Université de Montréal

L'apprentissage social chez les pirates informatiques

Analyse de l'influence des relations d'entraide et de conflit sur le processus d'apprentissage

par Caroline Montégiani

École de Criminologie
Faculté des arts et des sciences

Travail dirigé présenté à la Faculté des études supérieures et postdoctorales
en vue de l'obtention du grade de Maître ès sciences (M. Sc.)
en criminologie
option Criminalistique et information

Août 2017

RÉSUMÉ

La technologie évolue à un rythme effréné depuis déjà plusieurs années, sans signe d'un quelconque ralentissement à venir. Avec la technologie, les techniques et les pratiques délinquantes associées au piratage informatique se développent également à la même vitesse. Ce faisant, afin de rester actuel dans leurs activités, les individus y participant se doivent de demeurer à l'affût des avancées dans le domaine et disposés à en faire l'apprentissage. Comme la littérature actuelle le mentionne, l'apprentissage est un processus fondamentalement social et les pirates informatiques forment une communauté qui repose sur le partage d'information et de connaissances. Plusieurs études ont abordé le processus d'apprentissage chez les délinquants et d'autres se sont penchées sur le processus de partage d'information au sein de la communauté des pirates informatiques. Toutefois, rares sont les études qui ont combiné les deux domaines afin d'essayer de comprendre le processus d'apprentissage qui s'opère dans la communauté des pirates informatiques par le biais du partage d'information.

Avec une méthodologie basée sur l'analyse de réseaux sociaux et un cadre théorique reposant sur les théories de l'association différentielle et de l'apprentissage social, cette étude s'intéresse donc à comprendre l'influence de l'entraide et des conflits sur le processus d'apprentissage social dans la communauté des pirates informatiques. Les analyses qui ont permis d'y parvenir ont été produites grâce à des données recueillies sur un forum de discussion en ligne. Les liens d'entraide et de conflit entre les participants ont été relevés afin d'en faire l'analyse, permettant ainsi d'observer que la communauté étudiée présentait des membres spécifiques qui concentrent les liens d'entraide et de conflit, faisant ainsi office de mentors ou de tyrans principaux et distribuant l'information (positive ou négative) de manière dispersée et à plusieurs destinataires différents. Cette recherche illustre donc la propension de la communauté des pirates informatiques à reposer sur les enseignements ou les critiques d'une minorité qui rejoindront une majorité d'acteurs.

Mots clés : Pirates informatiques, apprentissage social, association différentielle, entraide, conflit, analyse de réseaux sociaux.

ABSTRACT

Technology has evolved at an unprecedented pace for several years, with no sign of slowing down in the years to come. Likewise, delinquent techniques and practices associated with computer piracy and hacking are also developing at the same speed. Hence, in order to remain prevailing, the individuals involved in such activities must remain on the lookout for technological advances and must be willing to learn those new techniques. As scholars have stated before, learning is a fundamentally social process and hackers form a community that relies on sharing information and knowledge. Several studies have addressed the offenders learning process and others have addressed the process of information sharing within the hacker community. However, few studies have combined the two subjects to try and understand the learning process that is taking place within the hacker community through information sharing.

Using a methodology based on social network analysis and a theoretical framework based on theories of differential association and social learning, this study seeks to understand the influence of collaboration and conflict on the social learning process in the hacker community. The analyses that made it possible were produced using data from an on-line discussion forum from which the edges of mutual support and conflict between the participants were noted. The results of these analyses show that the observed community presents specific members that concentrate the links of mutual assistance and conflict thus serving as the main mentors or tyrants and distributing the information (positive or negative) in a dispersed way and to several recipients. This research therefore illustrates the propensity of the hacker community to rely on the teachings or criticism of a minority, that will reach a majority of actors.

Key words : Hackers, social learning, differential association, helping, conflicts, social network analysis.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

REMERCIEMENTS

Un travail de cette envergure est difficilement réalisable sans l'assistance et le soutien d'individus remarquables. Pour cette raison, je tiens tout d'abord à remercier mon directeur de recherche, David Décary-Hétu. Merci d'avoir vu un potentiel dans mon travail et pour tes connaissances sur le sujet que tu as su me partager tout au long du processus. Merci pour ta patience et ta compréhension lorsque j'avais du mal à respecter mes échéances, pour tes commentaires toujours justes et constructifs qui ont permis un travail d'une meilleure qualité, et surtout, merci pour ton soutien, ta confiance et ta disponibilité qui ont su calmer mes moments d'angoisse à quelques reprises!

Merci à ma famille qui était toujours présente pour moi. Vos encouragements et votre support m'ont été précieux dans la réalisation de ce travail et m'ont donné la force de persévérer jusqu'à la fin. Merci particulièrement à mes parents qui ont accepté ma réquisition de la table de cuisine comme bureau et qui n'ont jamais cessé de m'encourager et me supporter tout au long de ma scolarité, peu importe les projets que j'entreprenais.

Merci à mes amies pour leur compréhension et leur soutien lorsque je devais décliner des activités. Merci pour vos encouragements et votre présence tout au long de ce processus. Merci également à mes collègues devenues amies avec qui j'ai partagé une session d'étude incroyable en terre européenne. Chloé, Élodie et Félicia, vous avez fait de mon expérience à la maîtrise, l'une des plus belles de mon parcours scolaire et je garderai de très beaux souvenirs de vous toutes et de nos moments passés ensemble!

Enfin, je tiens absolument à remercier mon amie Maèva pour avoir cru en moi, quand même moi je n'y croyais plus. Merci d'avoir été présente pour moi tout au long de notre maîtrise. Merci d'avoir su rester positive et confiante quand j'étais découragée et prête à abandonner. Tu m'as donné la motivation nécessaire pour poursuivre le processus et venir à bout de ce travail. Merci pour tes conseils, pour ton support, pour ta disponibilité et pour ton écoute. Ton humour, ta passion et tes valeurs font de toi une amie précieuse et je remercie la vie de t'avoir mise sur mon chemin!

INTRODUCTION

Au cours des dernières décennies, l'essor de la technologie et l'arrivée d'internet ont modifié la manière dont les individus communiquent les uns avec les autres, notamment en réduisant les contraintes imposées par la distance physique et l'éloignement géographique. Toutefois, l'avènement d'internet n'a pas eu que des effets positifs. Effectivement, parallèlement au développement des technologies de l'information, il a été possible d'observer le déplacement de certains crimes vers la sphère virtuelle ainsi que l'apparition du phénomène de la cybercriminalité. Bien qu'étant une problématique de plus en plus actuelle, la cyberdélinquance demeure un concept particulièrement difficile à définir de manière concrète et exacte. Plusieurs auteurs se sont néanmoins intéressés au phénomène afin de parvenir à en qualifier les éléments qui le distingue des autres types de criminalité. Dans cet objectif, Wall (2007) propose une classification de trois types de délits considérés comme de la cybercriminalité. Cette typologie rassemble ainsi les délits qui menacent l'intégrité même des ordinateurs comme le piratage informatique ; ceux qui sont facilités par l'utilisation d'un ordinateur tels que le vol et la fraude ; ainsi que ceux qui se rapportent directement au contenu présent sur l'ordinateur comme la pornographie juvénile. D'ailleurs, le gouvernement canadien adhère visiblement à cette classification en définissant la cybercriminalité comme « une infraction criminelle ayant l'ordinateur pour objet (piratage informatique, hameçonnage, pollupostage) ou pour instrument de perpétration principal (pornographie juvénile, crime haineux, fraude informatique). » (Gouvernement du Canada, 2017). Faisant suite à cette montée des infractions impliquant la technologie, le Gouvernement du Canada a mis sur pieds la Loi sur la protection des Canadiens contre la cybercriminalité qui permet de réguler cette problématique (Gouvernement du Canada, 2014).

Par des actions de cyberdélinquance, les individus possédant les connaissances informatiques nécessaires peuvent tirer profits de leur savoir aux dépends d'individus plus vulnérables (Jeffray et Feakin, 2015). Toutefois, comme ces connaissances informatiques ne sont pas innées chez l'humain, elles doivent donc invariablement être apprises par l'individu qui veut les utiliser. De plus, la technologie étant un domaine qui évolue à très

grande vitesse, ceux possédant les connaissances préalables se doivent tout de même de demeurer à l'affût des nouvelles avancées et des nouvelles tendances dans le domaine. De cette manière, ils s'assureront de ne pas être dépassés dans leur pratique et de toujours conserver une longueur d'avance sur les techniques de détection employées par les autorités qui, elles aussi, évoluent au même rythme que la technologie. Afin d'acquérir un maximum de connaissances et demeurer dans un état d'apprentissage constant, il n'est pas rare de voir les hackers collaborer entre eux par le biais d'échanges d'information, de matériel, de connaissances et de techniques. Cela n'est pas sans rappeler la théorie de l'association différentielle de Sutherland (1947) qui expliquait la propension des délinquants à apprendre leur « métier » au contact de pairs plu expérimentés.

Le présent travail se veut donc une étude exploratoire du processus d'apprentissage permettant aux pirates informatiques d'acquérir les connaissances qui leurs seront nécessaires afin de commettre leurs actes de délinquance. À cette fin, ce document a été divisé en six chapitres distincts qui permettront d'aborder la question de la manière la plus complète possible. Tout d'abord, le premier chapitre fera état des connaissances existantes sur le sujet en dévoilant que les pirates informatiques sont des êtres sociaux qui communiquent majoritairement à l'aide de plateformes en ligne. Ce chapitre permettra également d'apprendre que les hackers forment une communauté basée principalement sur le partage d'information et qu'il n'est pas rare d'observer des collaborations entre ces derniers pour être en mesure de parvenir à leurs fins. Le second chapitre présentera le cadre théorique qui sous-tend l'ensemble de ce projet. Il y sera question de deux théories complémentaires concernant l'apprentissage chez les délinquants, soit la théorie de l'association différentielle qui explique que les délinquants apprennent les uns des autres, ainsi que de la théorie de l'apprentissage social qui renseigne sur la manière dont ces apprentissages s'effectuent. Par la suite, le troisième chapitre posera la problématique de recherche qui a poussé la réalisation de ce travail en énonçant les lacunes présentes dans la littérature actuelle au niveau des méthodologies utilisées et de la population difficile d'accès. C'est également dans cette section que les objectifs généraux et spécifiques de l'étude ainsi que les hypothèses qui y sont rattachées seront établis. Dans le quatrième chapitre, une description de la méthode de recherche sera proposée et une explication des

analyses effectuées sera faite. Il y sera question, entre autres, de la collecte de données à partir de forum de discussion en ligne et des mesures d'analyse de réseaux sociaux. Pour faire suite, le cinquième chapitre présentera les résultats obtenus grâce aux analyses de réseaux produites, alors que le sixième chapitre se voudra une discussion mettant en relation les résultats acquis et les éléments de la littérature ressortis dans les premiers chapitres. Pour conclure, une dernière section fera état de l'intégration, au sein du présent travail, de deux disciplines complémentaires, se nourrissant mutuellement de nouvelles connaissances, c'est-à-dire la criminologie et les sciences forensiques, notamment par l'utilisation marquée de traces numériques pour la réalisation de cette étude.

CHAPITRE 1 – RECENSION DES ÉCRITS

Le chapitre de la recension des écrits sera divisé en deux sections distinctes soit les cyberdéliquants et les sociabilités criminelles. La première section présentera un portrait des cyberdélinquants, plus particulièrement des pirates informatiques, ainsi que des compétences qui leur sont nécessaires pour la commission de leurs délits. La seconde section, pour sa part, fera état des connaissances actuelles concernant les sociabilités criminelles, notamment en définissant ce concept ainsi qu'en mettant en lumière les aspects sociaux du piratage informatique.

1.1 Les cyberdélinquants

1.1.1 Définition et communauté

Les cyberdélinquants sont aussi connus sous le terme de pirates informatiques, ou encore, selon l'appellation anglaise, *hackers*. Selon Shapiro (2003), la première utilisation du terme hacker, dans un contexte informatique, a été relevée dans la publication du 20 novembre 1963 du journal étudiant du Massachussetts Institute of Technologie, *The Tech*. L'article faisait état de hackers qui avaient accédé au réseau téléphonique de l'Institut et l'auraient utilisé sans autorisation préalable (Shapiro, 2003). Depuis cette époque et suite à l'essor de la technologie, bon nombre de chercheurs se sont intéressés au sujet du piratage informatique et ont tenté de décrire et définir les cyberdélinquants ainsi que leur communauté. Cependant, cette tâche s'avère plus complexe qu'il n'y paraît. Effectivement, étant donné son grand nombre d'acteurs aux comportements et motivations variés, cette catégorie de délinquant est, encore aujourd'hui, difficile à définir de manière adéquate (Décary-Hétu, 2013).

Dans son sens le plus large, tout individu qui accède à un système informatique sans autorisation préalable est considéré comme un cyberdélinquant (Sûreté du Québec, s. d.; Jordan et Taylor, 1998). Une classification bien connue des pirates informatiques divise cette communauté en deux groupes distincts : les *white hats* et les *black hats* (Crandall, Su, Wu et Chong, 2005). Bien que fondamentalement opposés quant à leur légitimité et leurs motivations, ces deux groupes n'en demeurent pas moins extrêmement semblables

(Kleinknecht, 2003 ; Décary-Hétu, 2013). Si les pirates blancs sont engagés par les compagnies afin de tester les mesures de sécurité informatiques et veiller à ce qu'aucune faille ne soit exploitable par des individus malveillants, il n'en demeure pas moins que, tout comme les pirates noirs, ces derniers ont pour objectif principal de trouver les vulnérabilités et les lacunes d'un réseau donné. Alors que les premiers le font pour pouvoir aider la compagnie qui les emploie à rendre leur système plus imperméable aux piratages et aux invasions extérieures ; les autres le font pour exploiter les failles découvertes à leur avantage, le plus souvent dans l'espoir d'en retirer un gain monétaire ou une meilleure réputation au sein de la communauté des pirates informatiques (Kleinknecht, 2003 ; Leeson et Coyne, 2005 ; Caldwell, 2011 ; Décary-Hétu, 2013 ; Lu, 2015 ; Dupont, Côté, Savine et Décary-Hétu, 2016).

D'autres auteurs parlent d'une dichotomie entre ceux qu'ils appellent les *crackers*, qu'il est possible d'associer aux black hats, et les *hackers*, qui se rapprochent davantage des white hats (Barber, 2001 ; Sehn, 2002 ; Raymond, 2003 ; Mitnick et Simon, 2011 ; eduCBA, 2016). Certains ajoutent également à cette typologie les *scripts kiddies*, désignant des jeunes pirates informatiques qui, étant dépourvus de compétences dans le domaine, tirent profit du travail d'autrui et utilisent leurs programmes à des fins malveillantes (Barber, 2001 ; Décary-Hétu, 2013). Dans le même ordre d'idées, les crackers sont considérés comme des individus amoraux dont l'objectif principal est la destruction. Ces derniers sont réputés pour avoir des intentions malicieuses et chercher à causer du tort à leurs cibles. De l'autre côté, toujours selon cette classification, les hackers sont reconnus comme des individus aux connaissances poussées en informatique qui s'intéressent à comprendre le fonctionnement des systèmes et à créer leurs propres programmes et outils. Ces derniers, dont la tâche principale vise à identifier les failles des systèmes afin d'être en mesure de les améliorer, sont vu comme ayant une grande éthique de travail (Barber, 2001 ; Sehn, 2002 ; Raymond, 2003 ; eduCBA, 2016). Cependant, il n'est pas rare, aujourd'hui, de voir dans les médias le terme *hacker* utilisé sans discernement pour définir ces deux groupes. C'est pourquoi la terminologie de *black hats* et *white hats* sera préconisée dans le présent travail lorsque la distinction sera nécessaire.

Dans l'imaginaire collectif, les hackers sont souvent perçus comme des «pimply-faced 14-year-old kids (mostly male) with anti-social tendencies and an addiction to Sci-Fi» (Barber, 2001). Ils sont considérés comme ayant des compétences informatiques extraordinaires ainsi qu'une aisance à pénétrer dans n'importe quel système informatique et ce, peu importe le niveau de sécurité du système en question (Barber, 2001). Or, la réalité n'est pas exactement conforme à cette image. Jordan et Taylor (1998) ont publié l'un des premiers articles encore cité aujourd'hui faisant une sociologie des pirates informatiques dans lequel ils présentent les facteurs internes et externes qui permettent de caractériser cette communauté. Dans ce contexte, les membres sont rarement directement en contact les uns avec les autres, comme c'est le cas dans les communautés plus traditionnelles, et c'est pourquoi, le concept de la communauté est vu comme une identité collective construite par les membres du groupe social autour d'une thématique commune, soit l'intérêt pour le piratage informatique (Jordan et Taylor, 1998).

Bien que datant de près de 20 ans, cette sociologie mentionne des caractéristiques qui sont, pour la plupart, encore d'actualité aujourd'hui, et qui ont été reprises par de nombreux autres auteurs depuis. Tout d'abord, il a été constaté que cette communauté, créée et maintenue par les hackers, entretient une relation aisée, quoique parfois accaparante, avec la technologie (Jordan et Taylor, 1998). Cette caractéristique a d'ailleurs été corroborée par de nombreux auteurs au fil du temps. Les hackers sont effectivement reconnus comme étant des individus éduqués et intelligents dont les compétences informatiques ne sont plus à prouver (Bachmann et Corzine, 2010). Ces derniers possèdent généralement une grande compréhension des différents concepts qui sous-tendent la programmation informatique et sont à même de mettre sur pieds leurs propres outils (Barber, 2001 ; Raymond, 2003 ; Choo, 2008).

La seconde caractéristique de cette communauté concerne la relation particulière qu'entretiennent les pirates informatiques à l'égard de la notion de secret (Jordan et Taylor, 1998). Cette relation se définit par une tension, chez le hacker, entre le besoin de conserver ses actes illégaux hors de la vue des autorités, tout en les exposant à la vue de ses pairs et du grand public. D'ailleurs, le partage d'informations et de connaissances, ainsi que la

volonté d'obtenir la reconnaissance de ses pairs, ont été identifiés à plusieurs reprises comme des caractéristiques représentatives de la communauté des hackers (Raymond, 2003 ; Holt, Strumsky, Smirnova et Kilger, 2012 ; Décary-Hétu, 2013 ; Abbasi, Li, Benjamin, Hu et Chen, 2014 ; Dupont, Côté, Savine, Décary-Hétu, 2016). Effectivement, la réputation et la reconnaissance des pairs est un élément primordial pour un hacker, devenant même, pour certains, la motivation première de leurs activités de piratage informatique (Leeson et Coyne, 2005). C'est d'ailleurs le cas pour les pirates informatiques impliqués dans la fraude de propriété intellectuelle en ligne, c'est-à-dire la scène des warez. Dans ce contexte, les hackers, qui évoluent majoritairement en groupe, ont pour objectif de distribuer le plus grand nombre de fichiers piratés afin de récolter le plus de reconnaissance de la part de leurs pairs (Décary-Hétu, Morselli et Leman-Langlois, 2012). Pour la communauté des pirates informatiques, la réputation est un élément particulièrement important au niveau de la reconnaissance. Effectivement, les hackers ayant la meilleure réputation auront tendance à être considérés avec plus d'égard et de respect au sein de la communauté, entraînant, pour ces derniers, des avantages non négligeables (Holt, Strumsky, Smirnova et Kilger, 2012 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). D'un autre côté, cette volonté d'être reconnu pour leurs activités illégales entraîne le risque d'une plus grande visibilité aux yeux des autorités. Afin d'être prolifique, les hackers doivent donc être en mesure de combiner ce besoin de publicité et la nécessité de garder le secret sur leurs activités illégales (Jordan et Taylor, 1998 ; Décary-Hétu, 2013).

D'ailleurs, dans l'espoir de pallier légèrement à cette tension, la communauté des hackers entretient également une relation particulière avec la notion d'anonymat (Jordan et Taylor, 1998 ; Décary-Hétu, 2013 ; Coleman, 2014 ; Jeffray et Feakin, 2015). Bien que fortement lié au concept de secret, l'anonymat s'en distingue au niveau de l'objet dissimulé. Si le secret fait référence au fait de conserver l'acte de piratage invisible aux yeux des autorités, l'anonymat signifie de camoufler l'identité du pirate. Pour ce faire, les hackers utilisent diverses méthodes comme l'emploi de pseudonymes afin de signer leurs actes, permettant que ceux-ci leur soient associés tout en protégeant leur identité (Jordan et Taylor, 1998), ainsi que la navigation privée par le biais de réseaux privés virtuels (VPN), permettant de couvrir leurs activités en ligne (Choo, 2008). D'ailleurs, la propension à l'anonymat chez

les hackers est décriée par de nombreux auteurs puisqu'elle rend cette communauté particulièrement difficile à étudier (Jordan et Taylor, 1998 ; Coleman, 2014). Dans son ouvrage sur le groupe de hackers activistes (des «hacktivistes») *Anonymous*, Coleman (2014) pousse la réflexion sur le sujet, rejetant l'idée selon laquelle la recherche d'anonymat chez les pirates informatiques servirait l'objectif de nier la responsabilité de leurs actes. Au contraire, elle affirme que, pour ces individus, rester anonyme n'est pas une coquille les protégeant de l'imputabilité, mais plutôt un cadre leur permettant d'agir (Coleman, 2014).

Une des conséquences notables du caractère anonyme et secret du piratage informatique est la fluidité des membres qui composent sa communauté. Les relations interpersonnelles à l'ère d'internet diffèrent effectivement de celles qui existent hors ligne de par leur nature éphémère et la faiblesse des liens qui unissent les individus entre eux (Jordan et Taylor, 1998 ; Décary-Hétu, 2013 ; Abbasi, Li, Benjamin, Hu et Chen, 2014 ; Coleman, 2014). Cette communauté, à l'instar de nombreux mouvements sociaux, est constituée d'un réseau informel aux frontières assez perméables. Contrairement aux organisations plus officielles, il n'existe aucune cérémonie ni coutume à respecter afin de devenir un hacker et donc, il est aisé pour un individu de devenir membre de cette communauté ou de la quitter. D'ailleurs, l'utilisation de pseudonymes simplifie grandement la tâche aux pirates qui désirent blanchir leur réputation. Comme les relations en ligne sont plutôt superficielles et que les individus n'échangent que très rarement des informations personnelles, ces derniers n'ont qu'à changer de surnom et ils pourront ainsi repartir avec une ardoise vierge sans risque d'être reliés à leur identifiant précédent (Craig, 2005, cité dans Décary-Hétu, 2013). Enfin, le caractère informel et la nature réseautée de la communauté des pirates informatiques, combinés à l'aspect illégal des actes posés ainsi que l'anonymat caractérisant leurs relations sociales, entraînent un roulement important chez les membres de cette communauté (Jordan et Taylor, 1998 ; Décary-Hétu, 2013 ; Coleman, 2014).

Finalement, un dernier élément qui a été soulevé dans la littérature comme étant caractéristique de cette communauté réside dans leur manière de penser. Effectivement, plusieurs auteurs considèrent que c'est la mentalité des pirates informatiques et leur

manière d'aborder les problèmes qui soudent cette communauté et leur donnent une identité commune (Jordan et Taylor, 1998 ; Barber, 2001 ; Raymond, 2003 ; Caldwell, 2011 ; Holt, Strumsky, Smirnova et Kilger, 2012 ; Décary-Hétu, 2013 ; Coleman, 2014 ; Zhang, Tsang, Yue et Chau, 2015). Les pirates informatiques sont majoritairement reconnus pour leur propension à valoriser l'apprentissage autonome, mais également leur penchant pour le partage d'informations. Raymond (2003) explique bien ce phénomène lorsqu'il mentionne qu'un hacker envisage le monde qui l'entoure comme étant rempli de problèmes fascinants qui n'attendent qu'à être résolus, mais qu'aucun de ces problèmes ne devrait avoir à être résolu deux fois. Pour cette raison, il n'est pas rare de voir un hacker ayant trouvé une solution à un problème, partager cette dernière avec la communauté des pirates informatiques, afin que les autres membres puissent utiliser leur temps à résoudre de nouvelles problématiques. D'ailleurs, cette curiosité caractéristique des hackers est souvent considérée comme l'une des motivations premières poussant un individu à s'engager dans des activités de piratage informatique (Jordan et Taylor, 1998 ; Barber, 2001 ; Raymond, 2003). Finalement, tous les facteurs identifiés dans la présente section permettent aux hackers d'avoir un langage commun, des ressources par lesquelles ils peuvent se reconnaître entre eux ainsi que des moyens pour les nouveaux venus de se joindre à la communauté.

1.1.2 Méthodes et compétences requises pour être un pirate informatique

Si l'objectif général d'accéder à un système informatique sans autorisation préalable est le même pour chaque attaque, les méthodes utilisées par les cyberdélinquants pour y parvenir sont, pour leur part, extrêmement variées. Pour le bien du présent travail, ces méthodes seront divisées en deux types : les méthodes dites sociales, aussi connues sous le terme d'ingénierie sociale (*social engineering*), et les méthodes techniques, c'est-à-dire, celles basées sur l'utilisations de logiciels et de failles de sécurité. Souvent, les hackers les plus expérimentés utiliseront une combinaison de ces méthodes dans des proportions qui varieront en fonction de la cible ou encore du dessein de l'attaque. Aussi, afin de bien comprendre les pirates informatiques, une bonne compréhension de ces deux types de méthodes est primordiale. C'est pourquoi la présente section détaillera chacune de ces

méthodes et présentera les compétences requises chez un hacker voulant les utiliser. Cependant, il est important de noter que, pour la poursuite de ce travail, une attention particulière sera accordée aux méthodes techniques de piratage informatique.

Ingénierie sociale

L'ingénierie sociale a été le sujet d'intérêt de nombreux auteurs au fil des ans et, bien que chacun en présente une définition légèrement personnalisée, tous s'entendent pour dire qu'elle repose sur l'utilisation délibérée de techniques de persuasion et de manipulation afin de prendre avantage d'une cible et d'obtenir des informations désirées (Casalegno, 2005 ; Peltier, 2006 ; Mitnick et Simon, 2011 ; Samani et McFarland, 2015 ; Fan, Lwakatare et Rong, 2017 ; The Social Engineering Framework, 2017). Bien que peu considérée dans l'imaginaire commun lorsqu'il est question de piratage informatique, l'ingénierie sociale n'en demeure pas moins une portion fondamentale et, bien souvent, la méthode la plus fructueuse (Jordan et Taylor, 1998). Effectivement, bon nombre d'auteurs identifient l'humain comme étant le maillon le plus faible d'un système de sécurité. Ce faisant, il est habituellement beaucoup plus aisé pour un hacker de convaincre une proie de lui fournir l'information qu'il recherche plutôt que de développer les outils informatiques qui lui seraient nécessaires pour l'obtenir (Peltier, 2006 ; Mitnick et Simon, 2011 ; Cheung, 2012 ; Fan, Lwakatare et Rong, 2017).

Contrairement à un appareil électronique doté d'un antivirus, l'humain est muni d'un libre arbitre lui permettant de choisir d'appliquer, ou non, les mesures et les normes de sécurité nécessaires à la protection d'un système d'information. De ce fait, un humain devra toujours analyser la situation à laquelle il fait face et prendre la décision volontaire de s'en tenir aux mesures sécurité mises en place ou de les ignorer. À ce propos, la volonté d'aider son prochain, la tendance à faire confiance à autrui, la peur d'offenser l'autre ainsi que la tendance à tourner les coins ronds ont été identifiées dans la littérature comme des attitudes, propres à l'humain, le rendant vulnérable aux attaques d'ingénierie sociale (Peltier, 2006 ; Cheung, 2012). Ces caractéristiques diminuent alors la méfiance dont un individu fait preuve envers autrui, l'amenant à baisser sa garde et à en faire une cible de choix. Il est à noter que ces attaques ne seront pas détaillées davantage puisque, comme il a été mentionné

précédemment, le présent travail s'intéresse davantage aux méthodes techniques ainsi qu'à leur apprentissage par les pirates informatiques qu'aux méthodes d'ingénierie sociale. C'est pourquoi la prochaine section sera consacrée à ces méthodes techniques et aux compétences requises pour les utiliser.

Méthodes de piratage techniques

Les méthodes de piratage techniques sont celles basées sur l'utilisation de logiciels malveillants et de failles de sécurité dans les systèmes d'exploitation et les logiciels, afin de pénétrer dans des systèmes inaccessibles à l'origine (Fan, Lwakatare et Rong, 2017). Tout comme c'était le cas pour les méthodes d'ingénierie sociale, celles-ci sont très variées et leur utilisation dépend des compétences, des préférences et de l'objectif du pirate informatique, ainsi que du niveau de protection de la cible visée. Les activités des hackers sont extrêmement diversifiées, allant de la fraude de carte de crédit au vol de propriété intellectuelle, en passant par l'activisme en ligne et la prise de contrôle d'appareil à distance (Décary-Hétu, 2013). Toutefois, dans le cadre du présent travail, l'intérêt sera porté sur les pirates s'attaquant à des systèmes d'informations sécurisés. Pour ce faire, trois modes d'opération distincts peuvent être utilisés par ces pirates pour parvenir à leurs fins : déjouer le système d'authentification en obtenant frauduleusement des identifiants, contourner ce système afin d'éviter l'identification ou encore, le bloquer afin d'empêcher quiconque d'accéder aux informations.

Les pirates qui exécutent le premier type d'attaque le font habituellement dans l'objectif de franchir les systèmes d'identification en devinant le mot de passe d'un utilisateur afin d'en usurper l'identité. Pour y parvenir, l'une des méthodes les plus simples et les plus utilisées par les pirates informatiques est celle des attaques par force brute. Ces attaques reposent sur la capacité du pirate à essayer, une à une, toutes les combinaisons possibles pour un mot de passe afin de trouver celle qui fonctionne. Cette technique, théoriquement infaillible, demande toutefois un temps d'exécution qui est non négligeable et exponentiellement proportionnel à la longueur de l'élément à deviner (Raza, Iqbal, Sharif et Haider, 2012). En effet, en considérant qu'un mot de passe est composé uniquement de lettres minuscules, les possibilités à tester lors d'une attaque par force brute sont de 26^n, où

n correspond au nombre de lettres dans le mot de passe (c'est-à-dire que pour un mot de passe d'une lettre, il existe 26^1=26 possibilités, mais que pour un mot de passe de 5 lettres, il en existe 26^5=11 881 376). Si, aux lettres minuscules, s'ajoutent des lettres majuscules, des chiffres et d'autres types de caractères, alors le nombre de possibilités se voit rapidement décuplé (Raza, Iqbal, Sharif et Haider, 2012). De ce fait, cette technique devient rapidement inutilisable et, pour cette raison, la plupart des pirates qui l'utilisent la combine avec d'autres techniques, permettant ainsi d'en diminuer le temps d'exécution et d'en augmenter l'efficacité. Une autre technique populaire chez les pirates informatiques est celle du *password sniffing*. Cette méthode implique que le hacker s'infiltre dans un réseau et surveille les activités qui s'y déroulent afin de collecter les données non cryptées qui sont transmises, plus précisément les mots de passe non sécurisés. Une fois le mot de passe enregistré, le pirate peut s'en servir selon le dessein voulu (De Vivo, De Vivo et Isern, 1998).

Le second mode d'attaque consiste à contourner les contrôles d'accès par l'utilisation de failles de sécurité, permettant au pirate de s'infiltrer dans le système sans en être un utilisateur. Pour ce faire, une technique très populaire chez les hackers consiste à exploiter des failles de sécurité d'une application interagissant avec une base de données (Su et Wassermann, 2006). Cette technique permet d'injecter, dans la requête envoyée au système d'informations, un morceau de requête non prévu par ce dernier afin d'en changer la logique, la sémantique ou la syntaxe, permettant ainsi d'en compromettre la sécurité (Halfond et Orso, 2005 ; Su et Wassermann, 2006). Plus concrètement, avec cette technique, un pirate viendra modifier une requête existante afin qu'elle effectue une action inattendue telle qu'afficher des données cachées, écraser des valeurs importantes, ou encore exécuter des commandes dangereuses pour la base de données (The PHP Group, 2017). Le mécanisme le plus souvent utilisé afin d'introduire des énoncés malveillants dans une application vulnérable est sans doute l'injection par l'entrée de l'utilisateur. Pour ce faire, le pirate repère une faille dans la page d'identification d'une application et se sert de la case d'entrée de l'utilisateur afin d'y injecter son code (Halfond, Viegas et Orso, 2006). De cette manière, le pirate peut avoir accès aux informations qu'il désire, tout en contournant les contrôles d'accès et d'identification mis en place.

Enfin, la troisième méthode consiste à empêcher l'accès aux données et rendre un service indisponible pour ses utilisateurs pour une période prédéterminée. Pour ce faire, les pirates peuvent utiliser des techniques telles que les attaques par déni de service (plus connu sous leur acronyme anglophone DoS pour *Denial of Service*) ou encore par déni de service distribué (DDoS pour *Distributed Denial of Service*). Une distinction est faite entre ces deux types d'attaques au niveau du nombre d'appareils impliqués. Si l'attaque par déni de service distribué utilise plusieurs appareils simultanément afin de lancer l'offensive contre une cible, l'attaque par déni de service n'en utilise qu'un seul, rendant cette dernière moins efficace et moins puissante (Mirkovic et Reiher, 2004). Par ces attaques, un pirate peut bloquer un serveur de fichier, rendre impossible la connexion à un serveur web, ou encore, empêcher la distribution de courriel dans une entreprise. Aujourd'hui, la grande majorité des attaques par déni de service distribué sont effectuées à l'aide de *botnets* (des réseaux d'ordinateurs infectés et contrôlés à distance par un pirate informatique), permettant ainsi d'en multiplier les sources. Ainsi, dû au nombre important de zombies (ordinateurs infectés) impliqués dans l'attaque et de leur situation géographique très étendue, il devient de plus en plus fastidieux pour une cible de se protéger contre de telles attaques (Sachdeva, Singh, Kumar et Singh, 2010).

Compte tenu de ce bref aperçu des activités d'un hacker et des techniques auxquelles ce dernier peut avoir recours, il ressort que, pour être prolifique, il est préférable pour un pirate informatique de présenter certaines caractéristiques et posséder certaines compétences bien spécifiques. À ce propos, il se dégage de la littérature qu'une majorité des pirates présentent des prédispositions telles qu'une curiosité pour le monde qui les entoure, une capacité d'apprentissage autonome, une volonté de partage de leurs connaissances, un certain refus de l'autorité ainsi qu'une bonne base en programmation informatique (Jordan et Taylor, 1998 ; Barber, 2001 ; Raymond, 2003 ; Choo, 2008 ; Décary-Hétu, 2013 ; Coleman, 2014 ; Zhang, Tsang, Yue et Chau, 2015). Comme évoqué précédemment, bon nombre de hackers voient le monde qui les entoure comme regorgeant de problèmes qui n'attendent qu'à être résolus. Ces derniers ressentent un certain enthousiasme à résoudre des problèmes, aiguiser leurs compétences et exercer leur intelligence (Barber, 2001 ; Raymond, 2003). Cela vient

rejoindre la seconde attitude observée chez les hackers, c'est-à-dire que ces derniers possèdent une bonne capacité d'apprentissage autonome. Effectivement, bien que les pirates ne soient pas nécessairement pourvus de toutes les connaissances nécessaires à la résolution d'un problème au départ, ces derniers sont motivés par l'apprentissage de nouvelles notions leurs permettant d'arriver à leurs fins. Comme la technologie est un domaine qui évolue très rapidement, il est important pour un pirate de rester à jours dans ses connaissances, ce qui sous-entend qu'il est préférable que ce dernier soit prêt à apprendre et passionné par ce domaine (Décary-Hétu, 2013 ; Zhang, Tsang, Yue et Chau, 2015). Une fois des connaissances acquises, il n'est pas rare de voir que les pirates seront avides de les partager avec leurs pairs. D'ailleurs, comme abordé précédemment, le partage d'information est l'une des caractéristiques principales unissant la communauté des hackers (Holt, 2007, cité dans Décary-Hétu, 2013). Raymond (2003) disait que le temps d'un pirate informatique est trop précieux pour qu'il soit occupé à résoudre un problème pour lequel quelqu'un a déjà trouvé une solution. C'est pourquoi, lorsqu'un pirate trouve une solution à un problème, une vulnérabilité dans un système ou acquiert une compétence quelconque, la coutume dans la communauté est que celui-ci l'enseigne et la partage avec ses pairs (Raymond, 2003). Ce partage de l'information transcende même parfois les limites de la communauté des pirates afin de rejoindre le grand public. C'est le cas des hacktivistes qui se dévouent à recueillir des informations, souvent gouvernementales, afin de les exposer à la population, prétextant une volonté de transparence et une liberté d'accès à l'information. Ces derniers refusent de voir l'autorité comme une entité pouvant les restreindre dans leurs actes et considèrent qu'il est de leur devoir de mettre au jour les renseignements et les injustices que le régime en place tient à garder secrets (Coleman, 2014). Enfin, la dernière prédisposition permettant à un hacker de se développer relevée dans la littérature concerne la programmation. Effectivement, plusieurs auteurs soulignent qu'il est avantageux pour un pirate d'avoir une certaine base en informatique et en programmation s'il désire mettre en œuvre les techniques d'attaques dont il a été question précédemment. Selon ces auteurs, les hackers doivent posséder un minimum de connaissances sur les ordinateurs, les systèmes d'exploitation, les logiciels et leurs vulnérabilités respectives afin de pouvoir prétendre au titre de pirate informatique (Choo, 2008, Raymond, 2003).

En conclusion, il est important de noter que les méthodes techniques de piratage informatique, tout comme les mesures de sécurité servant à s'en protéger, sont en évolution et perfectionnement constants (Barber, 2001). Ainsi, et comme il a été mentionné précédemment, les pirates se voient dans l'obligation de parfaire leurs techniques en permanence afin de demeurer au fait des dernières avancées dans le domaine (Décary-Hétu, 2013 ; Zhang, Tsang, Yue et Chau, 2015). Ce raffinement dans leurs méthodes entraîne une spécialisation grandissante chez les hackers qui tendent à concentrer leurs efforts dans un champs d'expertise particulier. En conséquence de cette spécialisation, les hackers se trouvent à être de plus en plus qualifiés, voire être des experts, dans des domaines de plus en plus restreints. Ce faisant, leurs connaissances dans les domaines connexes sont de moins en moins adéquates, les obligeant ainsi à collaborer avec d'autres hackers dont les compétences sont complémentaires aux leurs afin d'arriver à leurs fins. Ils peuvent alors faire appel à des collègues afin d'unir leurs forces et être en mesure de lancer l'attaque en équipe ou encore, tenter d'acquérir ces connaissances manquantes afin de parvenir à lancer l'attaque qu'ils souhaitent. Pour ce faire, les forums de discussion sont des outils de réseautage de plus en plus appréciés chez les hackers. Par leur mode de communication asynchrone et leur organisation en fonction des différents sujets de discussion et des publications des utilisateurs, les forums peuvent rapidement devenir une mine d'informations intéressantes pour tous, tant pour du partage de fichiers, de logiciels ou encore des discussions techniques (Décary-Hétu, 2013 ; Clais, 2016). Cette plateforme est donc un espace idéal, autant pour les novices qui cherchent à s'initier au piratage informatique que pour les experts cherchant à partager leurs connaissances ou à échanger sur les différentes techniques existantes. C'est pourquoi les forums de discussion sont considérés comme d'excellentes sources d'apprentissage pour la communauté des hackers et pourquoi le présent travail s'y intéressera de manière plus spécifique.

1.2 Les sociabilités criminelles

À la lumière des précédents propos, le stéréotype du hacker antisocial et reclus apparaît comme inadéquat pour décrire ces individus et leurs interactions. Effectivement, comme il a été mentionné, il n'est pas rare de voir les pirates informatiques interagir entre eux,

partager des informations, s'enseigner des concepts et collaborer sur des projets. Bien que les contacts physiques et les rencontres en face-à-face soient plus rares, cela n'empêche en rien le développement de relations sociales au sein de la communauté des hackers par le biais de plateformes favorisant la communication telle que les forums de discussion. La présente section permettra de faire le point sur les connaissances actuelles concernant les sociabilités criminelles et plus précisément leurs implications dans les relations sociales observées chez les hackers.

1.2.1 Définition

La sociabilité est la qualité de quelqu'un qui est sociable ; il s'agit de la capacité à établir un réseau de relations sociales dans des groupes présentant une cohérence idéologique, culturelle ou religieuse (Larousse, 2004). Les groupes sociaux auxquels un individu s'identifie dépendront grandement de l'individu en question, de ses valeurs et de ses expériences passées. Ce faisant, un certain individu pourra avoir une plus grande facilité à socialiser avec des collègues de travail, alors qu'un autre s'identifiera davantage à ses camarades d'école. Ceci fait référence au concept d'homophilie sociale voulant que l'humain ait tendance à fréquenter davantage ceux qui lui ressemblent (que ce soit au niveau du sexe, de l'âge, du degré d'éducation, etc.) (Grossetti, 2013 ; Éloire, 2014).

Dans un contexte de délinquance, la sociabilité se réfère donc à un réseau composé de délinquants partageant la même idéologie envers les normes sociales et le fait de les enfreindre. Ces associations sont souvent de deux natures. D'un côté, le délinquant peut s'associer avec des pairs commettant des infractions similaires aux siennes, lui permettant d'échanger avec eux et d'en apprendre davantage sur son milieu de délinquance. Ou encore, de l'autre côté, il peut s'associer à des délinquants qui opèrent dans un domaine complémentaire au sien, afin de prendre part à des opérations plus structurées et nécessitant des expertises diverses (Macdonald et Frank, 2017). Pour prendre un exemple concret, un cambrioleur pourrait, d'une part, s'associer avec d'autres cambrioleurs afin de discuter des différents modes opératoires utilisés pour entrer par effraction dans un domicile et, d'autre

part, s'associer avec des receleurs à qui il pourra vendre les bijoux qu'il vole lors de ses cambriolages.

1.2.2 Aspects sociaux du piratage informatique

Ainsi, ce concept s'applique autant, voire même plus, à la criminalité se produisant en ligne. Comme il a été déjà été mentionné, le piratage informatique est une délinquance très technique et nécessite que les pirates apprennent les uns des autres. Que ce soit un hacker expérimenté qui transmet son savoir ou un débutant cherchant les conseils d'un mentor, le partage d'information a été identifié comme l'une des bases fondamentales de la culture du piratage informatique et vient accentuer ce besoin de sociabilité (Jordan et Taylor, 1998 ; Raymond, 2003 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). La vitesse à laquelle la technologie évolue et la spécialisation des pirates dont il a été question précédemment incitent ces derniers à interagir les uns avec les autres afin de se tenir au courant des nouvelles techniques, de partager les nouveaux outils ou encore, d'unir leurs forces afin de lancer une attaque contre une cible commune. Un pirate isolé ne pourra que très difficilement arriver à ses fins et, c'est pourquoi la sous-culture des pirates informatiques est reconnue comme étant fondée sur une grande sociabilité. De ce fait, il n'est pas rare de voir des alliances ou des associations se former entre des individus en ligne.

Toutefois, vu la nature anonyme et intangible de ces relations, la littérature a établi que ces dernières étaient fragiles et éphémères, pour la plupart, limitant les individus à des communications majoritairement utilitaires (Craig, 2005 ; Choo, 2008 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). Afin de contrer légèrement les effets négatifs de l'anonymat sur les relations entre les pirates informatiques, la notion de réputation s'est développée comme étant un concept fondamental de cette sous-culture. De ce fait, à force de partage d'informations pertinentes ou d'enseignements utiles, une bonne réputation sera associée au pseudonyme du hacker. Sur les forums de discussion, par exemple, il existe des systèmes de pointage permettant aux membres d'attribuer une réputation positive ou négative aux autres membres, selon les interactions qu'ils ont eu avec eux. En se fiant sur les pointages de réputation des autres membres, il est alors possible pour un hacker de choisir de manière

plus éclairée qui sont ceux avec lesquels il veut s'associer (Lusthaus, 2012 ; Décary-Hétu, 2013 ; Dupont, Côté, Savine et Décary-Hétu, 2016).

Malgré cette complication au niveau de la confiance à accorder à ses pairs, la nature sociale de l'humain (Décary-Hétu, 2013), jumelée avec la curiosité et le désir de perfectionnement caractéristiques de la communauté des hackers (Raymond, 2003), poussent ces derniers à rechercher des associations délinquantes avec leurs pairs. La littérature fait d'ailleurs état de quelques études portant sur les interactions entre les hackers par le biais de forums de discussion et sur la structure des réseaux sociaux qui s'y créent. Bon nombre de ces auteurs s'intéressent à l'identification des acteurs clés de ces réseaux, en émettant l'hypothèse que, plus un acteur est impliqué sur le forum de discussion, plus ce dernier est important dans le réseau et donc plus importantes sont ses connaissances sur le piratage informatique (Lu, Luo, Polgar et Cao, 2010 ; Holt, Strumsky, Smirnova et Kilger, 2012 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). Zhang, Tsang, Yue et Chau (2015), de leur côté, se questionnent à savoir si les forums de discussion sont vraiment un espace propice à l'apprentissage, chez les pirates novices, de compétences qui leurs permettront de gravir les échelons de la hiérarchie des membres et de devenir des hackers expérimentés. Pour ce faire, ils considèrent le savoir qui est échangé sur les forums comme deux activités distinctes, soit la production de savoir (*knowledge provision*) et l'acquisition de savoir (*knowledge acquisition*). Selon leurs observations, les hackers les plus expérimentés, qu'ils présentent comme les *guru hackers*, sont ceux qui produisent le plus de connaissances et qui les partages le plus avec les hackers moins expérimentés de la communauté. Au contraire, les pirates débutants (*novice hackers*) sont identifiés comme étant dans les premiers stages d'apprentissage et produisent très peu de connaissances. Bref, la littérature démontre que les hackers apprennent effectivement les uns des autres et que, généralement, le savoir se transmet d'un hacker expérimenté et ayant une bonne réputation à un hacker novice.

CHAPITRE 2 – CADRE THÉORIQUE : THÉORIES DE L'APPRENTISSAGE CHEZ LES DÉLINQUANTS

Afin de mieux comprendre le partage d'information et d'enseignements qui s'effectue entre les pirates informatiques interagissant sur un forum de discussion, il est important de comprendre comment se produit un apprentissage. C'est pourquoi, dans la présente section, il sera question de deux théories expliquant l'apprentissage de la délinquance chez les individus, soit l'association différentielle de Sutherland ainsi que la théorie de l'apprentissage social de Akers.

Élaborée en premier, la théorie de l'association différentielle a posé les bases du processus d'apprentissage des comportements délinquants, alors que la théorie de l'apprentissage sociale a permis, par la suite, de préciser certains concepts et renchérir avec des notions qui n'avaient pas été considérées de prime abord. De par leur complémentarité, il a été jugé pertinent, dans le cadre du présent travail, de considérer ces deux théories conjointement. Aussi, puisque ces dernières ont d'abord été élaborées pour expliquer des délinquances hors-lignes, une courte description de chacune des théories sera faite, suivie d'un aperçu de leur application à la cyberdélinquance.

2.1 Association différentielle de Sutherland

2.1.1 Définition

C'est en 1947, dans la quatrième édition de son ouvrage *Principles of criminology*, qu'Edwin H. Sutherland présente la version retravaillée et finale de sa théorie de l'association différentielle. Dans cette théorie qui se veut une explication universelle du crime (Bruinsma, 1992), Sutherland énonce neuf propositions qui viendront révolutionner les conceptions de l'époque sur la manière dont un individu en vient à adopter des comportements délinquants (De Fleur et Quinney, 1966 ; Laub et Sampson, 1991).

Dès ses première propositions, Sutherland s'oppose à la conception de l'époque selon laquelle les comportements délinquants sont innés. Il affirme qu'il s'agit d'avantage d'un

apprentissage fait par le biais de processus communicatifs avec des pairs délinquants et survenant principalement au sein de petits groupes. Ainsi, cette théorie suppose que, si un individu ne possède aucune connaissance criminelle et n'a jamais été en contact avec la criminalité, il ne pourra développer des comportements de nature délinquante (Sutherland, Cressey et Luckenbill, 1992).

En s'intéressant au processus de socialisation permettant la transmission de modèles de comportements délinquants plutôt qu'à l'origine même de ces comportements (Merton, 1997), Sutherland affirme que l'individu développe des définitions internalisées, favorables ou défavorables aux violations de la loi, provenant majoritairement de son entourage et des pairs avec lesquels il s'associe. Ce sont d'ailleurs ces définitions internalisées qui détermineront les attitudes que l'individu adoptera face à la commission d'un acte délinquant (Akers et Jensen, 2006). Sutherland précise que les associations différentielles auront tendance à varier en fonction de la fréquence, de la durée, de la priorité et de l'intensité des contacts (Cressey, 1952 ; Sutherland, Cressey et Luckenbill, 1992). Ces quatre facteurs viendront donc influencer les probabilités qu'un individu s'associe ou non avec un pair et internalise ses définitions quant aux violations de la loi. Enfin, et c'est là le principe clé de la théorie de l'association différentielle, un individu adoptera des comportements délinquants dans la mesure où ses définitions favorables aux violations de la loi excèderont celles qui y sont défavorables.

2.1.2 Application de la théorie à la pratique

Comme bien des théories clés en criminologie, la théorie de l'association différentielle a été élaborée bien avant le développement des technologies informatiques, et donc, ne prend pas en compte l'environnement virtuel qui fait, aujourd'hui, parti du quotidien de l'homme moderne (Morris et Higgins, 2010). Quelques auteurs se sont toutefois intéressés à la situation et ont tenté de mettre à l'épreuve cette théorie criminologique en l'appliquant à la cybercriminalité. L'une des premières constations qui a été faite est que les crimes nécessitant l'usage d'un ordinateur sont considérés par plusieurs comme potentiellement plus dépendant de l'apprentissage par les pairs que les crimes traditionnels. Effectivement,

les individus cherchant à commettre ce type de crimes doivent nécessairement acquérir un minimum de compétences techniques, ne serait-ce que pour être en mesure de se servir de l'ordinateur, qui ne peuvent être apprises par le biais des expériences communes de la vie de tous les jours et doivent donc recourir à l'aide de leurs pairs (Chantler, 1996 ; Morris et Higgins, 2010).

En ce qui concerne l'association différentielle de manière plus spécifique, il s'agit de l'une des théories les plus largement testées et supportées des théories du crime (Pratt et al., 2010) et une littérature grandissante démontre son applicabilité dans un environnement de cyberdélinquance. Par exemple, Hollinger (1993) a trouvé que l'implication d'amis dans des activités de piratage informatique augmente significativement les probabilités d'implication d'un individu dans le même type d'activités. Dans le même ordre d'idées, Skinner et Fream (1997) rapportent que l'association différentielle avec des amis qui participent à des crimes informatiques est le meilleur prédicteur d'un futur comportement de délinquance informatique chez l'individu. Pareillement, Morris et Higgins (2009) ont trouvé que l'association différentielle était le prédicteur théorique le plus important au niveau du piratage informatique auto-rapporté par leurs sujets.

Hawdon (2012), pour sa part, aborde la question sous un autre angle. Effectivement, dans son étude sur la propagation des groupes de haine dans les médias sociaux et leur influence sur le développement de comportements violents, il en vient à la conclusion que, à la manière soulignée dans la théorie de l'association différentielle, les groupes de haine en ligne peuvent servir d'agents producteurs de violence. À l'époque de Sutherland, les associations et les apprentissages se produisaient majoritairement dans le cadre de relation en face-à-face avec des pairs. Toutefois, aujourd'hui, avec les médias sociaux, il est beaucoup plus facile pour quelqu'un d'entrer en contact avec d'autres individus qui pourront avoir une influence sur les définitions internalisées sans pour autant les rencontrer en personne. C'est donc dire qu'un individu cherchant à s'associer avec des groupes haineux y parviendra beaucoup plus aisément aujourd'hui, grâce aux médias sociaux, puisque ceux-ci lui permettent d'entrer en contact avec des individus qui lui étaient jusqu'alors inaccessibles. Aussi, selon les conclusions de Hawdon (2012), l'influence des

pairs rencontrés par le biais de réseaux virtuels est aussi importante que celle des pairs rencontrés en personne.

Pour conclure, la théorie de l'association différentielle a connu son lot de critiques depuis sa première publication, la plus virulente étant que le ratio entre les définitions favorables et défavorables utilisé par Sutherland pour expliquer la criminalité ne peut être déterminé empiriquement (Glueck, 1956 ; Short, 1956 ; Cressey, 1960). Malgré tout, et compte tenu des résultats présentés précédemment, il semble que les principes de base de la théorie, selon lesquels l'apprentissage d'un comportement délinquant chez un individu se fait par le biais des définitions transmises par ses pairs, soient confirmés et applicables à plusieurs types de criminalité, dont la cybercriminalité.

2.2 Les théories de l'apprentissage social

2.2.1 Définition

Bien que plusieurs théories reçoivent encore aujourd'hui l'appellation de théorie de l'apprentissage social, la plus connue demeure sans doute celle établie par Albert Bandura en 1977. Bandura déplorait la faiblesse des explications que les approches telles que la théorie du conditionnement opérant de Skinner ou les modèles d'apprentissage social de l'époque, proposaient au niveau de l'apprentissage de nouveaux comportements chez l'individu (Bandura, 1969). Pour pallier à cette lacune, et contrairement aux théories behavioristes qui l'ont précédé, Bandura ne limite pas le processus d'apprentissage aux renforcements positifs ou négatifs qu'un individu subit suite à l'adoption d'un comportement. Effectivement, la théorie de l'apprentissage social de Bandura, qu'il renommera ultérieurement la théorie sociale cognitive (*Social Cognitive Theory*) propose qu'un processus d'apprentissage entre également en jeu lorsqu'un individu observe un pair adopter un comportement et être récompensé ou puni pour ce comportement.

Comme c'est le cas pour la majorité des théories innovantes, la théorie de l'apprentissage sociale de Bandura a été utilisée et modifiée afin de l'adapter à divers domaines d'étude. Ce sont d'ailleurs les américains Ronald Akers et Robert Burgess qui, en 1966, ont été les

premiers à amorcer cette tâche dans le domaine de la criminologie. Enfin, c'est en combinant les principes de l'apprentissage social de Bandura, du conditionnement opérant de Skinner et de l'association différentielle de Sutherland que Akers (1985) pose les derniers jalons de ce qui deviendra sa théorie de l'apprentissage social. Cette théorie se veut une explication de l'acquisition, du maintien et de la modification des comportements délinquants, prenant en considération les facteurs sociaux, non-sociaux et culturels qui interagissent dans la promotion ou la dévalorisation de ces comportements. Pour y parvenir, la théorie de l'apprentissage social de Akers repose sur quatre concepts fondamentaux : l'association différentielle, les définitions, le renforcement différentiel et l'imitation (Akers et Jensen, 2006 ; Brauer et Tittle, 2012).

Dans le contexte de l'apprentissage social, l'association différentielle fait directement référence à l'association et l'interaction d'un individu avec des pairs qui sont eux-mêmes engagés dans certains types de comportements ou qui expriment des normes, des valeurs et des attitudes qui encouragent de tels comportements (Akers et Jensen, 2006). Akers spécifie d'ailleurs que le rôle de l'entourage principal d'un individu ne se limite pas à exposer ce dernier à des définitions à adopter, mais également à lui fournir des modèles comportementaux qu'il peut imiter et à concilier les renforcements sociaux qu'il doit considérer pour chaque comportement appris (Akers, 1996). Pour leur part, les définitions interviennent comme des stimuli facilitants ou inhibiteurs des comportements d'un individu en agissant moins comme des sources de motivation directes, mais davantage comme des signaux indiquant, dans une situation donnée, qu'un certain comportement sera approprié et susceptible d'être récompensé ou, au contraire, inapproprié et à risque d'être puni (Burgess et Akers, 1966 ; Akers, 1985). De son côté, le renforcement différentiel fait référence à l'équilibre entre les récompenses et les punitions attendues et réelles faisant suite à un comportement chez l'individu. L'acquisition et le maintien d'un comportement, qu'il soit conforme ou déviant, dépend des récompenses et des punitions, passées et présentes, associées à ce comportement ainsi que des récompenses et des punitions associées au comportement alternatif (Akers, 1977). Ainsi, un individu pourrait s'abstenir de contrevenir à la loi, malgré qu'il ait appris des définitions qui y sont favorables, dans l'éventualité où il anticipe des coûts supérieurs aux récompenses liées à cette violation

(Akers, 1996). Enfin, le concept de l'imitation consiste à l'engagement d'un individu dans un comportement, suite à l'observation directe ou indirecte d'un comportement similaire chez un pairs, et dépend des caractéristiques propres au modèle, au comportement observé ainsi qu'aux conséquences du comportement observé (Akers et Jensen, 2006). Pour conclure, il est important de noter que ces quatre concepts sont tous corrélés les uns aux autres et s'influencent mutuellement dans le processus d'acquisition et de maintien d'un nouveau comportement chez l'individu (Akers, Krohn, Lanza-Kaduce et Radosevich, 1979).

2.2.2 Application de la théorie à la pratique

Au cours des années écoulées depuis sa publication, la théorie de l'apprentissage social de Akers a été l'objet de nombreuses études visant à valider sa pertinence. Les thèmes abordés afin de tester empiriquement cette théorie sont extrêmement variés, couvrant des délits tels que l'abus de substances, la délinquance générale, les agressions sexuelles et les comportements alcooliques, pour n'en nommer que quelques-uns (Akers et Cochran, 1985 ; Brownfield et Thompson, 1991 ; Adams, 1996 ; Catalano, Kosterman, Hawkins, Newcomb et Abbott, 1996). La grande majorité de ces études présentent d'ailleurs une forte relation entre les prédicteurs théoriques et les résultats associés aux variables d'intérêt. Dans le même ordre d'idées, certaines études se sont intéressées à tester l'application de la théorie de l'apprentissage social à des infractions de cybercriminalité, lui permettant ainsi d'amasser un support empirique significatif au niveau de l'explication des diverses formes de piratage en ligne (Higgins, Wilson et Fell, 2005 ; Higgins et Wilson, 2006 ; Higgins, Wolfe et Marcum, 2008 ; Hinduja, 2008).

Par exemple, Morris et Higgins (2010) évaluent la capacité de la théorie de l'apprentissage social à expliquer la probabilité qu'un individu s'engage dans des activités de piratage numérique. Dans le contexte de cette étude, le concept de piratage numérique, ou *digital piracy*, fait référence à l'acte de se procurer illégalement toute forme de média digital par le biais d'un partage de fichier ou de téléchargement illégal. La théorie de l'apprentissage social étant une théorie générale du crime, les auteurs émettent l'hypothèse qu'elle devrait

être en mesure d'expliquer une variation substantielle dans l'adhérence d'un individu au piratage numérique. En conformité avec cette hypothèse, les conclusions de cette étude montrent que la théorie de l'apprentissage social semble expliquer une étendue respectable de la variation dans la probabilité qu'un étudiant universitaire s'engage dans le piratage numérique (Morris et Higgins, 2010). Une critique est cependant soulevée par ces auteurs, tout comme certains l'avaient fait avant eux, selon laquelle la théorie pourrait bénéficier de certaines modifications dans ses composantes afin de prendre en compte le réseau de pairs virtuels de l'individu (Skinner et Fream, 1997 ; Warr, 2002 ; Morris et Higgins, 2009).

Pour faire suite à cette critique, Hinduja et Ingram (2009) se sont intéressés à la différence entre l'impact que peuvent avoir les sources d'influence (pairs et médias), selon qu'elles se trouvent en ligne ou hors-ligne, sur l'adoption de comportements cyberdélinquants. S'il est clair que la théorie de Akers fournit une explication significative à ce phénomène, il n'en demeure pas moins intéressant de savoir si ce sont les sources d'apprentissage provenant du cyberespace qui ont le plus de poids dans le comportement délinquant de l'individu, ou celles trouvées hors-ligne. Cette connaissance permettra d'ailleurs, par la suite, de mieux orienter les méthodes de prévention et les stratégies de réponses afin de venir contrer ce type de délinquance. En se basant sur les relations observées entre les différentes mesures analysées dans le cadre de cette étude, Hinduja et Ingram (2009) ont été en mesure d'identifier un pattern intéressant. Ce pattern illustre que les sujets qui rapportent être influencés par des pairs hors-ligne semblent rapporter un impact moins important des autres sources d'influence analysées (pairs en ligne, médias hors-ligne et médias en ligne). Au contraire, les sujets qui rapportent être influencés par des pairs rencontrés en ligne semblent être également influencés par les deux sources de médias analysées. Ces résultats, en concordance avec les recherches précédentes ayant été menées sur le sujet (Skinner & Fream, 1997 ; Higgins et Makin, 2004 ; Higgins, Fell et Wilson, 2006 ; Higgins et Wilson, 2006), démontrent que les pairs hors-ligne sont la source d'influence la plus forte en ce qui a trait à l'adoption de comportements de piratage numérique, suivi par les pairs rencontrés en ligne et les sources de médias en ligne, qui sont également importants à considérer. Ce faisant, l'étude de Hinduja et Ingram (2009) fournit

les preuves que l'apprentissage autant en ligne que hors-ligne joue un rôle important dans l'adoption de comportements de piratage numérique.

CHAPITRE 3 – PROBLÉMATIQUE DE RECHERCHE

La technologie a connu un essor important au cours des dernières décennies et, avec elle, s'est développée la délinquance en ligne. Que ce soit en facilitant la commission de délits tels que la traite d'enfants ou le trafic de stupéfiants (Choo, 2008 ; Wyble, 2008, cité dans Vidal, 2016), ou encore en étant l'outil de perpétration du délit, comme dans le cadre du piratage informatique, la technologie se trouve de plus en plus impliquée dans diverses infractions (Barber, 2001 ; Décary-Hétu, 2013). De ce fait, le sous-terrain informatique est rapidement devenu un sujet de prédilection pour les chercheurs afin de démystifier cet univers et les individus qui composent sa communauté, nommément les pirates informatiques. Bien que plusieurs éléments comme la légitimité, les motivations, les techniques utilisées ou la spécialisation peuvent différencier les hackers et venir créer une certaine barrière entre ces derniers (Barber, 2001 ; Sehn, 2002 ; Kleinknecht, 2003 ; Raymond, 2003 ; Crandall, Su, Wu et Chong, 2005 ; Mitnick et Simon, 2011 ; Décary-Hétu, 2013 ; eduCBA, 2016), il n'en reste pas moins que cette communauté est reconnue comme étant basée sur le partage d'information, l'entraide et le réseautage (Jordan et Taylor, 1998 ; Raymond, 2003 ; Holt, Strumsky, Smirnova et Kilger, 2012 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). Comme il a été possible d'observer dans les chapitres précédents, les hackers évoluent dans des réseaux sociaux volatiles et aux liens fragiles permettant un grand roulement dans leurs membres. Ces relations permettent les échanges d'information, d'outils et même, de valeurs et d'objectifs normatifs, tout en permettant aux pirates de se développer individuellement (Jordan et Taylor, 1998 ; Holt, Strumsky, Smirnova et Kilger, 2012). Le partage de connaissances, d'outils ou de programmes, entre les pirates informatiques sur des plateformes de communication telles que les forums de discussion sont, d'ailleurs, au cœur de la sous-culture des cyberdélinquants (Raymond, 2003 ; Holt, Strumsky, Smirnova et Kilger, 2012 ; Décary-Hétu, 2013 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). Dans ce contexte, ce sont majoritairement les hackers les plus expérimentés qui partagent leurs connaissances et qui produisent des outils afin d'aider les novices à évoluer dans le domaine qui les intéresse (Zhang, Tsang, Yue et Chau, 2015).

Puisqu'il s'agit d'un domaine en constante et rapide évolution, la littérature sur la cyberdélinquance, et plus particulièrement sur le piratage informatique, se doit de demeurer d'actualité et de suivre cette tendance de développement. Afin de prévenir ces infractions, il est primordial d'être en mesure d'en comprendre les auteurs, incluant le processus qui permet à un individu de devenir un pirate informatique. Bien que les connaissances commencent à se développer dans ce domaine, plusieurs avenues demeurent inexplorées. Précédemment, il a été fait mention que les pirates informatiques tenaient leurs connaissances de leurs interactions avec d'autres pirates de la communauté (Holt, Strumsky, Smirnova et Kilger, 2012 ; Abbasi, Li, Benjamin, Hu et Chen, 2014) et que, selon les théories de l'apprentissage analysées, les pairs sont d'une grande importance dans le processus d'apprentissage pour un cyberdélinquant (Hollinger, 1993 ; Hinduja et Ingram, 2009 ; Morris et Higgins, 2009 ; Morris et Higgins, 2010). Bien qu'il soit établi que les pirates apprennent les uns des autres, les connaissances sont encore lacunaires quant à la facilité et l'accessibilité de ce processus. Dans un objectif de compréhension, il apparaît intéressant de se questionner afin de savoir s'il s'agit d'un processus accessible à tous ou si seuls certains privilégiés peuvent en franchir les échelons. Malgré la mentalité des hackers qui favorise un climat d'échange entre les membres de la communauté, il est inévitable que certains conflits et frictions se créent entre ces derniers, comme cela se produit également hors-ligne. Toutefois, l'impact de ces conflits sur le processus d'apprentissage et le développement de pirates novices n'est que très peu discuté dans la littérature. Également, il a été établi à de nombreuses reprises que l'apprentissage est crucial pour que les pirates développent les connaissances et les habiletés nécessaires à leurs activités (Jordan et Taylor, 1998 ; Raymond, 2003 ; Abbasi, Li, Benjamin, Hu et Chen, 2014).

Étant donné que l'apprentissage est un processus fondamentalement social (Akers, 1977 ; Sutherland, Cressey et Luckenbill, 1992), une volonté de compréhension du processus d'apprentissage passe nécessairement par un exercice de compréhension des relations et des interactions sociales entre les apprentis et les mentors de la communauté à l'étude. Dans le cadre du présent travail, la communauté visée en est une particulièrement difficile d'accès (Jordan et Taylor, 1998 ; Coleman, 2014) obligeant bien souvent l'utilisation de

méthodologies indirectes de la part des auteurs telles que des sondages de criminalité auto-révélée administrés, majoritairement, à des étudiants de collèges américains (Hollinger, 1993 ; Higgins et Makin, 2004 ; Morris et Higgins, 2009 ; Hinduja et Ingram, 2009). Bien que plusieurs études se soient intéressées à la structure des réseaux de pirates informatiques évoluant sur les forums de discussion (Décary-Hétu, Morselli et Leman-Langlois, 2012 ; Holt, Strumsky, Smirnova et Kilger, 2012 ; Abbasi, Li, Benjamin, Hu et Chen, 2014), très peu ont jumelé cet intérêt avec l'étude du processus d'apprentissage et c'est donc par cette combinaison que le présent travail se distingue et permettra de faire évoluer la littérature sur le sujet.

De ce fait, la présente étude vise à **comprendre le processus d'apprentissage social chez les pirates informatiques**. Plus précisément, une analyse de réseaux sociaux sera effectuée sur les participants d'un forum de discussion dans l'objectif de **qualifier les liens d'entraide** venant favoriser l'apprentissage social dans la communauté des pirates informatiques ; **qualifier les liens de conflit** nuisant à l'apprentissage social dans cette même communauté ; et **identifier les acteurs clés** de ces deux réseaux pour en faire la comparaison. De ces analyses découlera une meilleure compréhension des interactions par lesquelles un individu peut transmettre et/ou acquérir des connaissances dans son domaine d'expertise. Selon les résultats de Zhang, Tsang, Yue et Chau (2015), il est attendu que les participants qui ressortiront comme centraux de ce réseau soient vraisemblablement les plus expérimentés, partageant leurs connaissances avec les novices. Aussi, une distinction sera faite entre les interactions d'entraide et de conflits afin de pouvoir évaluer si certains individus provoquent plus inéluctablement des réactions de conflits que d'autres. Ainsi, il est attendu que les membres cherchant à profiter du savoir des autres sans jamais redonner à la communauté en produisant leur propre savoir, soient plus à même d'être impliqués dans des relations de conflits. Ces individus sont identifiés dans la littérature sous l'appellation de *crackers* et s'attirent souvent les foudres des hackers pour leurs comportements amoraux (Barber, 2001 ; Sehn, 2002 ; Raymond, 2003 ; Mitnick et Simon, 2011 ; eduCBA, 2016).

Dans un contexte comme celui d'aujourd'hui où les connaissances sur la cybercriminalité et les technologies présentent un besoin constant d'approvisionnement scientifique, une telle étude trouve sa pertinence. Effectivement, une meilleure compréhension des processus d'apprentissage et des relations qui unissent les pirates informatiques représente une opportunité pour les autorités de mieux anticiper les comportements de ces délinquants. Ce faisant, une prévention plus efficace et des interventions plus appropriées pourront être mises en place afin de réduire l'impact de cette délinquance dans la société.

CHAPITRE 4 – MÉTHODE ET DONNÉES

La présente section vise à décrire et expliquer le processus de collecte de données employé dans le cadre de ce travail, ainsi que la stratégie de recherche mise sur pieds en ce qui a trait à l'analyse de ces données. Comme il a été mentionné précédemment, la présente étude se distingue quant à sa méthodologie d'analyse de réseaux ainsi que sa population visée. L'attrait d'une telle stratégie de recherche est d'être en mesure d'observer le phénomène d'apprentissage social directement pendant qu'il se produit plutôt que rétroactivement, comme le permettent les méthodologies par sondages utilisées dans la majorité des études existantes dans ce domaine. Les prochains paragraphes permettront d'illustrer comment s'est articulée cette stratégie de recherche afin de répondre aux objectifs spécifiques posés dans la section précédente soit qualifier les liens d'entraide et de conflit dans la communauté des pirates informatiques ainsi que leur influence sur le processus d'apprentissage social et d'identifier les acteurs clés de chacun de ces réseaux pour en faire la comparaison.

4.1 Collecte des données

4.1.1 Source de données

Tout d'abord, la présente recherche est basée sur une seule et unique source de données, c'est-à-dire le forum de discussion en ligne hackforum.net. Cette plateforme, qui n'en est pas à sa première utilisation en tant que source de donnée ou sujet d'intérêt (Andrews, Holloway et Massoglia, 2015 ; Bukac, Stavova, Nemec, Riha et Matyas, 2015 ; Dupont, Côté, Savine et Décary-Hétu, 2016), compte actuellement plus de 3,6 millions de membres et présente plus de 3,8 millions de fils de discussion (aussi appelé *threads*) compilant un total de plus de 55,5 millions de messages (aussi appelé *posts*). Le contenu de cette plateforme est divisé en nombreuses catégories distinctes allant du piratage informatique à l'actualité cinématographique, en passant par la programmation, les jeux vidéo et plusieurs autres, le tout permettant aux utilisateurs de choisir le type de discussions auxquelles ils veulent prendre part. Dans le cadre du présent travail, la sous-catégorie *Beginner Hacking* a été identifiée comme la plus pertinente, puisqu'il s'agit de celle où les relations entre un

pirate novice, cherchant à apprendre les bases, et un pirate expérimenté, cherchant à transmettre ses connaissances, sont les plus propices de se développer. Une fois la sous-catégorie identifiée, les fils de discussion ont été classés en ordre chronologique de publication, puis tous ceux ayant été publiés entre le 1 et le 31 janvier inclusivement ont été sélectionnés, totalisant 570 fils de discussion et 3636 messages.

4.1.2 Méthode de collecte de données

Au niveau de la collecte en elle-même, tous les messages ont été lus afin d'en ressortir les relations d'entraide et de conflit entre les membres. Une seule et même personne a lu et analysé tous les messages, limitant ainsi les risques de désaccord inter-juges et les irrégularités dans la collecte. À la lecture, plusieurs scénarios étaient possibles et la présence d'une seule analyste permettait de favoriser une certaine constance dans les réponses face à ces différents scénarios. Le premier scénario observé, et sans doute le plus fréquent dans l'échantillon analysé, consistait en un utilisateur A qui publie un fil de discussion contenant une question sur une notion informatique quelconque et un utilisateur B qui répond au questionnement de A en lui fournissant les informations nécessaires. Dans une telle situation, une relation d'entraide allant de B (aidant) à A (aidé) était consignée. Toutefois, toutes les situations n'étaient pas aussi faciles à analyser nécessitant, de ce fait, la mise en place de certaines règles pour rendre le tout plus objectif pour l'analyste. Ainsi il a été établi qu'une relation d'entraide correspondait à un individu qui apporte son concours à quelqu'un, qui joint ses efforts aux siens dans ce qu'il fait, qui lui est utile et qui facilite son action. De l'autre côté, une relation de conflit est caractérisée par la moquerie et le dessein de nuire à autrui ; c'est faire du tort et porter atteinte ou préjudice à un autre individu.

Enfin, certaines situations plus complexes ont également été rencontrées lors de la collecte de données, obligeant l'analyste à prendre la décision de catégoriser l'interaction comme une situation d'entraide, de conflit ou comme une situation ne devant pas être comptabilisée. Par exemple, si A pose une question, que B répond à la question, mais que par la suite C mentionne que la réponse de B n'est pas bonne et que, sans donner de réponse,

il ne fait que dénigrer la réponse de B, il sera comptabilisé pour cette situation qu'une relation d'entraide part de B vers A et qu'une relation de conflit part de C vers B. Effectivement, il est considéré que l'intention première du répondant est d'aider le demandeur et donc, à moins d'indication de sarcasme ou de volonté de d'induire en erreur, les réponses données étaient envisagées comme des tentatives d'entraide. Un autre exemple de situation qui a été relevée présente A qui pose une question, B qui répond à la question, C qui renchérit en posant une deuxième question et D qui répond directement à C. Dans cette situation, deux relations d'entraide sont comptabilisées, soit une partant de B vers A et une partant de D vers C.

Suite à cette collecte, les données ont été nettoyées et anonymisées afin de créer deux matrices présentant d'une part les relations d'entraide et d'autre part les relations de conflit relevées dans les discussion présentes sur le forum. Une fois les matrices créées dans Excel, ces dernières ont été transformées afin de pouvoir être analysée dans UCINET, un logiciel développé par Lin Freeman, Martin Everett and Steve Borgatti afin de permettre l'analyse de réseaux sociaux (Borgatti, Everett et Freeman, 2002). Grâce à ce logiciel, deux réseaux ont été générés, soit un réseau présentant les acteurs et les liens impliqués dans les relations d'entraide et un second pour les acteurs et les liens impliqués dans les relations de conflit. Enfin, une fois les réseaux construits, plusieurs analyses, qui seront décrites dans la prochaine sous-section, ont été effectuées afin de répondre aux différents objectifs de la présente étude.

4.2 Analyse des données

4.2.1 Concepts clés

Grâce à l'analyse de réseaux sociaux, il est maintenant possible de qualifier la structure d'un réseau de différentes manières et selon différents concepts. Dans le cadre du présent travail, deux concepts principaux ont été choisis afin d'y parvenir soit, le concept de la cohésion et celui du pouvoir. Si le concept de cohésion aide à comprendre la facilité avec laquelle l'information circule dans un réseau donné, le concept du pouvoir permet d'acquérir une meilleure compréhension de la présence d'acteurs clés dans ce même

réseau. De cette manière, ensembles, ces deux concepts favoriseront une compréhension globale du processus d'apprentissage chez la population visée.

Le premier concept à l'étude est celui de la cohésion. Dans un réseau social, la cohésion correspond à la propension des acteurs à être unis les uns aux autres ou, au contraire, à se diviser en sous-groupes distincts. Afin d'être cohésif, un réseau doit être composé d'acteurs qui sont proches les uns des autres et qui se font confiance mutuellement. Or, dans une communauté comme celles des pirates informatiques, où il a été précédemment établi que les relations sont éphémères et fragiles, il est attendu que la cohésion soit plutôt faible avec la présence marquée de sous-groupes au sein du réseau. De son côté, le second concept à l'étude, celui du pouvoir, est souvent défini comme la capacité d'un acteur du réseau à contrôler l'information qui est transmise. Dans le contexte de l'étude actuelle, cette information peut être de deux natures soit, des enseignements circulant, habituellement, directement d'un mentor vers un novice ou encore des agressions provenant d'un acteur dont le but est de nuire aux autres notamment en les empêchant d'apprendre. Ce faisant, les mesures utilisées permettront de savoir qui sont les individus centraux du réseau, qui sont ceux qui distribuent l'information, positive ou négative, qui sont ceux qui reçoivent cette information, de quelle manière s'articulent leurs relations et surtout, de savoir si le partage repose sur un petit groupe d'individus responsable de la formation d'une majorité des pirates informatiques novices.

4.2.2 Méthodes d'analyse des données

Ayant comme visée principale de qualifier les liens d'entraide et de conflit, les analyses de la présente étude demeurent à un niveau égocentrique et sociométrique. De cette manière, elles permettront la caractérisation de la structure des deux réseaux ainsi que leur comparaison. Pour ce faire, les analyses ont été divisées en plusieurs étapes distinctes.

Tout d'abord, une analyse de la **densité** et du **coefficient d'agglomération** (Watts et Strogatz, 1998) de chacun des réseaux a été effectuée. En comparant ces mesures, il sera possible d'observer si la communauté des hackers est soudée ou si, au contraire, elle se

divise en sous-groupes. Plus la densité d'un réseau est élevée, plus ce dernier est composé de relation un à un entre les acteurs. Ainsi, si le coefficient d'agglomération est supérieur à la mesure de densité, cela signifie que le réseau est plus à même d'être divisé en sous-groupes et donc, que les acteurs sont moins uniformément unis.

La seconde mesure utilisée a permis de connaître le **degré de centralisation** du réseau (Freeman, 1978). Cette mesure présente la tendance d'un réseau à concentrer les liens entrants (c'est-à-dire les enseignements et les insultes reçus) ou les liens sortants (c'est-à-dire les enseignements et les insultes donnés) dans un acteur en particulier. Il est à noter que, lorsqu'il sera question du réseau de conflit, les relations entre les principaux acteurs seront plutôt considérées comme des relations entre des tyrans (propageant les commentaires négatifs) et des victimes (recevant les commentaires négatifs) ; alors que pour le réseau d'entraide, il est question de relations entre des mentors et des apprentis. De ce fait, au niveau individuel, les mesures de centralité permettront d'analyser si un acteur peut être considéré comme un mentor (s'il concentre les liens d'entraide sortants), un apprenti (s'il concentre les liens d'entraide entrants), un tyran (s'il concentre les liens de conflit sortants), ou finalement une victime (s'il concentre les liens de conflit entrants). Dans le même ordre d'idées, la troisième mesure consiste à trouver la **réciprocité** des liens dans le réseau (Costa, Rodrigues, Travieso et Villas Boas, 2007). À cette fin, pour chaque acteur, les nombre de liens entrants et sortants a été calculé, tant pour les apprentissages que pour les conflits, permettant ainsi d'obtenir un taux du nombre de liens entrants divisé par le nombre de liens sortants. Ces informations ont, par la suite, été agrégées au niveau du réseau entier, permettant de comprendre si un apprentissage ou une insulte mène à un second apprentissage ou une seconde insulte. Plus ce taux se rapproche de 1, plus une action aura une conséquence de répétition : une insulte appelle à une insulte, un apprentissage appelle à enseigner à d'autres.

Enfin, alors que les trois mesures dont il a été question précédemment portaient davantage sur les réseaux en général, les prochaines se rapportent plus spécifiquement aux individus composant ces réseaux. La quatrième mesure permettra de connaître le nombre de mentors que chaque novice possède. De cette manière, il sera possible d'observer si le mode de

transmission de l'information se produit davantage dans un contexte un à un ou encore d'un groupe de mentor vers un même novice. Pour sa part, la cinquième mesure permettra d'évaluer la réciprocité des liens chez les acteurs et donc d'identifier ceux qui présentent des relations d'apprentissage mutuel d'égal à égal avec leurs pairs ou ceux qui jouent davantage un rôle de mentor ou d'apprenti dans le réseau. Pour conclure les analyses, la dernière mesure permet de faire la distinction entre les acteurs du cœur et ceux de la périphérie des différents réseaux à l'étude (Borgatti et Everett, 2000). Ainsi, il est possible de déterminer qui sont les acteurs au cœur des échanges, c'est-à-dire **les acteurs clés** du réseau, et qui sont ceux minimalement impliqués dans la distribution des liens. Étant les acteurs les plus impliqués dans les relations du réseau, les acteurs clés sont souvent considérés comme les plus importants du réseau. Pour la présente étude, l'identification des acteurs clés pourra permettre d'évaluer qui sont les utilisateurs qui participent le plus aux relations d'entraide et de conflit qui se développent au sein d'un forum de discussion. De ce fait, il sera possible de comparer les acteurs clés qui ressortent pour chacun des réseaux et de voir si les individus qui se trouvent au cœur des échanges d'entraide se trouve également au centre des relations de conflit ou s'il s'agit d'acteurs différents. Pour conclure, selon les résultats obtenus, des hypothèses pourront être émises afin de tenter d'expliquer ce qui motiverait un individu à présenter une forte participation à l'un des réseaux en particulier ou aux deux en même temps.

CHAPITRE 5 – RÉSULTATS ET ANALYSE

Le présent chapitre permettra de détailler les résultats obtenus par le biais des analyses réalisées sur les données provenant du forum de discussion hackforum.net. Pour ce faire, une première section présentera une description sommaire de chacun des réseaux à l'étude, alors qu'une seconde section s'intéressera davantage à qualifier la structure de ces réseaux par des analyses plus approfondies sur les liens et les acteurs qui la composent. De cette manière, un portrait global et complet de la situation pourra être obtenu et la compréhension du processus d'apprentissage social au sein de la communauté des pirates informatiques en sera maximisée.

5.1 Description sommaire des réseaux

La collecte de données effectuée a permis d'identifier 821 membres ayant participé aux échanges sur le forum de discussion à l'étude. Après les analyses, il a été possible de noter que, de ces 821 membres, 261 (32%) sont impliqués autant dans des relations de conflit que d'entraide, alors que les 560 autres (68%) se limitent à un seul type d'échange.

Le réseau composé des liens d'entraide entre les utilisateurs du forum de discussion comptabilise 683 acteurs et 1152 liens dirigés. Un sociogramme de ce réseau est présenté à la Figure 1. Il est possible d'y voir plusieurs acteurs principaux au centre qui semblent être les points de rencontre de nombreux liens, alors qu'en périphérie, plusieurs relations à sens unique entre deux acteurs peuvent être observées.

Pour ce qui est du réseau basé sur les relations de conflit entre les utilisateurs du forum, ce dernier est illustré par la Figure 2. Il est d'ailleurs possible d'y observer le même genre de patterns que pour le réseau d'entraide, c'est-à-dire qu'avec ses 399 acteurs et ces 548 liens dirigés, deux acteurs centraux ressortent du sociogramme semblant concentrer les liens et plusieurs dyades sont visibles en périphérie du réseau.

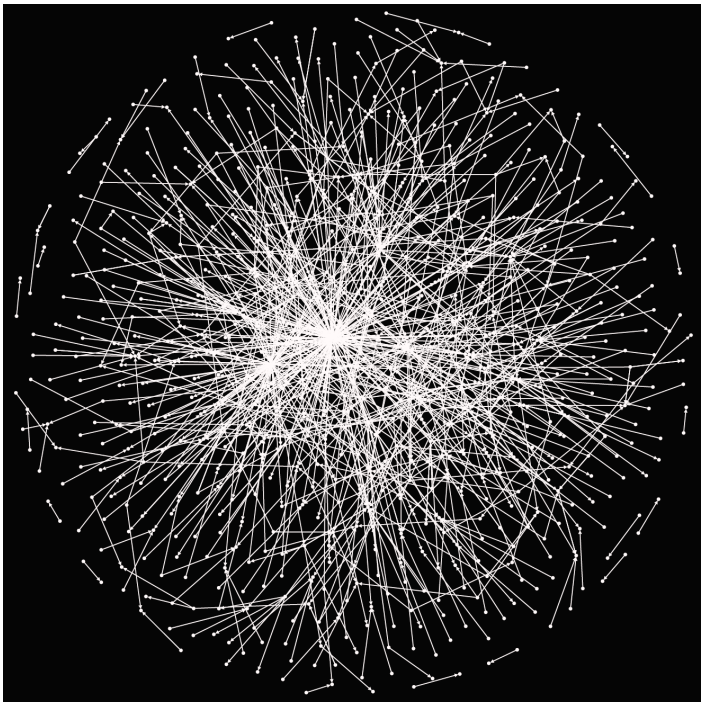

Figure 1. Sociogramme présentant les relations d'entraide entre les utilisateurs du forum de discussion hackforum.net

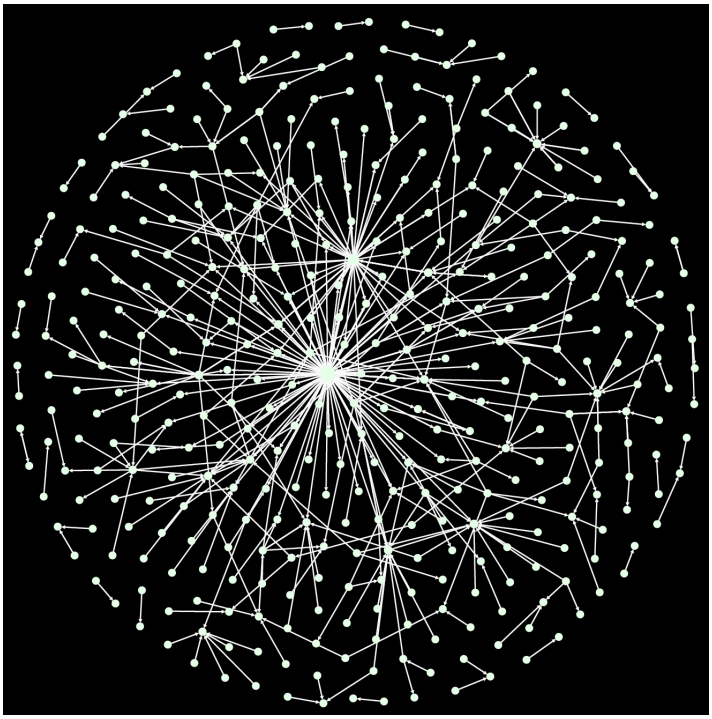

Figure 2. Sociogramme présentant les relations de conflit entre les utilisateurs du forum de discussion hackforum.net

5.2 Structure des réseaux

5.2.1 Densité

Comme discuté brièvement précédemment, la densité d'un réseau est une mesure de cohésion simple à obtenir et pourtant révélatrice sur la structure même du réseau à l'étude. Cette mesure permet de connaître la densité des liens dans un réseau en calculant la proportion des connections réelles présentes au sein de ce réseau sur le nombre de liens potentiels. Par exemple, un réseau non-dirigé de trois acteurs (A, B et C) compte trois liens possibles (A-B, B-C, et C-A). Or, pour le réseau d'entraide à l'étude, composé de liens dirigés, les possibilités s'élèvent au nombre de 465 806 liens. Une fois les analyses réalisées, il en ressort que le réseau d'entraide présente une densité de 0,00247, c'est-à-dire que seulement 0,247% des liens possibles sont effectivement présents. Pour ce qui est du réseau de conflit, le nombre de liens possibles s'élevait à 158 006 liens et le résultat des analyses confirme une densité de 0,00347, c'est-à-dire qu'il y a présence de 0,347% des liens possibles dans ce réseau.

Toujours dans le but d'évaluer la cohésion de chacun des réseaux à l'étude, la mesure du coefficient d'agglomération a été prise. Cette mesure rend compte du niveau de connexion dans le voisinage de chaque acteur du réseau. Pour le bien du présent travail, c'est la version globale du coefficient d'agglomération qui a été considérée, permettant de connaître l'agglomération du réseau en tant que tel, plutôt que le coefficient local et spécifique de chacun des nœuds. Une valeur de coefficient d'agglomération élevée est caractéristique d'un réseau «petit monde» (*small world network*), c'est-à-dire un réseau où les contacts d'un acteur sont également liés entre eux. Les résultats des réseaux étudiés affichent un coefficient d'agglomération de 0,042 pour le réseau illustrant les relations d'entraide et de 0,091 pour celui des relations de conflit. Dans les deux cas, bien que la mesure soit plus élevée pour le réseau de conflit, la valeur du coefficient demeure faible. Zéro étant la valeur caractérisant habituellement les réseaux bâtis au hasard avec des acteurs aléatoires, il est possible de conclure que les deux réseaux à l'étude présentent une densité plutôt minimale.

Enfin, les résultats des analyses de la densité des réseaux d'entraide et de conflit permettent d'observer que tous deux présentent une tendance plus importante, bien que faible, à la division en sous-groupes, plutôt qu'à l'union de chacun de ses membres. Effectivement, tous deux exhibent un coefficient d'agglomération supérieur à la mesure de densité, ce qui dénote une faible connectivité entre les membres respectifs de chacun de ces réseaux et une tendance à la formation de cliques.

5.2.2 Centralité

Dans le cadre d'une analyse de réseau, les mesures de centralité sont souvent utilisées afin d'identifier les individus possédant le plus de pouvoir au sein de la communauté. Dans le cadre des réseaux à l'étude, les échanges et le partage d'information s'effectuent naturellement de l'acteur qui émet vers l'acteur qui reçoit. Pour cette raison, il a été conclu que la mesure de centralité de degré était la plus appropriée pour les besoins du présent travail, puisqu'elle permet de mesurer et qualifier directement les liens entre les individus qui composent les réseaux. Cette mesure indique le nombre de liens que possède chaque acteur, en plus de donner spécifiquement leurs liens entrants et sortants respectifs dans le cas de réseaux dirigés. Grâce à la centralité de degré, il est également possible de dégager un index de centralisation du réseau global. Cette mesure, basée sur la différence entre la centralité de l'acteur le plus central et tous les autres, indique la tendance d'un simple acteur d'être plus central que tous ses pairs impliqués dans le réseau. Il ressort des analyses effectuées que, le degré de centralisation du réseau d'entraide s'élève à 0,0134 pour les liens sortants et 0,0019 pour les liens entrants, alors que, pour le réseau de conflit, il n'est que de 0,0055 pour les liens sortants et 0,0009 pour les liens entrants. Bien que tous ces résultats témoignent d'une faible centralisation dans les réseaux, caractéristique des réseaux où tous les nœuds sont égaux, deux éléments demeurent dignes de mention. Tout d'abord, il est possible de noter que la centralisation est d'environ 2,5 fois plus importante dans le réseau d'entraide que dans celui de conflit. Toutefois, et c'est là le second élément qui ressort de ces résultats, bien que les valeurs de centralisation soient supérieures pour le réseau d'entraide, l'ordre de grandeur entre les liens sortants et entrants de chacun des réseaux demeure plutôt similaire. Effectivement, il apparaît que la centralisation des liens

sortants est six fois plus grande que pour les liens entrant dans le réseau de conflit, alors que ce taux s'élève à sept fois plus de liens sortants pour le réseau d'entraide. En d'autres termes, ces résultats révèlent que la centralisation est plus grande au niveau des relations d'entraide et que les individus qui reçoivent l'information (qu'elle soit positive ou négative) sont plus dispersés que ceux qui l'envoient.

Sur une note plus individuelle, certains utilisateurs ressortent des analyses comme étant des individus centraux des différents réseaux à l'étude. Comme mentionné précédemment, le concept de pouvoir, dans le domaine de l'analyse de réseaux sociaux, correspond à la capacité d'un acteur à contrôler l'information qui circule. C'est pourquoi, dans le contexte des analyses à l'étude, une attention particulière a été portée au degré de centralité entrant et sortant pour chacun des acteurs afin de révéler ceux ayant le rôle de mentor ou tyran (forte concentration de liens sortants) et d'apprenti ou victime (forte concentration de liens entrants). Suite à ces analyses, il a été possible de ressortir les degrés de centralité des liens sortants ainsi que des liens entrants pour chacun des acteurs de chacun des réseaux à l'étude. Pour chacune de ces mesures, une démarcation était observable entre le groupe d'individus ayant obtenu les résultats les plus élevés et le reste des acteurs du réseau. La mesure présentant le groupe d'acteurs le plus important comptait cinq utilisateurs avant d'observer cette démarcation. C'est pourquoi, par souci d'uniformisation, la présente section illustrera ces résultats en identifiant les cinq acteurs ayant obtenu les résultats les plus élevés pour chacune de ces mesures.

Grâce au Tableau 1, il est possible d'observer que l'utilisateur N343 est, de loin, le plus actif de la communauté en ce qui a trait à la distribution des enseignements. Effectivement, avec ses 148 liens sortants dans le réseau d'entraide, il va sans dire que cet utilisateur semble être le mentor principal du groupe. Il est d'ailleurs intéressant de noter que, de ces 148 liens, 110 (74,32%) sont pour des utilisateurs différents. Cette proportion semble indiquer que l'utilisateur N343 ne concentre pas ses interventions dans une clique spécifique, mais propage plutôt ses connaissances à un grand nombre de membres différents. Enfin, un dernier élément à souligner concerne la dernière colonne du tableau qui présente la proportion des liens de l'acteur par rapport à tous les liens sortants du réseau.

Avec son résultat de 0,054, il apparaît que l'utilisateur N343 produit 5,4% des liens sortants du réseau d'entraide. Ce résultat semble pointer vers l'existence d'un mentor qui s'adresse à l'ensemble du réseau, distribuant ainsi son savoir à une grand nombre d'apprentis.

Tableau 1. *Cinq utilisateurs présentant les degrés de centralité sortants les plus importants du réseau d'entraide*

Utilisateur	Nombre de liens sortants	Nombre de liens entrants	Proportion des liens sortants
N343	148,000	11,000	0,054
N242	85,000	1,000	0,031
N245	27,000	0,000	0,010
N416	22,000	0,000	0,008
N427	17,000	0,000	0,006

Par la suite, avec ses 108 liens sortant dans le réseau de conflit, l'utilisateur N343 ressort comme étant également le plus actif du réseau de conflit (voir Tableau 2). De ces 108 liens sortants, 78 (72,22%) s'adressent à des individus différents ce qui dénote de nouveau que cet acteur distribue ses interventions de manière dispersée et non concentrée en une seule clique d'acteurs. Ces résultats permettent donc de conclure qu'en plus d'être le mentor principal de la communauté, comme le propose les résultats du Tableau 1, N343 serait également le tyran principal du réseau de conflit. Un autre acteur digne de mention est l'utilisateur N242 qui émerge au second rang quant à sa centralité de degré sortant au sein des deux réseaux à l'étude. Bien que son nombre de liens sortants soit nettement inférieur à celui de N343, il demeure grandement supérieur à l'utilisateur occupant le troisième rang dans chacun de ces réseaux.

Tableau 2. *Cinq utilisateurs présentant les degrés de centralité sortants les plus importants du réseau de conflit*

Utilisateur	Nombre de liens sortants	Nombre de liens entrants	Proportion des liens sortants
N343	108,000	16,000	0,039
N242	54,000	6,000	0,019
N628	15,000	1,000	0,005
N387	7,000	0,000	0,003
N591	6,000	1,000	0,002

Aussi, il est intéressant de noter que la variation dans les résultats de la centralité de degré entrant, autant pour le réseau d'entraide que pour le réseau de conflit, est beaucoup moins prononcée que celle pour la centralité de degré sortant. Effectivement, avec la proportion de liens entrants la plus élevée des deux réseaux, l'utilisateur N168 n'obtient qu'un résultat de 0,008 (voir Tableau 3), c'est-à-dire qu'il concentre 0,8% des liens entrants du réseau auquel il appartient. Ce résultat semble pointer vers des apprentis qui reçoivent une quantité d'aide similaire de la part de leurs pairs, contrairement à ce qui a été mentionné précédemment sur l'existence d'un mentor principal s'adressant à une grande proportion du réseau.

Tableau 3. *Cinq utilisateurs présentant les degrés de centralité entrants les plus importants du réseau d'entraide*

Utilisateur	Nombre de liens entrants	Nombre de liens sortants	Proportion des liens entrants
N168	22,000	9,000	0,008
N789	22,000	0,000	0,008
N418	19,000	12,000	0,007
N223	18,000	0,000	0,007
N743	16,000	0,000	0,006

Un autre élément digne de mention dans le Tableau 3, concerne une fois de plus l'utilisateur N343, identifié précédemment, qui se retrouve au deuxième rang au niveau du degré de centralité entrant dans le réseau de conflit. C'est-à-dire que, de tous les acteurs de ce réseau, N343 est la deuxième victime de commentaires négatifs la plus fréquente du réseau. Ceci dit, la quantité de liens de conflit partant de cet utilisateur demeure nettement supérieure à ceux qu'il reçoit. Ce résultat laisse envisager que ces liens négatifs reçus proviennent de pairs lui ayant tenu tête suite à un commentaire négatif de sa part.

Tableau 4. *Cinq utilisateurs présentant les degrés de centralité entrants les plus importants du réseau de conflit*

Utilisateur	Nombre de liens entrants	Nombre de liens sortants	Proportion des liens entrants
N563	18,000	0,000	0,006
N343	16,000	108,000	0,006
N371	15,000	1,000	0,005
N815	15,000	0,000	0,005
N542	14,000	0,000	0,005

Enfin, les mesures de centralité ont permis d'observer que les acteurs possédant des degrés de centralité sortant importants présentaient rarement des degrés de centralité entrants notables, et vice-versa. Ces résultats indiquent une faible tendance chez les acteurs des réseaux à inverser les rôles. Ainsi, il semblerait qu'un acteur qui est considéré comme un mentor (ou un tyran) dans le réseau étudié n'agira que rarement en tant qu'apprenti (ou victime) et, au contraire, un apprenti (ou une victime) ne deviendra que rarement un mentor (ou un tyran). En d'autres termes, les acteurs des réseaux analysés, sur la période de temps étudiée, ne jouent que très rarement les deux rôles au sein d'un même réseau. Il est cependant important de noter que, compte tenu de la courte période de temps à l'étude, il aurait été surprenant d'observer un tel inversement dans les rôles d'un acteur.

5.2.3 Réciprocité

Dans le contexte de l'analyse d'un réseau dirigé, quatre types de relations dyadiques sont possibles : A et B ne sont pas connectés ; un lien existe partant de A et se dirigeant vers B ; un lien existe de B et se dirigeant vers A ; ou encore, A et B sont unis par un lien bidirectionnel. Ainsi, l'analyse de la réciprocité dans un réseau social mesure la probabilité que les acteurs soient mutuellement reliés, c'est-à-dire que les liens entre deux acteurs soient bidirectionnels. Dans les réseaux où un transfert d'information s'effectue, l'efficacité du réseau est d'autant plus importante si la réciprocité est élevée. Plus simplement, cela signifie que plus les liens entre les nœuds seront bidirectionnels, plus l'information circulera facilement dans le réseau.

La première mesure de réciprocité analysée dans le cadre de la présente étude correspond à la réciprocité globale de l'ensemble du réseau. Les résultats de cette mesure indiquent, pour le réseau d'entraide, que seules trois dyades sont symétriques sur les 997 présentes ce qui correspond à une réciprocité de 0,0030. De son côté, le réseau de conflit affiche une réciprocité de 0,0305, avec 14 dyades symétriques sur les 459 le composant. Ces résultats signifient que, de toutes les paires d'acteurs possédant une connexion dans le réseau d'entraide, 0,3% possèdent un lien bidirectionnel, alors que ce chiffre s'élève à 3,05% pour le réseau de conflit.

Deux autres mesures de réciprocité ont été désignées comme étant dignes d'intérêt dans le cadre du présent travail. La première de ces deux mesures permet de connaître, pour chaque acteur, la proportion des liens sortants qui ne sont pas symétriques, alors que la seconde indique la proportion de liens entrants qui sont symétriques. Plus simplement, la première mesure rend compte de la proportion de liens où un acteur enseigne sans rien recevoir en retour, alors que la seconde constate la proportion des apprentissage d'un acteur qui le mène à enseigner à son tour à son mentor.

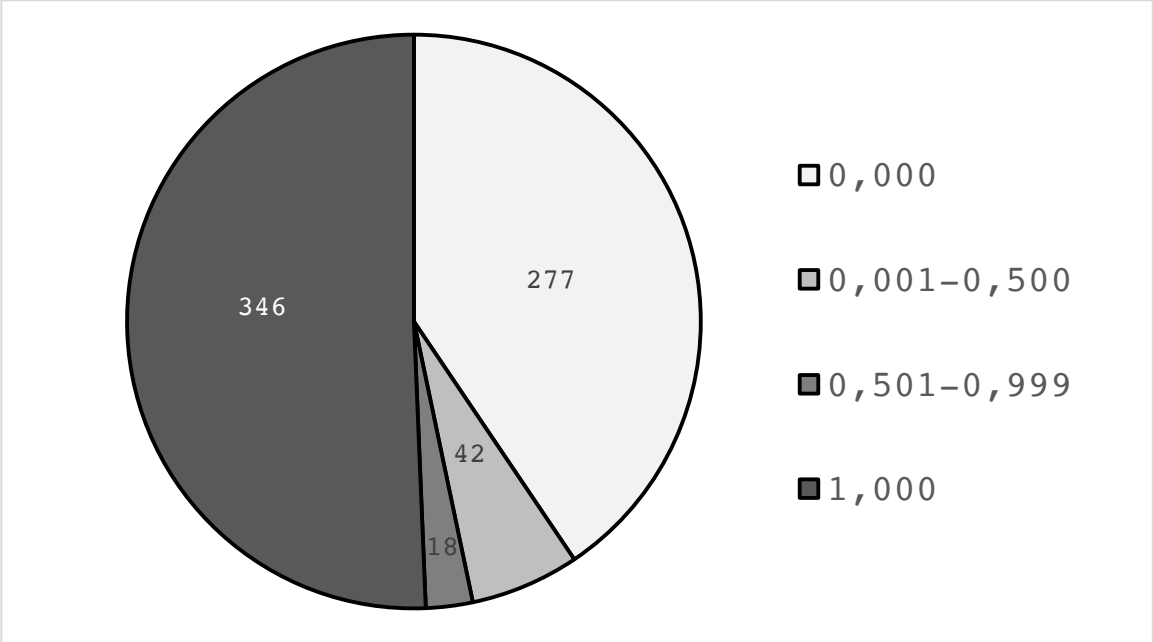

Figure 3. Diagramme circulaire de la répartition des acteurs du réseau d'entraide selon la proportion de leurs liens sortants qui sont non-symétriques.

Comme illustré par la Figure 3, il est possible de noter que plus de la moitié des membres du réseau d'entraide voient la totalité de leurs liens sortants non retournés. Effectivement, un effectif de 346 acteurs de ce réseau présente une proportion de 100% de leurs liens sortants qui sont non-symétriques. De l'autre côté, 277 utilisateurs voient la totalité de leurs liens sortants qui leur sont retournés, c'est-à-dire qu'ils affichent une proportion de 0,000 de leurs liens sortants qui ne sont pas symétriques. La Figure 4 présente les résultats de cette même mesure au niveau du réseau de conflit. Avec cette représentation graphique, il est possible d'observer que la répartition des deux réseaux est sensiblement similaire et donc, que plus de la moitié des acteurs du réseau de conflit ne voient pas leurs liens sortants être retournés par leur pairs.

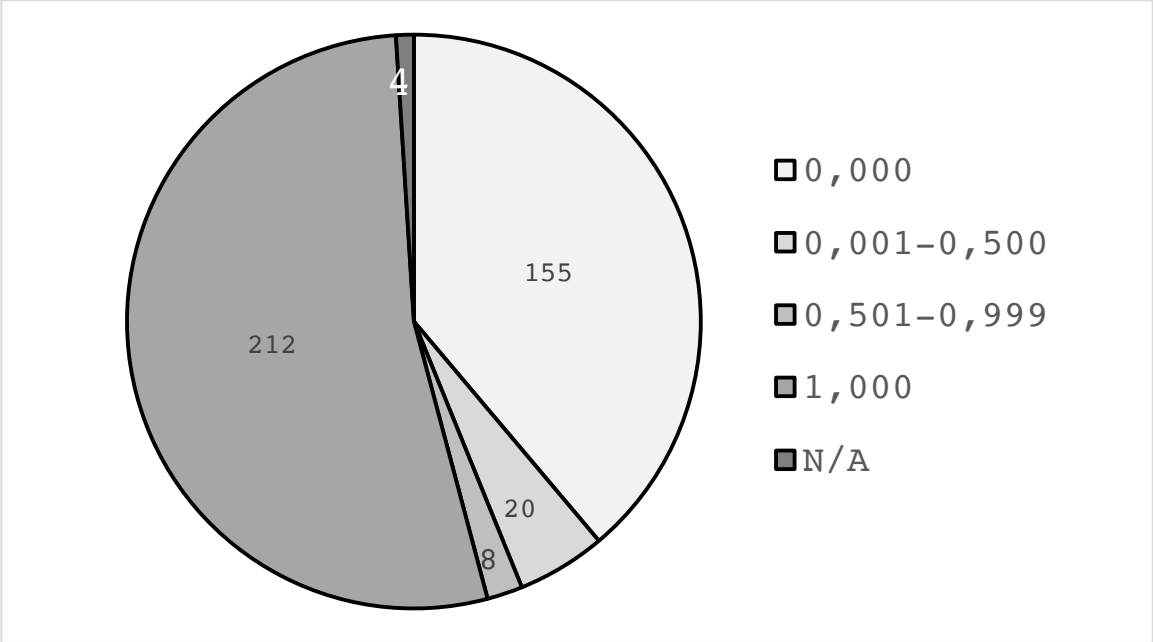

Figure 4. Diagramme circulaire de la répartition des acteurs du réseau de conflit selon la proportion de leurs liens sortants qui sont non-symétriques.

Enfin, en ce qui a trait aux liens entrants qui sont symétriques, ceux-ci sont beaucoup moins nombreux et ce, autant pour le réseau d'entraide que le réseau de conflit. Effectivement, les analyses révèlent uniquement deux acteurs dont les liens entrants sont symétriques pour le réseau d'entraide, soit les utilisateurs N80 et N752. Pour ces deux acteurs, 100% de leurs liens entrants sont symétriques, c'est-à-dire que, pour tous les apprentissages qu'ils font, ces derniers enseignent en retour à leur mentor. Pour le réseau de conflit, ces acteurs sont au nombre de neuf. Ces résultats viennent appuyer la conclusion déjà abordées de la tendance des membres de la communauté à se confiner dans un seul rôle, c'est-à-dire que ceux qui enseigne n'apprennent pas, et vice-versa.

5.2.4 Acteurs clés

L'identification des acteurs clés dans un réseau peut avoir plusieurs fonctions distinctes, dépendamment de l'objectif visé. Effectivement, elle peut permettre de perturber un réseau, si l'objectif est de retirer du réseau les acteurs identifiés ; d'améliorer un réseau, si l'objectif est d'aider ces acteurs clés ; d'influencer un réseau, si l'objectif est d'inciter les acteurs clés à adopter des comportements spécifiques ; d'apprendre sur un réseau, si l'objectif est

de se renseigner sur les individus les plus connectés ; et finalement, de rediriger le réseau, si l'objectif est de remplacer les acteurs clés par d'autres individus. Compte tenu de l'objectif général du présent travail qui consiste à mieux comprendre le processus d'apprentissage social chez les pirates informatique, il a été décidé de procéder à l'identification des acteurs clés afin de comparer les résultats obtenus pour chacun des réseaux et de déterminer qui sont les acteurs qui permettent à l'information de circuler dans chacun de ces réseaux. Afin d'y parvenir, et d'être en mesure d'identifier les acteurs les plus centraux pour chacun des réseaux, il a été décidé d'utiliser trois méthodes d'analyses distinctes. Comme chaque mesure n'évalue pas les acteurs clés de la même manière, les résultats ne seront pas nécessairement les mêmes pour chacune des mesures. C'est pourquoi, en utilisant plusieurs mesures, il sera possible de comparer les différents résultats obtenus et, ainsi, si certains acteurs ressortent avec plusieurs mesures, il sera plus évident que ces derniers sont des acteurs clés. Enfin, en ciblant ainsi les individus impliqués dans le cœur de chacun des réseaux, c'est-à-dire dans la clique la plus active des réseaux, il sera possible de connaître ceux qui facilitent les échanges dans chacun des réseaux et de comparer les résultats des deux réseaux à l'étude.

La première analyse choisie est celle du cœur/périphérie en mode continu. La structure cœur/périphérie d'un réseau social est définie par un cœur, aussi appelé noyau, où les acteurs sont unis et présentent une grande concentration des liens, ainsi qu'une périphérie où les nœuds sont plus étendus et faiblement connectés. Ainsi, les acteurs identifiés comme faisant partie du noyau du réseau sont alors considérés comme les acteurs clés de ce réseau. L'analyse du cœur/périphérie en mode continu considère le réseau à analyser, suggère un nombre de nœuds à considérer dans le noyau du réseau et classe tous les acteurs en fonction de leur *coreness*. Le terme *coreness* utilisé dans le contexte de l'analyse de réseau ne possède pas d'équivalent exact dans la langue française, de ce fait, et pour le bien du présent travail, le terme *centralité* sera utilisé afin de référer au coreness. La mesure de centralité est un indicateur de la position de chaque acteur par rapport au point central du cœur du réseau. Ainsi, plus la centralité est élevée, plus cet acteur se trouve près du centre du cœur.

Les Figures 5 et 6 présentent les résultats des analyses du cœur/périphérie en mode continu pour les réseaux d'entraide et de conflit en ce qui a trait à la centralité. Ainsi, pour le réseau d'entraide, les résultats proposent un cœur composé de trois utilisateurs soit N242 avec une centralité de 0,714, N427 avec une centralité de 0,513 et N343 avec une centralité de 0,313. Pour le réseau de conflit, les résultats suggèrent un cœur composé d'un seul acteur, c'est-à-dire l'utilisateur N343 avec une centralité de 0,943. Il est également intéressant de noter que parmi les 683 utilisateurs composant le réseau d'entraide, seuls 22 d'entre eux possédaient une centralité supérieure à 0 et que pour le réseau de conflit, il est question de 18 utilisateurs parmi les 399 formant le réseau. Ces résultats témoignent, pour les deux réseaux à l'étude, d'une périphérie très importante et une grande disparité entre les nœuds associés au cœur et ceux associés à la périphérie de chacun des réseaux.

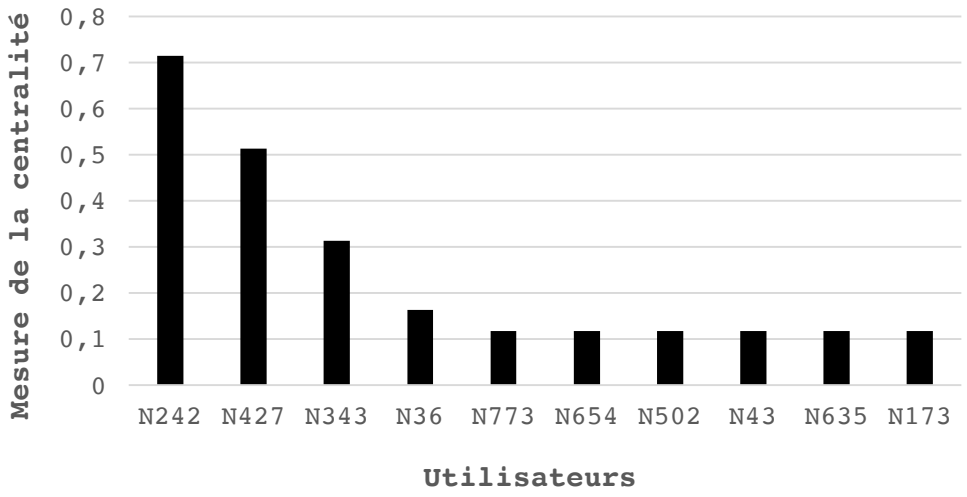

Figure 5. Représentation graphique des 10 utilisateurs ayant la centralité la plus élevée dans le réseau d'entraide

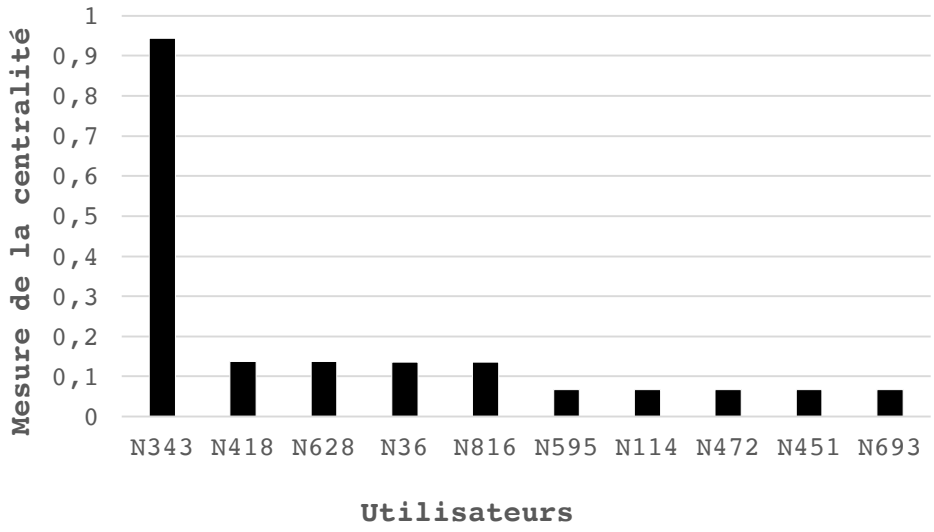

Figure 6. Représentation graphique des 10 utilisateurs ayant le coreness le plus élevé dans le réseau de conflit

La seconde mesure utilisée afin d'identifier les acteurs clés est celle du cœur/périphérie en mode catégoriel. À la différence du mode continu, le mode catégoriel sépare directement les acteurs en deux groupes, soit un pour le cœur et le second pour la périphérie. Suite aux analyses, six acteurs ont été identifiés comme faisant partie du cœur dans le réseau d'entraide alors que seulement quatre sont ressortis dans le cœur du réseau de conflit. Pour le réseau d'entraide, ce sont les utilisateurs N168, N242, N343, N442, N196 et N418 qui se distinguent de la périphérie. En ce qui a trait au réseau de conflit, aux trois utilisateurs N242, N343 et N418 qui se distinguent de nouveau s'ajoutent l'utilisateur N815 afin de compléter le cœur du réseau.

Enfin, la troisième et dernière mesure utilisée pour identifier les acteurs clés des réseaux à l'étude, est obtenue à l'aide du logiciel KeyPlayer 2. Cette mesure permet à l'analyste d'effectuer des simulations en choisissant un nombre d'acteurs à retirer du réseau et le logiciel répond en évaluant le pourcentage de fragmentation du réseau qui en résulte et en identifiant les acteurs à retirer afin d'obtenir ce pourcentage. La Figures 7 présente les courbes des pourcentages de fragmentation en fonction des différentes simulations qui ont été menées par l'analyste. Le trait le plus pâle représente les résultats pour le réseau d'entraide, alors que le plus foncé représente le réseau de conflit.

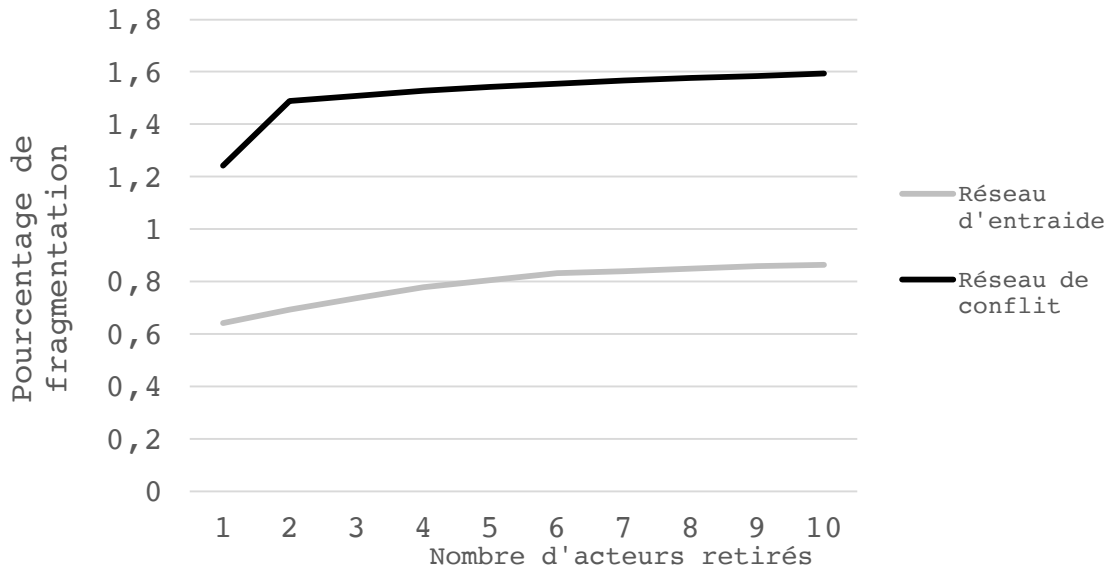

Figure 7. Représentation graphique des pourcentages de fragmentation en fonction du nombre d'acteurs retirés pour les réseaux d'entraide et de conflit

Comme illustré par ce graphique, le pourcentage de fragmentation est plus élevé pour le réseau de conflit et ce, quel que soit le nombre d'acteurs retirés. Il est également possible d'observer que la courbe du réseau de conflit connaît une augmentation rapide au début, mais atteint son plateau assez rapidement, c'est-à-dire à partir du retrait de trois acteurs. Selon les résultats dans le logiciel KeyPlayer 2, les trois acteurs qui devraient être retirés du réseau de conflit pour obtenir ce pourcentage de fragmentation sont les utilisateurs N242, N343 et N371. En ce qui a trait au réseau d'entraide, la progression de la courbe est plus constante que celle du réseau de conflit. Toutefois, il est tout de même possible d'observer que cette progression ralentie lorsque le nombre d'acteurs retirés est de sept. Ces sept acteurs clés à retirer afin d'obtenir le pourcentage de fragmentation évalué sont N46, N168, N242, N250, N343, N418 et N591. En considérant ces résultats, il est toutefois important de mentionner que le pourcentage de fragmentation demeure plutôt faible pour les deux réseaux. Cela pourrait être causé par la faible densité du réseau observée précédemment. Ainsi, comme les acteurs sont peu reliés entre eux et que la tendance des réseaux tend davantage vers la formation de clique, le retrait d'acteurs aura un impact limité sur la fragmentation du réseau complet, que ce soit pour le réseau d'entraide ou de conflit.

Pour conclure, le Tableau 5 présente les différents utilisateurs ayant été identifiés comme des acteurs clés selon chacune des mesures utilisées. Il est donc possible d'observer que l'utilisateur N343 est identifié comme un acteur clé par toute les mesures autant pour le réseau d'entraide de que le réseau de conflit. Similairement, l'acteur N242 est ressort pour les trois mesures du réseau d'entraide et pour deux d'entre elles pour le réseau de conflit. Enfin, les utilisateurs N168 et N418 sont chacun identifié deux fois comme des acteurs clés pour le réseau d'entraide. Selon ces résultats, il semble justifié de conclure que les acteurs clés, c'est-à-dire ceux qui sont les plus impliqués dans la clique la plus active du réseau et qui, par le fait même, facilite les échanges dans les réseaux, sont N242, N343, N168 et N418 pour le réseau d'entraide. Tandis que pour le réseau de conflit, ces acteurs sont N343 et N242.

Tableau 5. *Résumé des résultats pour les acteurs clés en fonction de la mesure utilisée pour les réseaux d'entraide et de conflit.*

	Méthodes de mesures utilisées	**Utilisateurs identifiés comme acteurs clés**
Réseau d'entraide	**Cœur/Périphérie en mode continu**	N242, N427, N343
	Cœur/Périphérie en mode catégoriel	N168, N242, N343, N442, N196, N418
	Logiciel KeyPlayer 2	N46, N168, N242, N250, N343, N418, N591
	Méthodes de mesures utilisées	**Utilisateurs identifiés comme acteurs clés**
Réseau de conflit	**Cœur/Périphérie en mode continu**	N343
	Cœur/Périphérie en mode catégoriel	N242, N343, N418, N815
	Logiciel KeyPlayer 2	N242, N343, N371

CHAPITRE 6 – DISCUSSION

Suite aux résultats présentés précédemment, il est possible de tirer certaines conclusions et d'émettre des hypothèses qui viendront confirmer ou réfuter les connaissances actuelles provenant de la littérature dans le domaine de la cyberdélinquance. La présente section se veut donc une discussion sur les résultats obtenus et leur signification quant aux théories abordées afin d'être en mesure de répondre aux objectifs posés dans le cadre de ce travail.

6.1 Qualifier les liens d'entraide favorisant l'apprentissage

La première étape établie dans le but de mieux comprendre le processus d'apprentissage social chez les pirates informatiques, est de caractériser les liens d'entraide au sein de cette communauté. Pour ce faire, et comme il a été présenté précédemment, plusieurs analyses de la structure du réseau affichant les liens d'entraide ont été effectuées et plusieurs résultats dignes d'intérêt ont pu en être dégagés. Avant toute chose, la distribution des acteurs et des liens dans le réseau d'entraide laisse voir une organisation où quelques acteurs semblent concentrer les liens en son centre et où plusieurs petites cliques distinctes sont visibles en périphérie. Afin de corroborer ces observations, des mesures de densité, de centralité et de réciprocité ont été produites.

Tout d'abord, les analyses de la densité ont permis de constater que seulement 0,247% des liens possibles dans le réseau d'entraide sont effectivement présents et de révéler un coefficient d'agglomération de 0,042 (4,2%). Ces deux résultats plutôt faibles sont caractéristiques d'une cohésion minimale au sein du réseau ainsi que d'une légère propension à la formation de cliques. Ces résultats ne sont pas sans rappeler les propos de Sutherland (1947) mentionnant que les petits groupes favorisent l'apprentissage de nouveaux comportements. Ces résultats viennent également confirmer la position selon laquelle les relations interpersonnelles en ligne sont caractérisées par leur nature éphémère et la fragilité des liens unissant les individus (Décary-Hétu, 2013 ; Coleman, 2014 ; Jordan et Taylor, 1998 ; Abbasi, Li, Benjamin, Hu et Chen, 2014).

Par la suite, les résultats des analyses de centralité révèlent une centralité de degré sortant pour le réseau d'entraide de 0,0134 et une centralité de degré entrant de 0,0019. Ces résultats, bien que faibles, indiquent une tendance plus marquée pour la centralisation des liens sortants, c'est-à-dire les liens allant d'un mentor vers un apprenti. En d'autres termes, ces données indiquent qu'il est plus probable de constater, dans le réseau d'entraide, un mentor qui propage ses enseignements à un grand nombre de novices que le contraire. Ces résultats abondent d'ailleurs dans le même sens que les conclusions de Zhang, Tsang, Yue et Chau (2015), qui affirment que les hackers les plus expérimentés sont ceux qui partagent la plus grande quantité d'information au sein de la communauté. Les analyses de la centralité ont également permis d'identifier les acteurs concentrant le plus de liens entrants et/ou sortants. Pour le réseau d'entraide, il ressort qu'avec 148 liens sortants, l'utilisateur N343 est le mentor le plus important du réseau, suivi par N242 avec 85 liens sortants, N245 à 27 liens, N416 à 22 liens et finalement N427 à 17 liens sortants. Au niveau des liens entrants, ce sont les utilisateurs N168 et N789 qui arrivent tous deux au premier rang avec un total de 22 liens, suivi de N418 à 19 liens, N223 à 18 liens et N743 à 16 liens entrants. Avec ces résultats, il est possible d'observer que N343 et N242, présentent une quantité de liens très au-dessus des autres acteurs identifiés. Cela vient d'ailleurs corroborer la conclusion énoncée précédemment selon laquelle les mentors sont plus à même de développer des relations avec une quantité importante d'apprentis (Zhang, Tsang, Yue et Chau, 2015). Enfin, en s'intéressant spécifiquement à l'utilisateur N343, il a été possible de déterminer que ce dernier dirige près de 75% de ses liens sortants vers des utilisateurs différents, ce qui dénote un désir de partage d'information important de la part de cet acteur. Ce résultat n'est pas sans rappeler les propos relevés de la littérature relatant la propension de la communauté des pirates informatiques à reposer sur le partage des connaissances et des outils (Holt, 2007, cité dans Décary-Hétu, 2013, Raymond, 2003)

Finalement, il a été possible de ressortir des analyses que la réciprocité globale du réseau d'entraide est de 0,0030 avec seulement trois dyades qui sont symétriques sur les 997 qui composent le réseau. C'est-à-dire que 0,3% de toutes les paires d'acteurs qui composent le réseau présentent un lien bidirectionnel, toutes les autres sont constituées de liens dirigés. En s'intéressant plus en détail à ce concept, il a été possible d'observer que plus de la moitié

des acteurs du réseau d'entraide voient leurs liens sortant non retournés par l'acteur qui le reçoit et que seuls deux acteurs présentent des liens entrants symétriques. Ce résultat semble signifier que les relations entre deux acteurs sont basées sur une certaine compréhension des rôles de chacun et que ceux-ci ne varient pas au fil des échanges. Ainsi, pour une relation où le mentor et l'apprenti sont définis dès le départ, il sera très rare de voir les rôles s'inverser et voir l'apprenti devenir le mentor de son mentor. Toutefois, il est important de mentionner que ces conclusions sont tirées grâce aux données récoltées sur une période de seulement un mois. Peut-être qu'avec une collecte plus longue les résultats seraient différents. Cette limite sera abordée plus en profondeur dans une prochaine section.

En conclusion, grâce aux analyses effectuées et à l'interprétation qui a été faite des résultats obtenus, il est possible de proposer un modèle d'apprentissage observé chez les pirates informatiques. Il semble effectivement que la communauté des hackers présente un processus d'apprentissage qui se fait directement d'un mentor vers un apprenti en relation un à un ou en petit groupe très restreint. Bien qu'il soit rare de voir un mentor enseigner à plusieurs apprentis en même temps, il n'en demeure pas moins que chaque mentor distribue habituellement leur savoir à plusieurs individus différents dans la communauté. Enfin, pour ce qui est des apprentis, ces derniers sont souvent liés à plusieurs mentors simultanément, leur permettant ainsi d'apprendre de plusieurs sources différentes.

6.2 Qualifier les liens de conflit nuisant à l'apprentissage

Le second objectif spécifique de la présente étude était de qualifier les liens de conflit entre les membres de la communauté des pirates informatiques afin d'en voir l'impact sur le partage d'enseignements. Comme il a pu être observé dans la section portant sur les résultats, les liens au sein du réseau de conflit sont sensiblement similaires à ceux constatés dans le réseau d'entraide. Ainsi, la présente sous-section fera état des résultats notables concernant le réseau de conflit et les mettra en relation avec les observations proposées ci-haut.

Tout d'abord, au niveau de la distribution du réseau, il est possible d'observer que cette dernière est grandement similaire à celle signalée pour le réseau d'entraide. Effectivement, bien que comptabilisant moins d'acteurs, le réseau de conflit présente une configuration analogue où il est possible de voir quelques rares acteurs centraux qui cumulent une majorité de liens et plusieurs unités isolées en périphérie. Ainsi, à première vue, la structure du réseau de conflit semble caractériser un réseau où la cohésion est faible et le pouvoir est concentré dans quelques acteurs spécifiques. Comme cela avait été le cas pour le réseau d'entraide, ces observations préliminaires quant à la structure interne du réseau de conflit ont été validées par des analyses plus approfondies quant à la densité, la centralité et la réciprocité des liens qui le compose.

Tout d'abord, le résultat pour la densité globale du réseau de conflit s'élève à 0,00347, c'est-à-dire que 0,347% des liens possibles sont effectivement présents dans ce réseau. De plus, le coefficient d'agglomération observé pour le réseau de conflit est de 0,091. Pour ces deux mesures, quoique demeurant plutôt faibles, les résultats du réseau de conflit sont supérieurs à ceux qui ont pu être relevés pour le réseau d'entraide. Effectivement, il apparaît que la cohésion du réseau de conflit est plus importante que celle du réseau d'entraide, bien que les valeurs révélées présentes encore une tendance pour le réseau à la formation de clique, dû au coefficient d'agglomération qui surpasse la densité. Cette différence entre les résultats des deux réseaux à l'étude pourrait être expliquée par le fait que, dans une situation de conflit, plusieurs individus peuvent vouloir venir ajouter leur grain de sel à la conversation. Au contraire, lorsqu'un apprentissage est fait, suite à une réponse satisfaisante à la question d'un apprenti, il est rare de voir un autre utilisateur renchérir et répondre de nouveau à la question. Or, pour les situations de conflit, suite à un commentaire négatif d'un tyran vers une victime, il est plus fréquent de voir des utilisateurs qui choisissent de s'impliquer dans la conversation en faisant part, eux aussi, de leur opinion sur le sujet. Cela pourrait donc expliquer pourquoi, bien que les acteurs soient moins nombreux pour le réseau de conflit, les liens entre ces derniers y sont vraisemblablement plus dense que dans le réseau d'entraide.

Pour leur part, les mesures de centralisation globale du réseau de conflit sont de 0,0055 pour les liens sortants et 0,0009 pour les liens entrants. Avec une valeur plus de six fois supérieure, la centralisation des liens sortants est, comme c'était le cas dans le réseau d'entraide, plus importante que celle des liens entrants. Cela signifie donc qu'il est plus probable de voir un même tyran dispenser plusieurs commentaires négatifs que de voir une même victime en recevoir une panoplie. Au niveau individuel, il a été possible d'établir qui sont les utilisateurs les plus centraux, autant pour les liens sortants que les liens entrants, dans le réseau de conflit. Il en ressort que les acteurs ayant le plus de liens sortants sont N343 avec un total de 108 liens, N242 avec 54 liens, N628 avec 15 liens, N387 avec sept liens et finalement N591 avec six liens. De ces résultats, deux éléments sont dignes de mention. Premièrement, il est possible de noter que l'utilisateur N343 et N242 sont une fois de plus les individus présentant le plus de liens sortants, comme c'était le cas dans le réseau d'entraide. Deuxièmement, ces deux acteurs présentent un nombre total de liens hautement supérieur à celui des autres acteurs analysés. Ces données extrêmes pourraient d'ailleurs venir expliquer, en partie, la différence entre la centralisation globale obtenue pour les liens sortants et les liens entrants. Enfin, les utilisateurs comptant le plus de liens entrants sont N563 avec 18 liens, N343 avec 16 liens, N371 et N815 avec 15 liens et finalement N542 avec 14 liens. Comme il avait été soulevé lors de la présentation de ces résultats, l'utilisateur N343 se trouve de nouveau dans les acteurs les plus centraux, ce qui signifie qu'il est non seulement le tyran le plus central de ce réseau, mais également l'une des victimes de commentaires négatifs les plus fréquentes. Or, ce résultat peut être expliquer par l'implication de cet acteur dans une grande proportion des échanges, augmentant ainsi ses chances d'être la cible de conflit avec d'autres membres du réseau. Effectivement, à la lecture des échanges sur le forum de discussion au cours de la collecte de données, il a été possible d'observer que plusieurs éléments pouvaient entraîner une réaction conflictuelle de la part d'un utilisateur et plus précisément ceux ressortant comme les tyrans principaux du réseau. Ainsi, il a été noté que les utilisateurs qui ne faisaient aucun effort pour apprendre (c'est-à-dire qu'ils posaient des questions déjà posées et répondues, qu'ils n'utilisaient pas la terminologie adéquate pour poser leur question, qu'ils ne cherchaient pas à apprendre une technique de piratage, mais à ce que les utilisateurs du forum l'exécutent pour eux, etc.) s'attiraient davantage les foudres de la communauté, ce

qui n'est pas sans rappeler le comportement et les attitudes des *crackers* mentionnés précédemment (Barber, 2001 ; Sehn, 2002 ; Raymond, 2003 ; Mitnick et Simon, 2011 ; eduCBA, 2016). Au contraire, les utilisateurs polis, démontrant un intérêt pour l'apprentissage et disposés à faire les efforts nécessaires étaient beaucoup plus à même d'obtenir l'aide qu'ils recherchaient.

Enfin, la mesure de réciprocité globale du réseau de conflit affiche 14 dyades symétriques sur les 459 le composant, ce qui correspond à 3,05% des paires d'acteurs qui possèdent une connexion bidirectionnelle. Plus spécifiquement, comme cela était le cas pour le réseau d'entraide, il ressort que plus de la moitié des acteurs du réseau voient la totalité de leurs liens sortants non retournés. Toutefois, il apparaît que le nombre de liens entrants symétriques est plus élevé dans le réseau de conflit que pour celui d'entraide. D'ailleurs, neuf acteurs voient la totalité de leurs liens entrant être symétriques. Ce résultat peut être expliquer par une propension, chez les victimes de commentaires négatifs, à se défendre et répliquer à leurs assaillant par un nouveau commentaire négatif, rendant ainsi les liens entre les deux, symétriques. Au contraire, les relations d'entraide et de partage d'information, souvent qualifiées par leur caractère utilitaire (Craig, 2005 ; Choo, 2008 ; Abbasi, Li, Benjamin, Hu et Chen, 2014), ont tendance à être à sens unique et à cesser une fois l'information partagée par le mentor. D'ailleurs, compte tenu de cette tendance habituelle à la rétorque chez les individus qui se voient insultés et à l'anonymat et le sentiment d'impunité qui caractérise les échanges en ligne, il est plutôt intéressant de noter que le taux de réciprocité n'est pas plus élevé pour le réseau de conflit. Il serait intéressant, pour une recherche future, de considérer le cheminement des individus victime de commentaires négatifs afin d'en apprendre plus sur les techniques de gestion de conflit chez la communauté des pirates informatiques.

En conclusion, comme il avait été possible de le faire pour les relations d'entraide, certaines propositions peuvent être faites afin de caractériser les relations de conflits entre les hackers d'une même communauté. Ainsi, les conflits semblent se produire au sein de petits groupes. Tout comme pour l'apprentissage, les tyrans du réseau de conflit propagent leurs commentaires négatifs à de nombreuses victimes différentes et les victimes semblent

recevoir des messages de conflits provenant de quelques tyrans simultanément. Une différence notable entre les deux réseaux tient dans la réciprocité des liens puisque, bien que faible pour le contexte d'internet, comme il a été mentionné précédemment, les victimes de conflits semblent retourner leurs liens plus souvent que les apprentis. C'est donc dire que ces derniers répliquent davantage à leurs assaillants. Enfin, il apparaît que les relations de conflit sont, somme toute, moins nombreuses que celles d'apprentissage, laissant apparaître une tendance de la communauté des pirates informatiques au partage de savoir et à l'entraide.

6.3 Comparer les acteurs clés des deux réseaux à l'étude

Finalement, le troisième et dernier objectif spécifique de la présente étude consistait à comparer les deux réseaux à l'étude grâce, entre autres à l'identification des acteurs clés des réseaux d'entraide et de conflit. Tout d'abord, en s'intéressant uniquement à la composition de ces deux réseaux, il est possible d'observer que les situations d'entraide, et donc d'apprentissage, sont beaucoup plus fréquentes que celles de conflit. Effectivement, avec ses 683 acteurs impliqués dans un total de 1152 liens, le réseau d'entraide compte un peu plus de 1,7 fois le nombre de participants du réseau de conflit et plus du double de liens recensés. Ce résultat vient d'ailleurs confirmer les données de la littérature présentant la communauté des hackers comme prompte à la solidarité entre ses membres et ouverte à tous, principalement ceux qui désirent apprendre (Raymond, 2003).

Ensuite, un élément important afin de comparer les réseaux d'entraide et de conflit réside dans les acteurs clés de ces réseaux respectifs. À ce sujet, les résultats permettent de distinguer quatre acteurs clés pour le réseau d'entraide et deux pour le réseau de conflit. Ainsi, au sein du réseau d'entraide, les utilisateurs N343, N242, N168 et N418 sont reconnus comme étant les acteurs clés les plus impliqués dans les échanges d'informations qui s'y opèrent. Pour le réseau de conflit, ce sont les acteurs N343 et N242 qui s'illustrent comme acteurs clés. Le réseau d'entraide comptant un nombre de participants plus élevé que celui de conflit, il n'est pas surprenant de voir que ce dernier propose un nombre d'acteurs clés plus important. Toutefois, un élément digne d'intérêt à ce propos tient au fait

que, malgré la quantité importante d'acteurs composant les deux réseaux à l'étude, très peu d'entre eux s'illustrent comme des acteurs clés. En effet, comme il a été relaté dans la section des résultats, la méthode permettant d'identifier le maximum d'acteurs clés n'a permis d'en distinguer que sept pour le réseau d'entraide et quatre pour le réseau de conflit. Afin d'expliquer ces résultats, il est possible d'évoquer la nature éphémère et volatile des relations bâties au sein de la communauté des pirates informatiques (Décary-Hétu, 2013 ; Coleman, 2014 ; Jordan et Taylor, 1998 ; Abbasi, Li, Benjamin, Hu et Chen, 2014). Effectivement, puisqu'il n'est pas rare de voir des membres se joindre ou quitter la communauté sur une base régulière, les interactions observées ont tendance à être de courte durée et superficielles. De ce fait, les individus qui persistent et qui adhèrent pleinement à la communauté sont plus susceptibles d'acquérir les connaissances qui leurs permettront de devenir experts dans le domaine, contrairement à ceux qui quittent la communauté et qui demeureront des novices. Ces conclusions expliquent le fait que les réseaux analysés présentent une faible proportion de mentors, persistants dans la communauté et partageant leurs connaissances, pour une grande quantité de novices, débutant dans le domaine et se joignant aux discussions.

Un autre élément intéressant relaté par ces résultats tient au fait que les deux acteurs identifiés pour le réseau de conflit se distinguent également au niveau du réseau d'entraide. Cela signifie que les mêmes individus qui sont le plus impliqués dans le processus d'apprentissage pour les novices, les mentors les plus importants du réseau d'entraide, sont également responsable de la grande majorité des échanges de conflits qui s'opèrent dans la communauté étudiée. Bien que ce résultat puisse sembler étonnant de prime abord, il n'est pas sans rappeler les propos de la littérature quant à la relation entretenue entre les hackers et les crackers (Sehn, 2002 ; eduCBA, 2016 ; Raymond, 2003 ; Barber, 2001 ; Mitnick et Simon, 2011). Effectivement, comme établi par Zhang, Tsang, Yue et Chau (2015), les individus responsables du plus grand partage d'information dans la communauté sont vraisemblablement ceux qui possédant la plus grande expertise dans le domaine. Ainsi, il est possible de conclure que N343 et N242 sont les hackers possédant les connaissances les plus importantes de la communauté à l'étude. Or, il a également été illustré dans la littérature que, bien que basée sur le partage d'information et la collectivité, la communauté

des pirates informatiques ne possèdent que très peu de patience et de respect pour les individus qui ne fournissent pas les efforts nécessaires à leurs apprentissages. De ce fait, il n'est pas contre-intuitif de voir les pirates les plus expérimentés d'un réseau être également les mieux placés pour reconnaître les membres mal intentionnés ou n'adhérant pas aux valeurs de la sous-culture des hackers. Ainsi, en tant qu'experts des réseaux analysés, N343 et N242 sont plus à même de s'opposer à ces individus et c'est pourquoi ils s'illustrent comme acteurs clés autant au sein du réseau d'entraide que de conflit.

CONCLUSION

L'objectif général de la présente étude était de comprendre le processus d'apprentissage social chez les pirates informatiques. Pour ce faire, une collecte de données a été effectuée sur le forum de discussion hackforum.net en classant les interactions selon qu'elles participaient à des relations d'entraide ou de conflit entre les différents utilisateurs. Avec ces données, deux réseaux ont été produits afin d'illustrer ces relations. Puis, des analyses de densité, de centralité et de réciprocité ont été effectuées pour les deux réseaux afin d'être en mesure de qualifier les liens les composant et d'en étudier les impacts sur le processus d'apprentissage des hackers. Enfin, une analyse critique des réseaux d'entraide et de conflit a été effectuée en misant principalement sur l'identification des acteurs clés de chacun.

Selon la littérature considérée et le cadre théorique envisagé, il était attendu que les participants centraux des réseaux analysés soient les plus expérimentés et, de ce fait, ceux qui partagent le plus leurs connaissances avec les participants novices de la communauté. Suite aux analyses, il est possible de conclure que les résultats obtenus par la présente étude abondent dans le même sens que la littérature en ce qui a trait à ces deux concepts. Il a été possible d'établir qu'un acteur spécifique se distingue comme étant central et ce, dans tous les aspects du réseau. Ainsi, l'utilisateur N343 est reconnu comme central autant en ce qui a trait à ses liens d'entraide que ceux de conflit. En conséquence, il est possible de conclure que cet acteur est un mentor pour un grand nombre d'utilisateurs du forum de discussion et que, possédant un certain pouvoir dans la communauté, ce dernier se permet de se dresser contre les utilisateurs qu'il considère indignes de son attention. Cette attitude est également observée chez l'utilisateur N242 qui est identifié au second rang des acteurs clés dans les deux réseaux. Grâce à ces résultats, il a été possible de conclure que, comme la littérature le mentionnait, les mentors en situation d'apprentissage sur les forums de discussion tendent à propager leurs connaissances aux utilisateurs novices, tout en ayant une patience limitée pour les individus qui n'adhèrent pas aux valeurs de la communauté des pirates informatiques. Enfin, il a également été possible de conclure que, toujours en accord avec la littérature, les apprentissages s'effectuent grâce à une petite quantité de mentors qui enseignent à une grande quantité d'apprentis et qu'une fois établis, les rôles au sein des échanges et des interactions ont tendance à demeurer les mêmes pour les acteurs impliqués.

En d'autres termes, un individu qui joue le rôle de mentor conservera vraisemblablement ce rôle tout au long de ses échanges.

Malgré les conclusions qui ont pu être tirées de la présente étude, il est important de mentionner quelques éléments en ayant limités les implications. La première limite à mentionner concerne la période de temps couverte par la collecte de données. Effectivement, pour des raisons de logistique, il avait été décidé d'entrée de jeu de collecter les données disponibles uniquement pour le mois de janvier 2017. Or, ce court intervalle restreint les analyses qui ont pu être effectuées dans le cadre de ce travail. Une période plus longue aurait encouragé des analyses temporelles, permettant ainsi d'observer l'évolution des participants des différents réseaux. Ainsi, il aurait été possible, entre autres, de voir après combien d'enseignements un novice a acquis suffisamment de connaissances pour devenir mentor à son tour. Enfin, une autre limite observée provient de la source des données en elle-même. Comme il a été mentionné précédemment, les données récoltées sont toutes issues d'un seul et même forum de discussion ce qui limite la possibilité de généralisation des conclusions proposées. Ayant bénéficié de ressources supplémentaires, il aurait été intéressant de multiplier les forums de discussion explorés afin de les comparer entre eux ou encore d'accéder aux messages privés entre les utilisateurs des forums afin de comparer les relations qui apparaissent au public et celles qui demeurent privées. Ce faisant, il aurait été possible d'observer comment les liens d'entraide et de conflit évoluent d'un forum à l'autre ou d'un contexte à l'autre (public vs. privé).

Pour conclure, bien que la présente étude ait permis de confirmer des notions connues dans la littérature et d'approfondir les connaissances concernant le processus d'apprentissage dans la communauté des pirates informatiques, certaines avenues demeurent inexplorées. Ainsi, pour faire suite et pousser plus loin la réflexion sur le sujet, des futures études pourraient s'intéresser spécifiquement aux acteurs clés afin d'en établir les profils (connaître le temps qui s'est écoulé depuis leur adhésion au forum, le nombre de messages qu'ils publient, les membres avec qui ils interagissent, etc.). De cette manière, un réseau égocentrique pourrait être construit autour de ces acteurs, permettant ainsi d'en apprendre davantage sur une autre facette de cette communauté que forment les pirates informatiques.

INTÉGRATION

Le présent travail s'inscrit dans un processus d'intégration de deux disciplines connexes et complémentaires, soit la criminologie et les sciences forensiques. Dans cette perspective, la combinaison de ces deux sciences peut être constatée sous trois angles distincts dans le contexte de la présente étude.

Tout d'abord, par sa méthodologie reposant sur des données colligées sur un forum de discussion et sur l'analyse de réseaux sociaux, cette étude permet l'intégration des sciences forensiques comme vecteur de connaissances criminologiques. Dans un premier temps, l'utilisation de traces numériques laissées par les participants du forum de discussion choisi (hackforum.net) a permis de suivre les interactions des différents individus entre eux. De cette manière, les noms d'utilisateurs, les métadonnées des communications entre les utilisateurs et le contenu de ces communications ont pu être analysés. Ces analyses ont permis d'illustrer les réseaux des interactions entre les hackers et de mettre en lumière les relations de pouvoir qui s'exercent au sein de ce réseau. Les résultats obtenus ont favorisé l'acquisition de connaissances plus complètes et approfondies du phénomène d'apprentissage social en ligne chez les pirates informatiques. Dans cette perspective, les traces numériques utilisées dans le cadre de ce travail ont permis d'approfondir les connaissances sur les habitudes et les comportements des hackers et ainsi, développer une meilleure compréhension de leurs pratiques criminelles.

Ensuite, les connaissances criminologiques du phénomène de cybercriminalité et du processus d'apprentissage social ont été en mesure d'informer les sciences forensiques et d'en influencer les pratiques. En effet, ce sont les connaissances sur la cybercriminalité et les modes opératoires des hackers qui permettent aux chercheurs, aujourd'hui, de savoir où et comment aller chercher les traces numériques nécessaires à leurs analyses. Par exemple, dans le cadre du présent travail, les connaissances criminologiques concernant la cyberdélinquance ont permis de savoir que les pirates informatiques utilisaient de plus en plus les forums de discussion afin de partager de l'information, des logiciels et des outils de piratage. Sans ces connaissances criminologiques, le processus d'apprentissage

délinquant serait demeuré inconnu pour les chercheurs et il aurait été beaucoup moins aisé de savoir quelles analyses effectuer et sur quels éléments porter une attention particulière.

Enfin, il est également possible d'utiliser la trace comme vecteur de connaissances au niveau de la prévention du phénomène criminologique. Ainsi, si les traces permettent d'obtenir de nouvelles connaissances sur le phénomène criminologique qu'est la cyberdélinquance et ces nouvelles connaissances permettront, à leur tour, un perfectionnement des techniques de prévention. Par exemple, s'il est possible d'observer un partage de connaissances entre les hackers et d'établir un modèle présentant les relations de pouvoir entre les différents acteurs, alors les connaissances criminologiques obtenues permettront aux autorités de modifier leurs approches face à ce phénomène. De cette manière, l'intégration entre la criminologie et les sciences forensiques au sein du présent projet pourrait permettre une prévention différente et plus adéquate de la cybercriminalité.

RÉFÉRENCES

Abbasi, A., Li, W., Benjamin, V. A., Hu, S. et Chen, H. (2014). *Descriptive Analytics: Examining Expert Hackers in Web Forums.* Communication présentée JISIC.

Adams, M. S. (1996). Labeling and differential association: Towards a general social learning theory of crime and deviance. *American Journal of Criminal Justice, 20*(2), 147-164.

Akers, R. L. (1977). *Deviant Behavior: A Social Learning Approach*. (2e éd.). Belmont, Calif.: Wadsworth.

Akers, R. L. (1985). *Deviant behavior: A social learning approach*. Wadsworth Publishing Company.

Akers, R. L. (1996). Is differential association/social learning cultural deviance theory? *Criminology, 34*(2), 229-247.

Akers, R. L. et Cochran, J. K. (1985). Adolescent marijuana use: A test of three theories of deviant behavior. *Deviant Behavior, 6*(4), 323-346.

Akers, R. L. et Jensen, G. F. (2006). The empirical status of social learning theory of crime and deviance: The past, present, and future. *Taking stock: The status of criminological theory, 15*, 37-76.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L. et Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. *American sociological review*, 636-655.

Andrews, L., Holloway, M. et Massoglia, D. (2015). DIGITAL PEEPHOLES.

Bachmann, M. et Corzine, J. (2010). Insights into the hacking underground. *The Future Challenges of Cybercrime, 5*, 31-41.

Bandura, A. (1969). Social-learning theory of identificatory processes. *Handbook of socialization theory and research, 213*, 262.

Bandura, A. (1977). Social learning theory Englewood Cliffs.

Barber, R. (2001). Hackers profiled—who are they and what are their motivations? *Computer Fraud & Security, 2001*(2), 14-17.

Borgatti, S. P. et Everett, M. G. (2000). Models of core/periphery structures. *Social networks, 21*(4), 375-395.

Borgatti, S. P., Everett, M. G. et Freeman, L. C. (2002). UCINET 6 for Windows: Software for Social Network Analysis. *Harvard, MA: Analytic Technologies*.

Brauer, J. R. et Tittle, C. R. (2012). Social learning theory and human reinforcement. *Sociological Spectrum, 32*(2), 157-177.

Brownfield, D. et Thompson, K. (1991). Attachment to peers and delinquent behaviour. *Canadian J. Criminology, 33*, 45.

Bruinsma, G. J. (1992). Differential association theory reconsidered: An extension and its empirical test. *Journal of Quantitative Criminology, 8*(1), 29-49.

Bukac, V., Stavova, V., Nemec, L., Riha, Z. et Matyas, V. (2015). *Service in denial–clouds going with the winds.* Communication présentée International Conference on Network and System Security.

Burgess, R. L. et Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social problems, 14*(2), 128-147.

Caldwell, T. (2011). Ethical hackers: putting on the white hat. *Network Security, 2011*(7), 10-13.

Casalegno, C. (2005). *Social Engineering : l'art de l'influence et de la manipulation* [Slides]. Repéré à https://www.christophe-casalegno.com/docs/social_engineering.pdf

Catalano, R. F., Kosterman, R., Hawkins, J. D., Newcomb, M. D. et Abbott, R. D. (1996). Modeling the etiology of adolescent substance use: A test of the social development model. *Journal of drug issues, 26*(2), 429-455.

Chantler, N. (1996). Profile of a computer hacker. *Florida: infowar*.

Cheung, A. (2012). *Social Engineering*. Repéré à http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Social%20Engineering%20A%20Cheung.pdf

Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime, 11*(3), 270-295.

Clais, J.-B. (2016). Observation des communautés et forums sur Internet. *Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique, 131*(1), 78-91.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books.

Costa, L. d. F., Rodrigues, F. A., Travieso, G. et Villas Boas, P. R. (2007). Characterization of complex networks: A survey of measurements. *Advances in physics, 56*(1), 167-242.

Craig, P. (2005). Software piracy exposed.

Crandall, J. R., Su, Z., Wu, S. F. et Chong, F. T. (2005). *On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits.* Communication présentée Proceedings of the 12th ACM conference on Computer and communications security.

Cressey, D. R. (1952). Application and verification of the differential association theory. *The Journal of Criminal Law, Criminology, and Police Science, 43*(1), 43-52.

Cressey, D. R. (1960). The theory of differential association: An introduction. *Soc. Probs., 8*, 2.

De Fleur, M. L. et Quinney, R. (1966). A reformulation of Sutherland's differential association theory and a strategy for empirical verification. *Journal of Research in Crime and Delinquency, 3*(1), 1-22.

De Vivo, M., de Vivo, G. O. et Isern, G. (1998). Internet security attacks at the basic levels. *ACM SIGOPS operating systems review, 32*(2), 4-15.

Décary-Hétu, D. (2013). Le capital virtuel: entre compétition, survie et réputation.

Décary-Hétu, D., Morselli, C. et Leman-Langlois, S. (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.

Dupont, B., Côté, A.-M., Savine, C. et Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*(2), 129-151.

eduCBA. (2016). Hackers vs Crackers: Easy to Understand Exclusive Difference. Repéré à https://www.educba.com/hackers-vs-crackers/

Éloire, F. (2014). Qui se ressemble s' assemble? *Actes de la recherche en sciences sociales*(5), 104-119.

Fan, W., Lwakatare, K. et Rong, R. (2017). Social engineering: Ie based model of human weakness for attack and defense investigations. *International Journal of Computer Network and Information Security, 9*(1), 1.

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social networks, 1*(3), 215-239.

Glueck, S. (1956). Theory and fact in criminology. *Brit. J. Delinq., 7*, 92.

Gouvernement du Canada (2014). *Loi sur la protection des Canadiens contre la cybercriminalité* Repéré à http://laws-lois.justice.gc.ca/fra/LoisAnnuelles/2014_31/page-1.html

Gouvernement du Canada (2017). *Cybercriminalité : Aperçu*. Repéré à http://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=fra&_ga=2.5477239.537538146.1503859344-1577748681.1503859344

Grossetti, M. (2013). Comprendre les réseaux personnels. *Mondes sociaux*. Repéré à https://sms.hypotheses.org/125

Halfond, W. G. et Orso, A. (2005). *AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks.* Communication présentée Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering.

Halfond, W. G., Viegas, J. et Orso, A. (2006). *A classification of SQL-injection attacks and countermeasures.* Communication présentée Proceedings of the IEEE International Symposium on Secure Software Engineering.

Hawdon, J. (2012). Applying differential association theory to online hate groups: a theoretical statement.

Higgins, G. E., Fell, B. D. et Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies, 19*(1), 3-22.

Higgins, G. E. et Makin, D. A. (2004). Does social learning theory condition the effects of low self-control on college students' software piracy. *Journal of Economic Crime Management, 2*(2), 1-22.

Higgins, G. E. et Wilson, A. L. (2006). Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software. *Security Journal, 19*(2), 75-92.

Higgins, G. E., Wilson, A. L. et Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture, 12*(3), 166-184.

Higgins, G. E., Wolfe, S. E. et Marcum, C. D. (2008). Digital piracy: An examination of three measurements of self-control. *Deviant Behavior, 29*(5), 440-460.

Hinduja, S. et Ingram, J. R. (2009). Social learning theory and music piracy: the differential role of online and offline peer influences. *Criminal Justice Studies, 22*(4), 405-420.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal, 4*(1), 2-12.

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., Strumsky, D., Smirnova, O. et Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891.

Jeffray, C. et Feakin, T. (2015). Underground web : The cybercrime challenge *Special Report*: Australian Strategic Policy Institute.

Jordan, T. et Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Kleinknecht, S. W. (2003). *Hacking hackers: Ethnographic insights into the hacker subculture-definition, ideology and argot.* (McMaster University).

Larousse (Firm). (2004). *Le Petit Larousse Ilustre 2005*. Larousse Editions.

Laub, J. H. et Sampson, R. J. (1991). The Sutherland-Glueck debate: On the sociology of criminological knowledge. *American Journal of Sociology, 96*(6), 1402-1440.

Leeson, P. T. et Coyne, C. J. (2005). The economics of computer hacking. *JL Econ. & Pol'y, 1*, 511.

Lu, D. (2015). When Ethical Hacking Can't Compete. *The Atlantic*. Repéré à https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/

Lu, Y., Luo, X., Polgar, M. et Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*(2), 31-41.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*(2), 71-94.

Macdonald, M. et Frank, R. (2017). The network structure of malware development, deployment and distribution. *Global Crime, 18*(1), 49-69.

Merton, R. K. (1997). On the evolving synthesis of differential association and anomie theory: A perspective from the sociology of science. *Criminology, 35*(3), 517-525.

Mirkovic, J. et Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53.

Mitnick, K. D. et Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Morris, R. G. et Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review, 34*(2), 173-195.

Morris, R. G. et Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice, 38*(4), 470-480.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Systems Security, 15*(5), 13-21.

Pratt, T. C., Cullen, F. T., Sellers, C. S., Thomas Winfree Jr, L., Madensen, T. D., Daigle, L. E., . . . Gau, J. M. (2010). The empirical status of social learning theory: A meta-analysis. *Justice Quarterly, 27*(6), 765-802.

Raymond, E. S. (2003). How to become a hacker. *Database and Network Journal, 33*(2), 8-9.

Raza, M., Iqbal, M., Sharif, M. et Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal, 19*(4), 439-444.

Sachdeva, M., Singh, G., Kumar, K. et Singh, K. (2010). DDoS Incidents and their Impact: A Review. *Int. Arab J. Inf. Technol., 7*(1), 14-20.

Samani, R. et McFarland, C. (2015). Hacking the Human Operating System: McAfee Labs.

Sehn, C. (2002). Hackers and Crackers: Who can we trust?

Shapiro, F. R. (2003). Antedating of "Hacker". *American Dialect Society Mailing List*.

Short Jr, J. F. (1956). Differential association and delinquency. *Soc. Probs., 4*, 233.

Skinner, W. F. et Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*(4), 495-518.

Su, Z. et Wassermann, G. (2006). *The essence of command injection attacks in web applications.* Communication présentée ACM SIGPLAN Notices.

Sûreté du Québec (s. d.). Prévention : Piratage informatique. Repéré à https://www.sq.gouv.qc.ca/services/prevention/

Sutherland, E. H. 1947. Principles of Criminology.

Sutherland, E. H., Cressey, D. R. et Luckenbill, D. F. (1992). *Principles of criminology*. Rowman & Littlefield.

The PHP Group (2017). Injection SQL. Repéré le 10 juin 2017à http://php.net/manual/fr/security.database.sql-injection.php

The Social Engineering Framework. (2017). Repéré le 10 mai 2017à https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Vidal, S. (2016). Shake and Bake: Analyse des recettes de méthamphétamine retrouvées sur Internet.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity.

Warr, M. (2002). *Companions in crime: The social aspects of criminal conduct*. Cambridge University Press.

Watts, D. J. et Strogatz, S. H. (1998). Collective dynamics of'small-world'networks. *nature, 393*(6684), 440.

Wyble, J. (2008). Methamphetamine-The New Eipidemic. Mich. St. *UJ Med. & L.*, 11, 115.

Zhang, X., Tsang, A., Yue, W. T. et Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers, 17*(6), 1239-1251.