botnet-author-nabbed/.

Krebs, B. (2010c). *Fraud Bazaar Carders.cc Hacked.* Récupéré le 20 février 2011 au: http://krebsonsecurity.com/2010/05/fraud-bazaar-carders-cc-hacked/.

Krebs, B. (2011a). *Cultural CAPTCHAs*. Récupéré le 20 février 2012 au: http://krebsonsecurity.com/2011/09/cultural-captchas/.

Krebs, B. (2011b). *Is Your Computer Listed For Rent?* Récupéré le 10 novembre 2011 au: http://krebsonsecurity.com/2011/04/is-your-computer-listed-for-rent/.

Krebs, B. (2012a). *Cyberheists ‘A Helluva Wake-up Call’ to Small Biz.* Récupéré le 6 décembre 2012 au: http://krebsonsecurity.com/2012/11/cyberheists-a-helluva-wake-up-call-to-small-biz/.

Krebs, B. (2012b). *The Value Of A Hacked PC, Revisited.* Récupéré le 2 décembre 2012 au: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/.

Kruskall, W H & W. A. Wallis. (1952). “Use Of Ranks In One-Criterion Variance Analysis.” *Journal of the American Statistical Association*. 47(260): 583-621.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional And Strategic Perspective*. Berlin, Allemagne: Springer.

Ku, S. R. (2002). “The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology.” *The University of Chicago Law Review*. 69(1): 263-324.

Lai, G., & Y.-M. Siu. (2006). ”Residential Mobility And Social Capital In Urban Shanghai.” *Asian Journal of Social Science.* 34(4): 573–599.

Landon, S. & C. E. Smith. (1997). “The Use of Quality and Reputation Indicators By Consumers: The Case of Bordeaux Wine.” *Journal Of Consumer Policy*. 20(3): 289–323.

Lee, Z. (1998). “The Effect Of Negative Buyer Feedback On Prices In Internet Auction Markets.” Proceedings Of The Twenty First International Conference On Information Systems. Atlanta (USA).

Lee, J.-S. & H. Jeong & J. Park & M. Kim & B. Noh. (2008). “The Activity Analysis of Malicious HTTP-based Botnets using Degree of Periodic Repeatability.” *International Conference On Security Technology*. Hainan Island, Chine.

Leeson, P. & C. J. Coyne. (2005). “The Economics Of Computer Hacking.” *Journal Of Law, Economy And Policy*. 1(2): 511-532.

Leman, Langlois, S. 2004. “Theft in the Information Age.” *Knowledge, Technology & Policy*. 17(3-4): 140-163.

Levi, Michael. (2008). *The Phanton Capitalists.* Aldershot, UK: Ashgate Publishing Ltd.

Levitt, S. D. & S. A. Venkatesh. (2000). “An Economic Analysis Of A Drug-Selling Gang’s Finances.” *The Quarterly Journal Of Economics*. 115(3): 755-789.

Li, Z. & Q. Liao & A. Striegel. (2009) *Botnet Economics: Uncertainty Matters*. Dans Johnson, E. (Ed.). *Managing Information Risk And The Economics Of Security*. New York, USA: Springer.

Li, Z. & Q. Liao & A. Blaich & A. Striegel. (2010). “Fighting Botnets With Economic Uncertainty.” *Security And Communication Networks*. 4(10): 1104-1113.

Lucking-Reiley, D. & D. Bryan & D. Reeves. (2000). “Pennies From eBay: The Determinants Of Price In Online Auctions.” *The Journal Of Industrial Economics*. 55(2): 223-233.

Lunceford, B. (2009). “Building Hacker Collective Identity One Text Phile At A Time: Reading Phrack.” *Media History Monographs*. 11(2): 1-26.

Lyng, S. (2004). *Edgework: The Sociology Of Risk Taking*. New York, USA: Routledge.

Malik, Z. & A. Bouguettaya. (2009). “Reputation Bootstrapping For Trust Establishment Among Web Services.” *IEEE Internet Computing.* 13: 40–47.

Mann, D. & M. Sutton. (1998). “Netcrime : More Change In The Organization of Thieving.” *British Journal Of Criminology*. 38(2): 201-229.

Mantel, N. (1966). "Evaluation Of Survival Data And Two New Rank Order Statistics Arising In Its Consideration." *Cancer Chemotherapy Reports.* 50(3): 163–70.

Marshall, L. (2002). “Metallica and Morality: The Rhetorical Battleground of the Napster Wars.” *Entertainment Law*. 1(1): 1-19.

Marshall, A. (2006). “Causes, Effects and Solutions of Piracy in the Computer Software Market.” *Review of Economic Research on Copyright Issues*. 4(1): 63-86.

McCarthy, B. & J. Hagan. (2001). “When Crime Pays: Capital, Competence, And Criminal Success.” *Social Forces*. 79(3): 1035-1059.

McDonald, C. (1999). “Reputatuion In An Internet Auction Market.” *Economic Inquiry*. 40(4): 633-650.

McGuire, M. (2007). *Hypercrime: The New Geometry Of Harm*. New York, USA: Routledge Cavendish.

Mell, A. (2012). “Reputation In The Market For Stolen Data.” *Department Of Economics Discussion Paper Series*.

Melnik, M. & J. Alm. (2002). “Does A Seller’s E-Commerce Reputation Matter? Evidence From eBay Auctions.” *The Journal Of Industrial Economics*. L(3): 337-349.

Merton, R. K. (1938). “Social Structure And Anomie.” *American Sociological Review*. 3(5): 672-682.

Merton, R. K. (1968). “The Matthew Effect in Science.” *Science*. 159(3810): 56-63.

Mielke, C.J. & H. Chen. (2008). “Botnets, And The Cybercriminal Underground.” *Intelligence And Security Informatics Conference.* Taipei, Taiwan.

Milgrom, P. & J. Roberts. (1982). “Predation, Reputation And Entry Deterrence.” *Journal Of Economic Theory*. 27(2): 280–312.

Monsma, E. & V. Buskens & M. Soudijn & P. Nieuwbeerta. (2010). *Partners In Cybercime*. Mémoire de maitrise. Universiteit Utrecht.

Morselli, C. (2001). ”Structuring Mr. Nice: Entrepreneurial Opportunities And Brokerage Positioning In The Cannabis Trade.” *Crime, Law And Social Change*. 35(3): 203-244.

Morselli, C. & P. Tremblay. (2004). “Criminal Achievement, Offender Networks, And The Benefits Of Low Self-Control.” *Criminology*. 42(3): 773-804.

Morselli, C. & P. Tremblay & B. McCarthy. (2006). “Mentors And Criminal Achievement.” *Criminology*. 44(1): 17-43.

Morselli, Carlo. 2009. *Inside Criminal Networks*. New York, NY: Springer.

Motoyama, M. & D. McCoy & K. Levchenko & S. Savage & G. M. Voelker. (2011). “An Analysis Of Underground Forums.” *Proceedings Of The 2011 Conference On Internet Measurement Conference.* Berlin, Allemagne.

Mowery, D. C. & T. Simcoe. (2002). “Is The Internet a US Invention? An Economic And Technological History Of Computer Networking.” Research Policy. 31(8-9): 1369-1387.

Moxley, R. L. & N. F. Moxley. (1974). "Determining Point-Centrality In Uncontrived Social Networks." *Sociometry*. 37: 122-130.

Mui, L. & A. Halberstadt & M. Mohtashemi. (2002). "Notions Of Reputation In Multi-Agents Systems: A Review." *AAMAS*. Bologne, Italie.

Mui, L. & M. Mohtashemi & A. Halberstadt. (2002). "A Computational Model Of Trust And Reputation." *Proceedings Of The 35th Annual Hawaii International Conference On System Sciences*. Hawaii, USA.

Nagan, D. S. (1999). "Analyzing Developmental Trajectories: A Semiparametric, Group-Based Approach." *Psychological Methods*. 4(2): 139-157.

Nasi, M. & P. Rasanen & V. Lehdonvirta. (2004). "Identification With Online And Offline Communitites : Understanding ICT Disparities In Finland." *Technology In Society*. 33: 4-11.

Nazario, J. & T. Holz. (2008). "As The Net Churns: Fast-Flux Botnet Observations." *International Conference On Malicious And Unwanted Software*. Vandoeuvre-les-Nancy, France.

Nguyen, H. & M. Bouchard. (2011). "Need, Connections, Or Competence? Criminal Achievement Among Adolescent Offenders." *Justice Quaterly*.

Nycyk, M. (2010). "Computer Hackers In Virtual Community Forums: Identity Shaping And Dominating Other Hackers." Online Conference On Networks And Communities: Debating Communities And Networks. Perth, Australia.

Ollmann, G. (2008). "Hacking As A Service." Computer Fraud & Security. 12: 12-15.

Paquerot, M. et al. (2011). "L'e-réputation ou le renforcement de la gouvernance par le marché de l'hôtellerie?" *Management & Avenir*. 5(45) : 280-296.

Parsky, L. H. (2005). "Statement of Laura H. Parsky, Deputy Assistant Attorney General Criminal Division, Department of Justice, before the Subcommittee on oversight of Government Management, the Federal Workforce, and the District of Columbia Committee on Homeland Security and Governmental Affairs." Récupéré le 27 juin 2011 au: http://www.justice.gov/criminal/cybercrime/ParskyIPtestimony061405.htm.

Pastor-Satorras, R. and A. Vespignani. (2004). *Evolution And Structure Of The Internet*. Cambridge, USA: Cambridge University Press.

Patil, E. (2009). *Analysis Of Rxbot*. Mémoire de maitrise. San José State University.

Pearson, K. (1895). "Contributions To The Mathematical Theory Of Evolution." *Philosophical Transactions Of The Royal Society Of London*. 186: 343-414.

Peretti, K.K. (2008). “Data Breaches: What The Underground World Of Carding Reveals.” *Santa Clara Computer & High Tech Law Journal*. 25(2): 375-413.

Ponte, L. (2008). “Coming Attractions: Opportunities and Challenges in Thwarting Global Movie Piracy.” *American Business Law Journal*. 45(331) : 338-339.

Poulsen, Kevin. (2011). *Kingpin: How One Hacker Took Over The Billion-Dollar Cybercrime Underground*. New York, USA: Crown Publishing.

Prabowo, H. Y. (2011). “Building Our Defence Against Credit Credit Card Fraud: A Strategic View.” *Journal Of Money Laundering Control*. 14(4): 371-386.

Prell, C. K. & C. Hubacek. & C. Quinn, & M. Reed (2008). “Who’s In The Network? When Stakeholders Influence Data Analysis”, *Systemic Practice and Action Research*. 21(6): 443-458.

Putnam, R.D. (1993). "The Prosperous Community: Social Capital And Economic Growth." *Current*. 356: 4.

R Core Team. (2012). “R : A Language And Environment For Statistical Computing.” *R Foundation for statistical computing*. Vienna, Austria: Version 2.14.2.

Rahim, N. & A. Seyal & M. Rahman. (1999). “Software Piracy Amongst Tertiary Students In Brunei Darussalam: An Empirical Study.” *Proceedings of the Australian Institute of Computer Ethics Conference*. Melbourne, Australie.

Rajab, M. A. & J. Zarfoss & F. Monrose & A. Terzis. (2006). “A Multifaceted Approach To Understanding The Botnet Phenomenon.” IMC’06. 41- 52.

Rao, H. (2006). “The Social Construction Of Reputation: Certification Contests, Legitimation, And The Survival Of Organizations In The American Automobile Industry (1895–1912).” *Strategic Management Journal*. 15: 29–44.

Raub, W. & J. Weesie. (1990). “Reputation and Efficiency in Social Interactions : An Example of Network Effects.” *American Journal Of Sociology*. 96(3): 626–654.

Raudenbush, S.W. & A. S. Bryk & R. Congdon. (2004). *HLM 6 for Windows [Computer software]*. Skokie, USA: Scientific Software International, Inc.

Rehn, A. (2003). “The Politics Of Contraband: The Honor Economies Of The Warez Scene.” *Journal of Socio-Economics*. 33: 359-374.

Resnick, P. & R. Zeckhauser & E. Friedman & K. Kuwabara. (2000). “Reputation Systems.” *Communications Of The ACM*. 43(12): 45–48.

Resnick, P. & R. Zeckhauser. (2001). “Trust Among Strangers In Internet Transactions: Empirical Analysis Of eBay’s Reputation System.” *Volume Advances In Applied Microeconomics*. 11: 127–157.

Resnick, P. & R. Zeckhauser & J. Swanson & K. Lockwood. (2006). "The Value Of Reputation On eBay: A Controlled Experiment." *Experimental Economics*. 9(2): 79–101.

Reuter, P. (1983). "Disorganized Crime: The Economics of the Visible Hand." MA, USA: *M.I.T. Press*.

Reuter, P. & M. A. R. Kleiman. (1986). "Risks And Prices: An Economic Analysis Of Drug Enforcement." *Crime And Justice*. 7: 289-340.

Roberts, P. W. & G. R. Dowling. (2002). "Corporate Reputation And Sustained Superior Financial Performance." *Strategic Management Journal*. 23(12): 1077–1093.

Rogers, M. (1999). "A New Hackers' Taxonomy". Récupéré le 27 juin 2011 au: http://homes.cerias.purdue.edu/~mkr/hacker.doc.

Rossow, C. & C. J. Dietrich & N. Pohlmann. (2009). *Botnets – Literature Survey And Report*. Récupéré le 10 novembre 2011 au: http://www.internet-sicherheit.de/fileadmin/docs/publikationen/dietrich/Christian-Rossow-Christian-J.-Dietrich-Literature-survey-and-Report.pdf.

Rush, H. & C. Smith & E. Kraemer-Mbula & P. Tang. (2009). *Crime Online: Cybercrime And Illegal Innovation*. Rapport de recherche du NESTA. Récupéré le 8 novembre 2010 au : http://eprints.brighton.ac.uk/5800/1/Crime_Online.pdf.

Sabater, J. & C. Sierra. (2002). "Reputation And Social Network Analysis In Multi-Agent Systems." *Proceedings Of The Autonomous Agents and Multi-Agent Systems*. Bologne, Italie.

Saleem, S. A. (2006). "Ethical Hacking As A Risk Management Technique." *Proceedings Of The 3rd Annual Conference On Information Security Curriculum Development*. New York, USA.

Sauvadet, T. (2006). *Le capital guerrier: Concurrence et solidarité entre jeunes de cité [The Warrior Capital : Competition and solidarity between youths living in ghettos]*. Paris, France: Armand Colin.

Schell, B. & J. L. Dodge & S. S. Moutsatsos. (2002). *The Hacking Of America: Who's Doing It, Why And How*. Westport, USA: Quorom Books.

Schultz, J. R. (2005). *Warez Everyone Going: An Exploratory Look at Online Piracy*. Thèse de maitrise. College Of Business Administration, California State University.

Shadowserver Foundation. (2005). "Botnet Maps." Retrieved On July 13th 2012 on: http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetMaps.

Shane, S. & D. Cable. (2002). "Network Ties, Reputation, And The Financing Of New Ventures." *Management Science*. 48(3): 364–381.

Shapiro, C. (1983). “Premiums For High Quality Products As Returns To Reputations.” *The Quarterly Journal Of Economics*. 98(4): 659–680.

Sharma, R. (2007). *Peeping Into A Hacker’s Mind: Can Criminological Theories Explain Hacking?* Récupéré le 10 novembre 2011 au : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1000446.

Shimomura, T. (1996). *Take-Down: The Pursuit And Capture Of Kevin Mitnick, America’s Most Wanted Computer Outlaw – By The Man Who Did It.* New York, USA: Hyperion.

Shklovski, I. & R. Kraut & J. Cummings. (2008). “Keeping In Touch By Technology: Maintaining Friendships After A Residential Move.” *Proceedings Of The Twenty-Sixth Annual SIGCHI Conference On Human Factors In Computing Systems.* Chicago, USA.

Sims, R. & H. Cheng & H. Teegen. (1996). “Toward A Profile Of Student Software Piraters.” *Journal Of Business Ethics*. 15: 839-849.

Snijders, C. & R. Zijdeman. (2004). “Reputation and Internet Auctions : eBay and Beyond.” *Analyse und Kritik: Zeitschrift für Sozialtheorie*. *26*: 158–184.

Stone-Gross, B. & M. Cova & B. Gilbert & R. Kemmerer & C. Kruegel & G. Vigna. (2011). “Analysis Of A Botnet Takeover.” *Security & Privacy*. 9(1): 64-72.

Sullivan, R. J. (2010). “The Changing Nature Of U.S. Card Payment Fraud: Issues For Industry And Public Policy.” Récupéré le 4 juillet 2012 au: http://weis2010.econinfosec.org/papers/panel/weis2010_sullivan.pdf.

Sutherland, Edward H. (1947). “Principles of Criminology Fourth Edition.” Chicago, IL: J.B. Lippincott.

Standlee, A. (2009). *The Real “Virtual World” : Techno-Mediated Relationships In The Lives Of College Age Adults*. Projet de thèse. Département de Sociologie, Syracuse University.

Steffensmeier, D. J. (1986). *The Fence: In The Shadow Of Two Worlds*. Lanham, USA: Rowman & Littlefied Publishing Group.

Steffensmeier, J. & J. T. Ulmer. (2005). “Confessions Of A Dying Thief: Understanding Criminal Careers And Illegal Entreprise.” NJ, USA: *Transaction Publishers*.

Sterling, A. (2008). *World Copyright Law*. London, UK: Sweet & Maxwell.

Stickel, S. E. (2012). “Reputation And Performance Among Security Analysts.” *The Journal of Finance*. XLVII(5): 1811–1836.

Stum, D. L. (2001). “Maslow Revisited: Building The Employee Commitment Pyramid.” *Strategy & Leadership*. 29(4): 4-9.

Sutton, M. (1995). “Supply By Theft.” British Journal Of Criminology. 35(3): 400-416.

Symantec. (2008). *Symantec Report On The Underground Economy*. Récupéré le 10 novembre 2011 au : http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

Tan, S. J. (1999). "Strategies For Reducing Consumers' Risk Aversion In Internet Shopping." *Journal Of Consumer Marketing*. 16(2): 163–180.

Taylor, P. A. (1998). "Hackers: Cyberpunks Or Microsefs?" *Information, Communication & Society*. 1(4): 401-419.

Taylor, P. A. (2000). Hackers : Crime In The Digital Sublime. New York: USA: Routledge.

Thelwall, M. & K. Buckley & G. C. Paltoglou & A. Kappas. (2010). "Sentiments Strength Detection In Short Informal Text." *Journal of the American Society for Information Science and Technology*. 61(12): 2544–2558.

Thelwall, M. & K. Buckley & G. C. Paltoglou. (2012). "Sentiments Strength Detection For The Social Web." *Journal of the American Society for Information Science and Technology*. 63(1): 163-173.

Therneau, T. & P. Grambsch. (2000). *Modeling Survival Data: Extending the Cox Model*. Berlin, Germany: Springer-Verlag.

Therneau, T. (2012). "A Package for Survival Analysis in R." R package version 2.36-14.

Thomas, R. & J. Martin. (2006). "The Underground Economy: Priceless." *USENIX: Login.* 31(6): 7-16.

Topalli, V. & R. Wright & R. Fornango. (2002). "Drug Dealers, Robbery And Retaliation: Vulnerability, Deterrence And The Contagion Of Violence." *British Journal of Criminology*. 42: 337–351.

TopSite. 2010. "The Best NFO Sites On The Web." Retrieved June 27th 2010 (http://www.topsite.com/best/nfo).

Toral, S.L. & M.R. Martinez-Torres & F. Barrero. & F. Cortes. (2009). "An Empirical Study Of The Driving Forces Behind Online Communities." *Internet Research*. 19(4): 378-392.

Tremblay, P. & M. Bouchard & S. Petit. (2009). "The Size And Influence Of A Criminal Organization: A Criminal Achievement Perspective." *Global Crime*. 10: 1-2, 24-40.

Tremblay, P. (2011). *Le criminel idéal*. Montréal, CA : Éditions Liber.

UK Cards Association. (2012). "Annual Report 2012." Récupéré le 4 juillet 2012 au: http://www.buzzwordcreative.co.uk/UK-Cards-Annual-Report-2012/html/index.html.

Utz, S. (2007). “Media Use In Long-Distance Friendships.” *Information, Communication & Society*. 10(5): 694-713.

Van Duyne, P. (1996). “The Phantom And Threat Of Organized Crime.” *Crime, Law & Social Change*. 24 (4): 341–377.

Voiskounsky, A. and O. Smyslova. (2003). “Flow-Based Model of Computer Hackers' Motivation.” *Cyberpsychology and Behavior*. 6(2): 171-179.

Wall, D. (2007). *Cybercrime: The Transformation Of Crime In The Information Age*. Cambridge, Angleterre: Polity.

Wang, Q. & W. T. Yue & K. Hui. (2012). ”Do Hacker Forums Contribute To Security Attacks?” Lecture Notes In Business Information Processing. 108: 143-152.

Wasserman, S. & J. Galaskiewicz. (1994). *Advances In Social Network Analysis*. Thousands Oaks, USA: Sage Publications.

Wasserman, S. & K. Faust. (1994). *Social Network Analysis: Methods And Applications*. Cambridge, USA: Cambridge University Press.

Watts, D. J. 1999. “Networks, Dynamics And The Small World Phenomenon.” American Journal Of Sociology. 105: 493–592.

Wellman, B. (1999). *From Little Boxes To Loosely Bounded Networks: The Privatization And Domestication Of Community*. Dans Abu-Lughod, J. (1999). *Sociology For The Twenty-First Century: Continuities And Cutting Edges*. Chicago, USA: University Of Chicago Press.

Wellman, B. (2001). “Physical Place And Cyber Place: The Rise Of Personalized Networking.” *International Journal Of Urban And Regional Research*. 25(2): 227-252.

Wellman, B. (2002). “Little Boxes, Glocalization, And Networked Individualism.” Lecture Notes In Computer Science. 2362: 337-343.

Wellman, B. & J. Boase & W. Chen. (2002). “The Networked Nature Of Community: Online And Offline.” *IT & Society*. 1(1): 151-165.

Wellman, B. & A. Quan-Haase & J. Boase & W. Chen & K. Hampton & I. I. de Diaz & K. Miyata. (2003). “The Social Affordances Of The Internet For Networked Individualism.” *Journal Of Computer-Mediated Communications*. 8(3).

Wilhelm, T. (2009). *Professional Penetration Testing: Creating And Operating A Formal Hacking Lab*. Rockland, USA: Syngress.

Williams, R. J. & J. D. Barrett. (2000). “Corporate Philanthropy, Criminal Activity, and Firm Reputation: Is There a Link?” *Journal Of Business Ethics*. 26(4): 341-350.

Wired. (2001). “Prison Urged For Mafiaboy.” Récupéré le 4 juillet 2012 au : http://www.wired.com/politics/law/news/2001/06/44673.

Xiong, L. & L. Liu. (2003). “A Reputation-Based Trust Model For Peer-To-Peer eCommerce Communities.” *IEEE International Conference On E-Commerce*. Atlanta, USA.

Yip, M. (2011). “An Investigation Into Chinese Cybercrime And The Applicability Of Social Network Analysis.” *Proceedings Of The ACM Web Sciences*. Koblenz, Allemagne.

Zhu, Z. & Y. Chen & J. F. Zhi & P. Roberts & H. Keesook. (2008). “Botnet Research Survey.” *Annual IEEE International Computer Software and Applications Conference*. Turku, Finlande.