Université de Montréal

De « skid » à *hacker* compétent:
L'apprentissage social chez les pirates informatiques

par
Jessie Wala Ahmad

École de Criminologie, Faculté des arts et 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 2021

© Jessie Wala Ahmad, 2021

Université de Montréal

Unité académique : École de criminologie, Faculté des arts et sciences

---

Ce mémoire intitulé

De « skid » à *hacker* compétent :

L'apprentissage social chez les pirates informatiques

Présenté par

Jessie Wala Ahmad

A été évalué par un jury composé des personnes suivantes

Benoît Dupont
Président-rapporteur

David Décary-Hétu
Directeur de recherche

Masarah Paquet-Clouston
Membre du jury

Résumé

La criminalité informatique n'est plus un nouveau phénomène. Toutefois, plusieurs auteurs s'entendent pour dire que le concept de pirate informatique est en constante transformation, ce qui contribue sans doute à la crainte et la fascination que ces derniers continuent de susciter, tant dans la culture populaire, mais aussi chez les chercheurs. En effet, à travers les années, de nombreux chercheurs ont tenté de les comprendre et les étudier, et la validité de la théorie de l'apprentissage sociale a été démontrée à de maintes reprises en lien avec la cyberdéviance. Par contre, aucune de ces études ne s'est basée sur des contacts directs avec pirates informatiques actifs. En fait, aucune ne s'est appuyée sur des entretiens avec des pirates informatiques. Il existe donc une lacune importante dans la littérature scientifique sur ce sujet.

Par conséquent, l'objectif de cette étude sera de comprendre comment les pirates informatiques apprennent les compétences essentielles à leurs activités au contact des autres, l'influence de leur entourage dans le monde réel et le monde virtuel, ainsi que le rôle de l'imitation dans ces apprentissages. Pour ce faire, des entretiens semi-dirigés ont été menés avec 17 pirates informatiques encore actifs, recrutés sur des forums de discussion dédiés aux activités de piratage informatique. L'analyse de ces entretiens a permis de dégager de grandes tendances en ce qui a trait au rôle joué par les pairs au sein de communautés de pirates informatiques, au niveau du partage de connaissances, à la façon dont ces connaissances sont transmises, l'importance de se retrouver en communauté, ainsi que le rôle des mentors dans leur processus d'apprentissage. La théorie de l'apprentissage social d'Akers a servi de cadre théorique pour la réalisation de cette étude.

Mots-clés : apprentissage social, pirate informatique, imitation, influence des pairs, mentor, forum de discussion, entrevue.

Abstract

Computer crime is no longer a new phenomenon. However, several authors agree to say that the concept of hacker is in constant transformation, which undoubtedly contributes to the fear and the fascination that they continue to exert, both in popular culture, but also among researchers. Indeed, over the years many researchers have attempted to understand and study them, and the validity of social learning theory has been demonstrated time and time again in connection with cyberdeviance. However, none of these studies were not based on direct contact with active hackers. As a matter of fact, none were based on interviews with hackers. Therefore, there is an important gap in the scientific literature on this subject.

Hence, the objective of this study will be to understand how hackers learn the skills essential to their activities in contact with others, the influence of those around them in the real and virtual world, as well as the role of imitation in these learnings. To do this, semi-structured interviews were conducted with 17 active hackers, recruited on discussion forums dedicated to hacking activities. The analysis of these interviews made it possible to identify major trends in terms of the role played by peers within hacker communities, in terms of knowledge sharing, the way in which this knowledge is transmitted, the importance of the community, as well as the role of mentors in their learning process. Akers's social learning theory served as the theoretical framework for this study.

Keywords : social learning, hackers, imitation, influence of peers, mentor, forums, interview.

Table des matières

Liste des tableaux

Liste des figures

“Never underestimate the determination of a kid who is time-rich and cash-poor.”

— Cory Doctorow

Remerciements / Acknowledgment

Maman, tu n'as jamais eu froid aux yeux et tu as été un modèle pour moi, dans ma quête de toujours vouloir me dépasser. Merci pour ton soutien indéfectible.

À mon directeur de recherche, **David**, j'aimerais te dire merci d'avoir composé avec mon processus un peu anarchique, de m'avoir encouragé dans mes moments de désespoir et de m'avoir guidé dans ce projet un peu ambitieux.

Jean-Philippe D.-M., merci pour ta compassion et ta compréhension. Je ne pouvais pas rêver d'un meilleur patron et ami dans les circonstances.

I would also like to give many thanks to **all the forums mods** (*you know who you are, alright*), and **all the friends** I made along the way. Thank you for trusting me, I know you *know* this project wouldn't have been possible without you.

Nathan, you were the first friend I made when I started this project, and you were always willing to help me until the end. Thanks for vouching for me and for your friendship.

Cassius V., thank you for your trust and for making me part of a community. You always kept me up to date with things, criticized my food, and provided me with awesome music.

Mitrovic M., you listened to me complain, accepted me with my lame memes, and made me laugh with your shenanigans. Thank you for helping me when I needed it.

Dan, thank you for being my go-to person to test my ideas, and for helping me understand all sorts of concepts I wasn't familiar with. Your inputs were always very helpful and appreciated. And yes, only *one* cup of coffee at 1 a.m. :P

Finalement et non le moindre, merci **Alexandre B.**, tu as été d'une aide et d'un soutien inestimable. Je t'en serais toujours reconnaissante de m'avoir endurée pendant cette période mouvementée.

Introduction

La validité de la théorie de l'apprentissage sociale a été démontrée à de maintes reprises en lien avec la cyberdéviance (Décary-Hétu, 2013a; Higgins et al., 2007; Higgins & Makin, 2004; Higgins & Wilson, 2006; Hinduja & Ingram, 2009; Holt et al., 2010, 2012; Holt & Copes, 2010; Marcum et al., 2014; Montégiani, 2017; Morris & Higgins, 2010; M. K. Rogers, 2001; Skinner & Fream, 1997). La théorie postule que la délinquance s'apprend au contact de pairs délinquants intériorisant des définitions favorables au crime, à l'exposition à des modèles déviants à imiter et au renforcement différentiel positif (Akers, 2009). Plusieurs études ont conclu que cette théorie jouait un rôle significatif dans la criminalité informatique, et que davantage d'études devraient être conduites à ce sujet (Boman & Freng, 2017; Hutchings & Holt, 2018; Marion & Twede, 2020; Navarro & Marcum, 2019a; Steinmetz & Nobles, 2018).

Ces recherches ne sont cependant pas basées sur des contacts directs avec pirates informatiques actifs. De plus, les rares études qui ont été recensées ont basé leurs analyses sur des données récoltées, soit sur un forum de discussion, soit sur des transcriptions de clavardage public, ou bien via un questionnaire auto-rapporté distribué à des étudiants (Décary-Hétu, 2013a; Marcum et al., 2014; Montégiani, 2017; M. K. Rogers, 2001). Aucune ne s'est basée sur des entretiens avec des pirates informatiques. Il existe donc une lacune importante dans la littérature scientifique sur ce sujet.

Par conséquent, ce travail dirigé cherche à comprendre et décrire les processus d'apprentissage social chez les pirates informatiques, en se basant sur dix-sept entretiens semi-dirigés réalisés avec des pirates informatiques. Les sous-objectifs de ce travail sont de décrire le rôle des pairs, ainsi que l'importance de l'imitation dans le processus d'apprentissage des pirates informatiques. Les trois premières parties de l'étude ont été consacrées à la définition des concepts inhérents à l'étude du phénomène, ainsi qu'à la recension des connaissances actuellement détenues sur le sujet. Ensuite, c'est tout naturellement qu'une problématique s'est manifestée et a été exposée dans le chapitre 4. La méthodologie concernant la collecte, l'analyse et les limites des données ont été détaillées dans le chapitre 5. Finalement, les résultats et la discussion entourant ces résultats ont été explicités dans les chapitres subséquents, ainsi que des pistes pour de futures études.

Chapitre 1 – Le pirate informatique

1.1 Définition de *hacker*

La définition de ce que représente un *hacker* a tellement changée et évoluée, en phase avec l'évolution des technologies et des perceptions que nous en avons, qu'il n'a toujours pas été possible d'en arriver à un consensus à cet effet, au sein de la communauté scientifique (Décary-Hétu, 2013b; Franklin et al., 2019; Holt & Schell, 2013; Lavoie et al., 2013; Oliver & Randolph, 2020; Steinmetz, 2015; Viano, 2017). Malgré l'évolution du terme « hacker » et des activités qui y sont liées, la grande majorité des chercheurs se concentreraient sur le pirate informatique dans le contexte d'une intention criminelle ou malveillante (Jordan & Taylor, 1998; Oliver & Randolph, 2020; Seebruck, 2015). Thomas avait déjà noté en 2002 à quel point le terme *hacker* était employé de manière péjorative en raison des stéréotypes, qui seraient davantage liés à l'anxiété du public face à l'ère de l'information, plutôt qu'ancrés dans la réalité (Thomas, 2002).

Au sens large, le terme *hacker*, ou pirate informatique, comprends autant la notion d'individu criminalisé que celle d'individu non criminalisé, et ce, même s'il ne s'agit pas de la façon dont le terme est souvent véhiculé, autant par les médias que par les chercheurs (Franklin et al., 2019; Holt & Schell, 2013; Kizza, 2013; Oliver & Randolph, 2020; Viano, 2017). Le fait d'avoir utilisé les termes *hackers* et cybercriminels de manière interchangeable a probablement contribué à exacerber cette confusion (Seebruck, 2015). En effet, des crimes informatiques de type « point-and-click », comme la cyberintimidation ou la pédopornographie, sont considérés comme des délits assistés par l'informatique, et ne requièrent pas nécessairement de compétences techniques avancées pour être réalisées (Gendarmerie Royale du Canada, 2016; Viano, 2017). Par contre, leurs auteurs seraient tout de même considérés comme étant des « cybercriminels » aux yeux de la loi, en raison de la présence d'un élément « virtuel » (Gendarmerie Royale du Canada, 2016; Lavoie et al., 2013; Viano, 2017). Par conséquent, la nuance importante à apporter est que les *hackers* ne sont pas tous des cybercriminels, mais également que pas tous les cybercriminels ne sont des *hackers* (Kizza, 2013; Oliver & Randolph, 2020; Steinmetz, 2015).

Au Canada, la Gendarmerie Royale du Canada (GRC) fait également une distinction entre le crime technologique au sens large, qui implique tous les types de dispositifs pouvant traiter des données numériques (guichet automatique bancaire, système d'alarme, etc.), et le crime informatique, qui lui sera, de manière plus spécifique, commis majoritairement à l'aide d'Internet et des technologies de l'information (ordinateurs, téléphone mobile, tablette, etc.) (Gendarmerie Royale du Canada, 2016; Leman-Langlois, 2008). Contrairement au délit assisté par l'informatique, mentionné précédemment, le délit informatique « pur » nécessite des compétences techniques plus poussées et va cibler une technologie de l'information (Gendarmerie Royale du Canada, 2016). C'est dans cette catégorie que se retrouve le piratage informatique.

Ainsi, alors que le terme anglophone "hacker" puisse généralement s'appliquer à un large éventail de personnes ayant des connaissances en informatique, qui souhaitent accéder à une cible identifiée (une entreprise, un groupe ou un réseau), mais qui diffèrent grandement dans leurs motivations, leurs compétences et l'usage qu'elles font de leurs connaissances informatiques (Bachmann, 2010; Madarie, 2017; Oliver & Randolph, 2020), il serait judicieux de traduire « pirate informatique » par « hacker malveillant » (*black hat hacker*), puisqu'en français, le terme « pirate » implique intrinsèquement la notion péjorative de détournement, en revêtant un caractère illicite. Le *hacker* malveillant est donc un individu qui utilise ses diverses connaissances et compétences informatiques pour cibler et accéder au système informatique ou au réseau d'une autre personne, ou organisation, sans permission ni autorisation, à des fins variées, dans une intention malicieuse (Brenner, 2001; Kizza, 2013; Marion & Twede, 2020).

1.2 Typologies

De nombreux auteurs ont tenté diverses méthodes de classification des *hackers*, en fonction de leurs compétences, de leurs motivations et de leurs capacités. Décary-Hétu (2013b) a relevé que la littérature différenciait les pirates informatiques selon deux axes principaux : leurs motivations, ainsi que leurs connaissances techniques.

Les typologies motivationnelles vont tenter de classifier les *hackers* en fonction de ce qui les pousse à passer à l'action (Décary-Hétu, 2013b; Madarie, 2017). D'autres facteurs peuvent s'avérer être gratifiants sans pour autant être un facteur de motivation (Goode & Cruise,

2005). De plus, les résultats de l'étude de Madarie (2017) suggèrent que la relation entre les motivations et les activités de piratage n'est pas aussi directe qu'on pourrait le croire, et que les évaluations des motivations relevées dans diverses études refléteraient davantage les motivations culturellement reconnues, que les véritables motivations personnelles. Il a cependant été possible de regrouper les diverses motivations recensées dans la littérature à l'intérieur de six grandes catégories : 1) Le défi technique, 2) la recherche de prestige, 3) le profit/gain financier, 4) les motivations idéologiques, 5) la curiosité/loisir et 6) la vengeance.

Le défi technique : Plusieurs études citent le défi technique comme étant l'élément le plus gratifiant du piratage, selon les pirates informatiques, supplantant les autres facteurs motivationnels (Goode & Cruise, 2005), et ce, que ce soit pour tester et pratiquer ses techniques, ou simplement pour la stimulation que leur rapporte le défi cognitif (Edwards, 2020; Goode & Cruise, 2005; Marion & Twede, 2020).

La recherche de prestige : La reconnaissance, recherche de notoriété ou de prestige est également un facteur de motivation souvent relevé dans la littérature (Baillargeon-Audet, 2010; Jordan & Taylor, 1998; Kizza, 2013; Marion & Twede, 2020; McBrayer, 2014; Seebruck, 2015). Pour les auteurs étudiés, elle représente la reconnaissance par les pairs et une forme d'acceptation dans leur communauté, et pouvant possiblement leur amener un avancement dans la hiérarchie, parmi ceux qui sont admirés et respectés pour leurs exploits (Baillargeon-Audet, 2010; Jordan & Taylor, 1998; Kizza, 2013; Marion & Twede, 2020).

Le profit / gain financier : Un autre facteur de motivation important est le profit (McBrayer, 2014). Pour certains auteurs, cela représente des sommes d'argent obtenues via le vol d'informations bancaires ou de cartes de crédit (Marion & Twede, 2020; Seebruck, 2015). Pour d'autres, cela peut également prendre la forme de la vente de service de piratage offert en ligne, une attaque menée envers un compétiteur, que ce soit une attaque technique l'empêchant de mener des affaires ou pour porter atteinte à sa réputation, jusqu'à l'espionnage industriel pour obtenir un avantage concurrentiel (Edwards, 2020; Kizza, 2013). Cette motivation n'a pas été repérée dans des études plus antérieures, comme celle de Jordan et Taylor (1998) laissant présager que la recherche de profit pourrait être un facteur motivationnel plus récent chez les pirates informatiques (Décary-Hétu, 2013b; Junger, 2019).

Les motivations idéologiques : Les motivations idéologiques regroupent plusieurs types de motivations (McBrayer, 2014). Le premier type couvre les pirates informatiques, comme les groupes Anonymous ou LulzSec, qui s'impliquent dans le militantisme politique. Ces *hackers* sont appelés *hacktivistes* et leurs actions sont appelées *hacktivisme*. Ces mots sont une combinaison du mot « hacker » et d'« activisme » (Décary-Hétu, 2013b; Marion & Twede, 2020). Ces derniers peuvent chercher à attirer l'attention médiatique dans le but de mobiliser ou sensibiliser la population vis-à-vis certains enjeux politiques ou sociaux, en commettant des actes de piratage, comme le défaçage d'un site Web, ou même en fuitant de l'information embarrassante concernant leurs cibles (Marion & Twede, 2020; Seebruck, 2015). Poussées à l'extrême, ces activités peuvent s'apparenter à du terrorisme lorsqu'elles ciblent les infrastructures essentielles d'une entité, pouvant provoquer une grave perturbation du fonctionnement de leurs systèmes et même conduire à une catastrophe nationale (Edwards, 2020; Kizza, 2013).

La curiosité / loisir : Les études démontrent que certains pirates informatiques justifient leurs activités en citant la curiosité de ce que l'on peut trouver sur le réseau mondial, le plaisir et le divertissement (Décary-Hétu, 2013b; Kizza, 2013; McBrayer, 2014; Madarie, 2017; Seebruck, 2015). En effet, plusieurs *hackers* considéreraient que leur vie hors ligne est ennuyeuse comparée au frisson que leur procurent leurs explorations en ligne (Jordan & Taylor, 1998).

La vengeance : La vengeance peut représenter un puissant moteur (McBrayer, 2014). Qu'il s'agisse d'un employé mécontent, d'un ex-conjoint, ou d'autres circonstances personnelles, ces situations peuvent conduire un pirate informatique à se servir de ses compétences pour réparer une injustice, qu'elle soit perçue ou réelle (Edwards, 2020; Kizza, 2013; Marion & Twede, 2020; Seebruck, 2015). Par ailleurs, il est important de noter que certains pirates sont simplement motivés par le désir de nuire à autrui. Ils peuvent donc chercher à divulguer des données personnelles ou embarrassantes (*doxxing*), simplement par plaisir malsain, sans nécessairement y avoir été provoqués au préalable (Marion & Twede, 2020).

En ce qui concerne les typologies basées sur les compétences techniques, les auteurs contemporains ont créé des typologies hybrides, qui prennent en compte les motivations des pirates informatiques (S. L. N. Hald & Pedersen, 2012; McBrayer, 2014; M. K. Rogers, 2006; Seebruck, 2015). La taxonomie qui a pu être recensée contient ainsi huit catégories, allant de ceux possédant peu de compétences techniques, à ceux ayant une maîtrise très avancée.

Tableau 1. – Typologie des *hackers* selon leur niveau de compétence et leurs motivations

Taxonomie	Définition	Niveau technique	Motivation(s)
Le pirate novice (*script kiddie*)	Pirate débutant qui s'appuie sur des outils préexistants (*tool kits*) pour mener ses attaques.	Très peu avancé	La reconnaissance
Le programmeur rebelle (*cyber punk*)	Pirate plutôt généraliste en matière de logiciels (*software*), de matériel (*hardware*), ainsi qu'en programmation, pouvant élaborer des logiciels malicieux.	Niveau modéré	• La reconnaissance • Le profit financier • La vengeance
Le simple délinquant adaptatif (*petty thief*)	Le délinquant traditionnel qui migre vers le monde virtuel par opportunité criminelle. Va généralement maîtriser les compétences spécifiques à son activité criminelle et n'a pas d'intérêt envers la technologie.	Niveau modéré	Le profit financier
La menace interne (*insider*)	Le pirate employé ayant des accès privilégiés et une bonne connaissance de l'infrastructure informatique de son employeur.	Niveau élevé	• La vengeance • Le profit financier
L'activiste politique (*hacktivist*)	Les hacktivistes politiques vont généralement opérer en groupe, avec un niveau de compétences variables d'un individu à l'autre, tout en ayant un noyau de membres aux compétences élevées.	Niveau élevé	Motivations idéologiques (politique)
Le pirate de vieille garde (*old guard hacker*)	*Hacker* de la vieille école, passionné d'informatique et recherchant la stimulation intellectuelle. N'a à priori pas d'intention criminelle, mais va préconiser l'exploration sans limite ou restriction.	Niveau élevé	• Le défi technique • La curiosité / loisir
Le pirate criminel professionnel (*professional criminal*)	Le pirate professionnel, spécialisé en crimes informatiques et qui en fera un métier. Ses services seront retenus par des entreprises, par des organisations criminelles, ou même par des acteurs Étatiques.	Niveau très élevé	Le profit financier

Le pirate au service d'un acteur Étatique (*Nation-State hacker*)	Le pirate œuvrant au sein d'une organisation gouvernementale ou d'une unité de renseignement, ayant accès à un nombre de ressources très étendues pour mener à bien des opérations ayant pour but d'influencer, déstabiliser ou d'espionner.	Niveau très élevé	Motivations idéologiques (politique)

Ce tableau se veut un récapitulatif de différentes études qui se sont penchées sur la création d'une typologie de *hackers* basée sur les compétences techniques et en lien avec leurs motivations (S. L. N. Hald & Pedersen, 2012; Kizza, 2013; McBrayer, 2014; M. Rogers, 1999; M. K. Rogers, 2006; Seebruck, 2015), mais il est important de garder en tête que ces catégories ne sont pas mutuellement exclusives. En effet, tout regroupement d'individus en catégories entraîne une certaine perte d'information, ce qui peut être problématique lorsqu'il s'agit de catégoriser des cyberdéviants qui s'engagent dans plusieurs types de crimes différents, et donc qui n'appartiennent pas à une seule catégorie (McBrayer, 2014; Seebruck, 2015).

Chapitre 2 – L'apprentissage social

La théorie de l'association différentielle d'Edwin Sutherland (1947 dans sa forme finale) a pour position centrale que le crime, comme tout autre comportement, est appris et que le principal vecteur d'apprentissage provient de personnes avec qui l'individu va s'associer « différentiellement », c'est-à-dire des individus qu'un acteur fréquente, à divers titres, et qui vont l'aider à développer des définitions favorables ou défavorables à la commission d'un crime (Akers et al., 2017, 2021; Holt & Copes, 2010; Navarro & Marcum, 2019b; Steinmetz & Nobles, 2018; Sutherland & Cressey, 1966; Tremblay, 2010). Ces définitions vont agir comme des « orientations, justifications, définitions d'une situation, et d'autres attitudes morales et évaluatives, qui définiront la commission d'un acte comme étant bon ou mauvais, désirable ou indésirable, justifié ou injustifié » (Akers, 2017, p. 88), selon s'il est susceptible d'être récompensé ou, au contraire, inapproprié et à risque d'être puni (Akers, 2009; Akers et al., 2017, 2021). Le facteur clé qui intervient donc entre les associations déviantes et le crime est l'acquisition de techniques, d'attitudes, de raisonnements et de motivations qui favorisent la

violation de la loi (Akers et al., 2021; Holt & Copes, 2010; Steinmetz & Nobles, 2018; Sutherland & Cressey, 1966).

Bien que la théorie de l'association différentielle de Sutherland ait eu un impact important en criminologie au 20e siècle, elle a été largement critiquée, car elle n'expliquait pas les mécanismes de l'apprentissage décrit, et ne prenait pas en compte les traits de personnalité spécifiques à un individu rationnel (Akers, 2009; Akers et al., 2017, 2021; Graham & Smith, 2019; Navarro & Marcum, 2019b; Salisbury, 2012; Steinmetz & Nobles, 2018). En effet, les humains sont des êtres indépendants et motivés individuellement, et par conséquent, ils peuvent ne pas apprendre à devenir des criminels de la façon dont le prédirait nécessairement une association différentielle.

Dans un effort de résoudre cette lacune concernant les mécanismes d'apprentissage, Burgess et Akers (1966) ont entrepris une extension de la théorie de Sutherland, qui est connue comme étant la théorie de l'apprentissage sociale de Ronald Akers (Akers et al., 2017, 2021; Navarro & Marcum, 2019a; Salisbury, 2012; Steinmetz & Nobles, 2018). Cette théorie, initialement proposée en collaboration avec Robert L. Burgess (Burgess and Akers, 1966) en tant que reformulation behavioriste de la théorie de l'association différentielle de Sutherland, s'est nommée l'association-renforcement différentielle (*differential association-reinforcement*) (Akers et al., 2017, 2021).

En effet, il s'agit d'une version révisée qui intègre les principes sociologiques de la théorie de Sutherland, à des principes du comportementalisme, ou béhaviorisme social en psychologie, tel que le conditionnement opérant (Akers et al., 2017, 2021; Navarro & Marcum, 2019b; Steinmetz & Nobles, 2018; Tremblay, 2010). Les concepts empruntés à la psychologie béhavioriste qui sont au cœur de cette extension théorique sont le renforcement différentiel et l'imitation (Salisbury, 2012; Steinmetz & Nobles, 2018; Tremblay, 2010). Le renforcement différentiel consiste en la balance entre les récompenses ou punitions, présentes ou anticipées, pour un comportement donné, et qui fera en sorte qu'un individu va continuer (renforcement positif) ou cesser ce même comportement (renforcement négatif) (Akers et al., 2017, 2021). L'imitation fait référence à la modélisation du comportement d'un associé, ou d'autrui, et qui exercera une grande influence sur l'acquisition initiale du comportement, qu'il soit criminel ou conformiste, auprès de l'individu (Akers et al., 2017, 2021).

Cela signifie que l'association avec des pairs déviants fournira également à l'individu des modèles de déviance à imiter, mettant en évidence les processus d'observation, ou « vicariants », dans cet apprentissage puisqu'il sera possible d'observer comment les autres seront traités pour ce même comportement (Akers et al., 2017, 2021; Salisbury, 2012). L'ajout de ces concepts a permis de prendre en compte l'acquisition, la continuation et le désistement d'un comportement (Navarro & Marcum, 2019a). En d'autres termes, la théorie de l'apprentissage social est un cadre permettant de comprendre les motifs qui poussent les individus à commettre des infractions ou à résister au crime (Akers et al., 2021; Navarro & Marcum, 2019a; Salisbury, 2012; Tremblay, 2010).

Ainsi, la théorie telle qu'élaborée par Akers et Burgess (1966) repose sur quatre grands principes théoriques : (1) l'association différentielle ; (2) le renforcement différentiel ; (3) les définitions (favorables, ou non, à la criminalité) ; et (4) l'imitation, ou *modelling* (Akers, 2009; Akers et al., 2017, 2021). Ils ont également revu les neuf propositions initialement proposées par Sutherland, et les amenées à sept énoncés centraux autour desquels s'articule leur théorie de l'apprentissage social (Akers, 2009):

1. Le comportement criminel est appris selon les principes du conditionnement opérant.
2. Le comportement criminel est appris à la fois dans des situations « non sociales », qui sont renforçantes ou discriminantes, et par l'interaction sociale dans laquelle le comportement des autres personnes est renforçant ou discriminant, pour le comportement criminel.
3. L'essentiel de l'apprentissage du comportement criminel se fait dans les groupes qui constituent la principale source de renforcement de l'individu.
4. L'apprentissage du comportement criminel, y compris les techniques spécifiques, les attitudes et les procédures d'évitement, est fonction des renforcements efficaces et disponibles, et des contingences de renforcement existantes.
5. La catégorie spécifique de comportements qui sont appris et leur fréquence d'apparition sont une fonction des renforcements, qui sont efficaces et disponibles, et des règles ou normes par lesquelles ces renforcements sont appliqués.
6. Le comportement criminel est une fonction des normes qui sont discriminatoires pour le comportement criminel, dont l'apprentissage a lieu lorsque ce comportement est plus fortement renforcé, que le comportement non criminel.

7. La force du comportement criminel est une fonction directe de la quantité, de la fréquence et de la probabilité de son renforcement.

En résumé, la théorie de l'apprentissage social suggère qu'un individu acquière des connaissances et des modèles de comportement par l'expérience, ou l'observation (énoncé 3), et que cela lui permet non seulement d'améliorer ses compétences et ses techniques, mais aussi de renforcer son impulsion, sa motivation et sa rationalisation concernant un comportement donné (énoncé 2). C'est un tel environnement qui permet à l'apprentissage social d'avoir lieu.

La version d'Akers de la théorie de l'apprentissage social a constitué l'une des avancées les plus importantes en criminologie (Holt et al., 2012; Navarro & Marcum, 2019a; Salisbury, 2012; Tremblay, 2010) et en raison de l'abondance des travaux de recherche basés sur son approche, il est raisonnable de penser que le soutien empirique réel de l'apprentissage social en tant qu'explication générale de la criminalité est considérable (Salisbury, 2012).

Chapitre 3 – L'apprentissage social chez les pirates informatiques

La théorie de l'apprentissage social en tant que théorie générale criminologique est très polyvalente dans sa capacité à expliquer un large éventail de comportements criminels et déviants. Bien que dans la littérature, la théorie du faible contrôle de soi de Gottfredson et Hirschi (1990) ait souvent été étudiée en lien avec diverses formes de crimes informatiques (Higgins et al., 2007; Higgins & Makin, 2004; Higgins & Wilson, 2006; Hinduja & Ingram, 2009; Holt et al., 2012; Marcum et al., 2014), lorsqu'étudiée en lien avec le piratage informatique, plus spécifiquement, cette théorie a produit des résultats mitigés, qui ne soutenaient pas entièrement sa validité (Bossler & Burruss, 2010 ; Holt et al., 2012; Marcum et al., 2014; Steinmetz & Nobles, 2018). De plus, des études ont démontré que le fait de s'associer à des pairs déviants pouvait exacerber l'effet de la variable de la faible maîtrise de soi sur la cyberdéviance en général (Gibson & Wright, 2001; Holt et al., 2012; Marcum et al., 2014). Il a donc été raisonnable de penser que la théorie d'Akers pouvait offrir un cadre empirique solide pour étudier la nouvelle forme de criminalité que représente le crime informatique (Boman &

Freng, 2017; Hinduja & Ingram, 2009; Steinmetz & Nobles, 2018). Comme de fait, s'inspirant du précédent établi par Skinner et Fream (1997), les théories de l'association différentielle et de l'apprentissage social sont devenues les théories de référence les plus fréquemment testées, et les plus souvent soutenues, pour expliquer la cybercriminalité (Boman & Freng, 2017; Morris & Higgins, 2010; Steinmetz & Nobles, 2018).

La vaste majorité des études recensées qui ont testé la validité de la théorie de l'apprentissage social en lien avec la cyberdéviance, se sont intéressées au téléchargement et l'utilisation de contenu illégal (musique, films ou logiciels piratés) (Higgins et al., 2007; Higgins & Makin, 2004; Higgins & Wilson, 2006; Hinduja & Ingram, 2009; Holt et al., 2010, 2012; Holt & Copes, 2010; Morris & Higgins, 2010; Skinner & Fream, 1997). En ce qui concerne le piratage informatique plus spécifiquement, l'étude de Skinner et Fream (1997) a cherché à observer l'occurrence de divers types d'activités numériques illégales chez des étudiants universitaires : le téléchargement, l'utilisation ou la distribution illégale de logiciel (*software piracy)*, l'écriture ou l'utilisation d'un script malicieux (*virus*), la tentative de deviner un mot de passe (*password guessing*) et l'introduction dans un système de façon non autorisée. Holt et al. (2012) ont également distribué un questionnaire dans des écoles pour étudier l'utilisation, le téléchargement et la distribution illégale de matériel protégé de droits d'auteurs (musique, films, logiciels, etc.), l'accès à un système de façon non autorisée, la participation à du harcèlement en ligne, et la consommation de pornographie en ligne... Puis, l'étude de Marcum, et al. (2014) s'est penché sur les activités de piratage informatique de jeunes mineurs (moins de 18 ans), tels que se connecter à l'adresse électronique ou le compte Facebook d'une autre personne sans son autorisation puis envoyer un message, ou accéder à un site web en n'étant pas autorisé, également en distribuant un questionnaire auto-rapporté.

Ces études sont toutes arrivées à la conclusion qu'il existait bel et bien un lien, à différents degrés de solidité, entre différentes composantes de l'apprentissage social et le comportement cyberdéviant observé (Higgins et al., 2007; Higgins & Makin, 2004; Higgins & Wilson, 2006; Hinduja & Ingram, 2009; Holt et al., 2010, 2012; Holt & Copes, 2010; Marcum et al., 2014; Morris & Higgins, 2010; Skinner & Fream, 1997).

3.1 L’association différentielle

Bien que les recherches sur l'évaluation du modèle complet de la théorie de l'apprentissage social (c'est-à-dire incluant l'association différentielle, le renforcement différentiel, les définitions favorables et l'imitation) soient limitées (Navarro & Marcum, 2019a), de nombreuses études ont confirmé l'importance cruciale de l'association différentielle en tant que facteur de risque pour la perpétration de divers cybercrimes, notamment le piratage (Décary-Hétu, 2013a; Higgins & Wilson, 2006; Holt et al., 2010; Holt & Bossler, 2014; Marcum et al., 2014).

Dans leur étude sur les comportements de piratage des jeunes, Marcum et al. (2014) ont trouvé un soutien significatif à la relation entre l'association de pairs déviants et la perpétration d’actes de piratage informatique. Plus précisément, les jeunes qui s'associaient à des pairs déviants étaient plus susceptibles de pirater le compte de messagerie ou le compte Facebook d'une autre personne, et aussi plus susceptibles de pirater des sites Web (Marcum et al., 2014).

Selon le troisième postulat proposé par Akers et Burgess, l'essentiel de l'apprentissage du comportement criminel se fait dans les groupes (Akers, 2009). L’association différentielle a été pensée pour permettre à presque n’importe quel individu côtoyé par un acteur de devenir un potentiel associé relativement important, qu’il s’agisse d’ami proche, d’une connaissance provenant d’un groupe de référence plus éloigné, ou même de personnalités présentées dans les médias de masse (Akers, 2009). Par contre, depuis le développement de la théorie, les associés différentiels ont été typiquement opérationnalisés comme étant les pairs ou les amis (Akers, 2009; Akers et al., 2017, 2021; Steinmetz & Nobles, 2018; Tremblay, 2010). À l’époque où Akers avait élaboré sa théorie, la réalité des interactions virtuelles n’existait pas encore (Boman & Freng, 2017; Steinmetz & Nobles, 2018), mais même à travers un écran d’ordinateur, les pairs délinquants peuvent exercer une influence réelle et observable sur un acteur, sans jamais avoir eu d'interaction en face à face (Boman & Freng, 2017; Steinmetz & Nobles, 2018).

En effet, les pirates informatiques s'associent à d'autres criminels informatiques, soit physiquement par le biais de conférences et de conventions, soit virtuellement par le biais de canaux de clavardage, de groupes de nouvelles ou forums de discussions, pour communiquer avec des pairs ou acquérir des connaissances (Baillargeon-Audet, 2010; Boman & Freng,

2017; Hinduja & Ingram, 2009; Holt, 2007; M. K. Rogers, 2001; Sharma, 2007; Steinmetz & Nobles, 2018; Zhang et al., 2015). En fait, il s'est avéré que la participation à des plateformes de communication en ligne (salons de clavardage) pouvait même représenter un prédicteur significatif de piratage (Hinduja & Ingram, 2009).

Plusieurs auteurs ont relevé que le partage d'informations et de connaissances prenait une place importante dans les interactions entre *hackers,* et s'est avéré être une caractéristique représentative de leurs communautés (Baillargeon-Audet, 2010; Hinduja & Ingram, 2009; Holt et al., 2012; Navarro & Marcum, 2019a; Sharma, 2007; Skinner & Fream, 1997). Étant donné la nature de nombreuses infractions liées à la cybercriminalité, surtout dans ses formes plus sophistiquées comme le piratage informatique, qui nécessite des habiletés spécifiques et une compréhension technologique avancée, les individus qui souhaitent s'y engager doivent acquérir des compétences qui ne sont pas acquises dans le cadre d'expériences courantes et quotidiennes (Hinduja & Ingram, 2009; Navarro & Marcum, 2019a; Sharma, 2007)**.** De plus, le piratage informatique est surtout une question d'expertise puisque l'informatique est un domaine extrêmement large, dont il est impossible de maîtriser tous les aspects pour un seul individu, qui souvent aura son propre champ d'expertise (Sharma, 2007). C'est pourquoi ces activités peuvent nécessiter de demander l'aide de pairs délinquants possédant les connaissances ou de s'associer à d'autres *hackers* plus chevronnés (Navarro & Marcum, 2019a). Par conséquent, les pirates informatiques vont chercher à développer leurs connaissances en échangeant des informations et des outils (Baillargeon-Audet, 2010; Sharma, 2007). Toutefois, même dans les formes de cybercrimes moins sophistiquées, comme dans les cas de téléchargement illégal ou de cyberintimidation, par exemple, les cyberdéviants doivent tout de même apprendre des tactiques et des méthodes pour éviter la détection (Navarro & Marcum, 2019a).

Ainsi, d'une certaine façon, les pirates informatiques actifs sont perpétuellement en quête de connaissance et en apprentissage (Franklin et al., 2019). La théorie de l'apprentissage social possède donc une valeur intrinsèque importante pour comprendre la commission de diverses formes de cybercriminalité, puisque les délinquants doivent apprendre, non seulement à faire fonctionner du matériel informatique et électronique, mais aussi être familier avec certains langages de programmation et maîtriser des techniques spécifiques pour pouvoir utiliser l'ordinateur à des fins détournées (Holt et al., 2012; Skinner & Fream, 1997).

Le contexte virtuel des communautés vers lesquelles les *hackers* vont se tourner pour effectuer ces apprentissages implique que les individus composants les associations différentielles peuvent appartenir à des groupes très diversifiés, où différents types d'utilisateurs jouent différents rôles de partage des connaissances au sein d'une communauté, requérant des novices motivés et des vétérans réceptifs, des apprentis et des experts (Boman & Freng, 2017; Tremblay, 2010; Zhang et al., 2015). Les pirates informatiques plus âgés et plus expérimentés partagent avec les novices leurs connaissances, leurs techniques, leurs points de vue et leurs définitions de ce qui est approprié et inapproprié.

Zhang et ses collègues (2015) ont d'ailleurs conduit une recherche intéressante, intitulée « The classification of hackers by knowledge exchange behaviors », où ils ont analysé les messages publiés dans un forum de pirates informatiques pour élaborer des profils d'utilisateurs sur la base des modèles de transfert de connaissances observés. Ils ont conclu que les communautés de *hackers* représentent principalement des communautés d'apprentissage, où ils ont pu observer une synergie entre : (1) les *hackers* plus expérimentés, qui prodiguent leurs conseils et perles de sagesse (*gurus type*) ; (2) ceux qui possèdent des compétences avancées, qui recherchent à élargir leurs connaissances et à les partager avec les autres (*learning type*) ; (3) les *hackers* qui observent passivement les échanges (*casual type*) ; (4) et finalement les apprentis (*novice*) (Zhang et al., 2015). Cet environnement propice au mentorat représente le type d'environnement d'apprentissage social qu'Akers décrit dans sa théorie, comme étant le fondement sur lequel les autres variables d'apprentissage social interagissent (Akers, 2009; M. K. Rogers, 2001).

D'ailleurs, l'étude de Décary-Hétu (2013a) a cherché à comprendre comment les pirates du monde informatique interagissent entre eux et construisent leurs propres réseaux personnels, et est arrivée à la conclusion que ces derniers ont tendance à se rassembler et former des groupes restreints et intimes, vraisemblablement dans le but de pouvoir cultiver un sentiment de confiance et de sécurité, favorisant ainsi du même coup les liens entre de potentiels mentors et leurs apprentis (Décary-Hétu, 2013a). Ainsi, les pirates peuvent apprendre leur comportement criminel respectif et faire valoir leurs compétences, parmi des individus qui ont une attitude positive envers ces types de comportements déviants.

Si bien, qu'il s'est avéré que l'un des principaux facteurs prédictifs de la criminalité informatique est le fait de fréquenter des pairs qui pratiquent ces activités (Décary-Hétu,

2013a; Higgins & Wilson, 2006; Holt et al., 2010; Marcum et al., 2014) (Holt and Bossler, 2014). Il n'est alors pas surprenant que l'apprentissage de la criminalité informatique soit principalement motivé par les pairs et le transfert de connaissances, sous la forme d'un apport de connaissances ou d'une recherche de connaissances, et qu'il joue un rôle important au sein de ces communautés (Baillargeon-Audet, 2010; Hinduja & Ingram, 2009; Holt et al., 2012; Larribeau, 2019; Navarro & Marcum, 2019a; Sharma, 2007; Skinner & Fream, 1997; Zhang et al., 2015).

3.2 Les définitions favorables

Il a été observé qu'au sein de ces communautés de pirates informatiques, il ne s'y effectue pas qu'un transfert de connaissances, d'outils et de techniques, mais également une assimilation de définitions favorables à la commission d'activités criminelles, qui détermineront l'attitude d'un acteur vis-à-vis cette forme de déviance (Akers, 2009; Akers et al., 2017, 2021; Baillargeon-Audet, 2010; Boman & Freng, 2017; Holt & Copes, 2010; Steinmetz & Nobles, 2018).

Si les définitions internalisées d'un usager d'Internet, provenant majoritairement de son environnement dans les communautés en ligne et des pairs avec lesquels il s'associe, sont favorables à la perpétration d'un cybercrime, il adoptera alors un comportement délinquant, et inversement, si elles sont défavorables à l'engagement dans cette voie, celle-ci sera évitée (Boman & Freng, 2017; Holt et al., 2012; Holt & Copes, 2010; Montégiani, 2017; Steinmetz & Nobles, 2018). En effet, un comportement en ligne considéré comme étant socialement déviant ou carrément illégal nécessite l'internalisation de définitions favorables pour le passage à l'acte, puisqu'il ne s'agit pas d'un type de criminalité auprès de laquelle n'importe qui peut s'engager, sans s'investir pour acquérir certaines techniques avancées (Hinduja & Ingram, 2009).

La plupart des études ayant mis à l'épreuve le lien de causalité entre l'intégration de définitions favorables et la commission d'un cybercrime se sont penchées sur l'utilisation, le téléchargement et la distribution de matériel numérique de manière illégale, tel que la musique, les films et les logiciels, et sont arrivées à des résultats concluants (Higgins et al., 2007; Higgins & Makin, 2004; Higgins & Wilson, 2006; Hinduja & Ingram, 2009; Holt & Copes,

2010; Morris & Higgins, 2010). En effet, les résultats de ces études ont démontré que les individus ayant montré des définitions et attitudes positives face à ces activités avaient également un score élevé au niveau de la participation à ce type de crime, confirmant les hypothèses préétablies par les auteurs.

Pour ce qui est du piratage informatique, Skinner et Fream (1997) ont trouvé qu'après l'association différentielle, l'intégration de définitions favorables représentait le prédicteur le plus constant pour ce type d'activité criminelle. L'étude de Rogers (2001) est arrivée aux mêmes résultats, à l'effet qu'un modèle prédictif composé des variables d'association différentielle et de définitions sera significatif pour les scores d'indice de criminalité. Cela signifie que, plus un individu définira un comportement informatique déviant comme étant positif, acceptable ou justifié, et qu'en plus il s'associe à des individus ayant des points de vue similaires, et plus la probabilité qu'il adopte ce comportement sera élevée.

Enfin, l'étude de Décary-Hétu (2013a), qui a observé la formation de réseaux restreints de pirates informatiques dans les canaux de clavardage, mentionne dans son analyse que cette structure de socialisation fourni un environnement idéal où peuvent se créer des liens de confiance entre des mentors et des apprentis, et mettre à l'œuvre les principes d'association différentielle, de renforcement et de définitions. En effet, l'identification criminelle d'un usager d'Internet peut se produire au cours d'une expérience directe dans des groupes d'appartenance délinquants, par une référence positive aux rôles criminels, ou en tant que réaction négative aux forces opposées au crime (Holt & Copes, 2010).

3.3 L'imitation

À ce jour, le principe de l'imitation n'a pas énormément été exploré dans la littérature concernant la cybercriminalité, mais ceux qui y sont aventurés ont souligné l'importance de l'imitation dans le processus d'apprentissage social, insistant sur la nécessité de prendre cet aspect en compte dans les études liées aux crimes informatiques (Holt et al., 2010; Navarro & Marcum, 2019a; Sharma, 2007; Skinner & Fream, 1997). Le processus d'apprentissage social est lié à la cybercriminalité, car les individus seraient plus susceptibles de commettre un cybercrime s'ils disposent de modèles déviants à imiter (Hinduja & Ingram, 2009; Holt et al., 2010, 2012; Skinner & Fream, 1997).

L’analyse de Holt et al. (2010) a démontré que l’imitation jouait même un rôle plus important que le renforcement différentiel dans l’apprentissage social des déviants. Selon les auteurs, ce résultat reflète la nature « unique » de la cyberdéviance puisque les compétences en informatique ne sont pas à la portée de tous, et que les individus doivent souvent s’en remettre à leurs pairs délinquants pour élargir leurs connaissances dans le domaine (Holt et al., 2010)

L'imitation peut se produire par de nombreuses voies conventionnelles (comme les amis, les parents, les enseignants, qui possèdent du matériel piraté, par exemple), mais également par voie non conventionnelle (plateformes en ligne) (Skinner & Fream, 1997), où ils peuvent observer ce que font leurs amis (Holt et al., 2010). Justement, les résultats les plus éloquents que Skinner et Fream (1997) ont obtenus sont liés à l’utilisation de babillards électroniques (*bulletin boards*) : la fréquentation de ce type de plateforme augmentait la fréquence des tentatives de deviner des mots de passe, dans le but d’obtenir un accès non autorisé (Skinner & Fream, 1997).

Les auteurs de ces études ont tout de même tenu à apporter des clarifications quant à leurs résultats. D’une part, un taux significatif pour l'imitation pourrait indiquer que l’échantillon contenait un nombre plus élevé de répondants qui en sont encore au stade de l'initiation à la cyberdéviance, plutôt que des délinquants plus expérimentés et chroniques (Holt et al., 2010). D’autre part, étant donné la difficulté d'appréhender et de sévir contre le piratage de matériel numérique (téléchargement illégal), l'imitation est susceptible de se produire en l'absence d'un contexte de dissuasion générale, communiqué via les médias, par exemple (Navarro & Marcum, 2019a).

3.4 Le renforcement différentiel

Cela nous amène à la question du renforcement différentiel en lien avec la criminalité informatique, selon laquelle un individu aura plus de chance de participer à des actes déviants s’il reçoit davantage de renforcement positif pour ses actes déviants, que pour ses actions conformes (Akers, 2009; Akers et al., 2017, 2021). À cet effet, certains auteurs ont avancé que les usagers d’Internet sont plus susceptibles de commettre un crime informatique s'ils font l'expérience d'un renforcement positif soutenant la violation des lois liées à la

cybercriminalité (Hinduja & Ingram, 2009; Holt et al., 2010, 2012; Navarro & Marcum, 2019a; M. K. Rogers, 2001; Skinner & Fream, 1997).

Les résultats obtenus par Skinner et Fream (1997), par Rogers (2001) et plus tard par Holt et al. (2010) ont soutenu ces affirmations lorsqu'ils ont révélé que les individus ayant participé à une activité informatique criminelle avaient des niveaux de renforcement différentiel plus élevés que les individus n'ayant pas participé à ce type d'activité criminelle. Skinner et Fream (1997) ont constaté que le renforcement différentiel avait un effet négatif sur l'accès non autorisé aux documents en ligne, une constatation qui sera plus tard également confirmée par les travaux d'Holt et al. (2010). En effet, en étudiant les croyances et les attitudes des pirates informatiques, il s'est avéré que les sanctions formelles de la part des forces de l'ordre jouaient un rôle très faible dans leur processus de décision, puisque même si les personnes interrogées étaient conscientes que des sanctions légales pouvaient résulter du piratage, elles pensaient qu'il était peu probable qu'elles soient détectées en raison de leurs pratiques de téléchargement prudentes (Holt & Copes, 2010; Sharma, 2007). Les *hackers* croient qu'ils opèrent dans un monde d'anonymat, où les chances de se faire prendre sont minuscules (Sharma, 2007).

D'ailleurs, nous savons qu'à travers leurs interactions en ligne, les pirates apprennent également la manière de reconnaître et d'éviter les risques associés au piratage, qui peuvent éventuellement amener des conséquences, donc un renforcement négatif (Décary-Hétu, 2013a; Holt & Copes, 2010), mais les éléments du renforcement différentiel observés ne sont pas toujours strictement de nature éducative. En effet, les interactions entre pairs délinquants en ligne permettent de se vanter de ses exploits et de recevoir des encouragements sociaux face à ceux-ci, des renforcements positifs qui peuvent jouer un rôle dans l'engagement de l'acteur dans cette forme de criminalité (Holt, 2007; Holt et al., 2010). Leurs résultats ont indiqué que les individus étaient plus susceptibles de commettre des actes de déviance informatique lorsqu'ils recevaient des éloges ou des encouragements à adopter ces comportements de la part de leur entourage, au travail ou à l'école (Holt et al., 2010). De plus, ils ont observé que le soutien à la déviance pouvait aussi se produire en dehors des réseaux de pairs délinquants, à travers des figures d'autorités, comme les professeurs ou les patrons, une source d'influence non négligeable (Holt et al., 2010).

La théorie de l'apprentissage social tel qu'élaborée par Akers peut donc constituer un excellent cadre théorique pour en savoir plus au sujet des pirates informatiques et leurs interactions au sein de leurs communautés, puisque l'association différentielle met en contact les pairs délinquants, les faisant potentiellement basculer vers les activités criminelles, tandis que l'acquisition de définitions favorables au crime, l'imitation et le renforcement différentiel peuvent le maintenir dans sa déviance. Globalement, les études recensées soutiennent de manière plus ou moins modeste, la corrélation entre différentes composantes de la théorie de l'apprentissage, lorsqu'appliqué à la criminalité informatique, et plus précisément au piratage informatique.

Le *hacker* malveillant est reconnu comme un criminel constamment en processus de développement, car il doit acquérir différentes connaissances et techniques tout au long de son parcours criminel, et même demander l'aide à des pairs délinquants lorsque nécessaire. Une fois qu'il s'intègre à une communauté et qu'un réseau social est créé, composé d'associations avec des individus favorables à la cybercriminalité et même de mentors, des modèles d'imitation et l'intériorisation de définitions favorable à cette forme de criminalité peuvent alors s'opérer. Ensuite, des éléments de renforcement peuvent jouer un rôle dans la détermination de la perpétuation du crime. Les études recensées ci-haut ont fait ressortir que l'association avec des pairs déviants, l'internalisation de définitions déviantes et l'imitation constituent des facteurs de risque significatifs dans la perpétration du piratage informatique.

Chapitre 4 – Problématique

Il n'a été possible de recenser que quelques travaux de chercheurs qui se sont réellement focalisés sur les pirates informatiques qui tentent d'accéder à des ressources de façon non autorisée, à travers la perspective de l'apprentissage social (voir Roger, 2001, Décary-Hétu, 2013, Marcum et al., 2014, et Montégiani, 2017). Les études de Rogers (2001) et de Marcum et al. (2014), se sont appuyés sur des données provenant des questionnaires auto-rapportés distribués dans des écoles. En ce qui concerne l'étude de Décary-Hétu (2013), l'analyse a été basée sur des conversations publiques récupérées sur une plateforme de clavardage, Internet Relay Chat (IRC), une plateforme largement fréquentée par les pirates informatiques à l'époque. Finalement, le mémoire de Montégiani (2017) s'est effectué sur la base de

publications publiques, extraites d'un forum de discussion dédié aux activités de piratage informatique.

Il existe donc très peu d'études qui ont considéré l'apprentissage social chez les pirates informatiques, malgré le nombre considérable d'auteurs qui ont souligné la pertinence de cette théorie pour examiner la cybercriminalité, ainsi que l'importance de s'y intéresser (Boman & Freng, 2017; Hutchings & Holt, 2018; Marion & Twede, 2020; Navarro & Marcum, 2019a; Steinmetz & Nobles, 2018).

De plus, mis à part les études de Décary-Hétu (2013) et de Montégiani (2017), qui ont analysé des échanges publics, la grande majeure partie des travaux qui se sont penchés sur la cyberdéviance, au sens large, ont soutenu leurs analyses sur la base de questionnaires auto-rapportés provenant de jeunes étudiants volontaires, au sein d'établissements participants. Le niveau de généralisation des conclusions de ces études est donc questionnable. En effet, l'échantillon de Higgins et Makin (2004) était principalement composé d'étudiants « blancs » d'un collège de l'Est des États-Unis, tandis que les échantillons de Higgins et Wilson (2006) et de Higgins et al. (2007) provenait d'une seule université américaine. Morris et Higgins (2010) ont quant à eux sondé des étudiants provenant de deux universités, et enfin Marcum et al. (2014) ont distribué leurs sondages dans quatre écoles secondaires, toutes situées dans le même comté rural.

Par conséquent, non seulement ces résultats ne sont peut-être pas généralisables à toute la population estudiantine, mais cela soulève également des questions quant à la possibilité de généraliser ces résultats à d'autres types de populations (Gauthier, 2010). Certains chercheurs ont justifié ce choix méthodologique en invoquant le fait que les jeunes éduqués faisaient partie d'une tranche de la population qui avait davantage de chance d'être familière avec ces « nouvelles technologies » et de s'en servir (Boman & Freng, 2017; Higgins & Makin, 2004; Holt et al., 2010). Or, avec une démocratisation sans cesse grandissante des ordinateurs et d'Internet, ces études risquent de ne plus être représentatives de la réalité actuelle. Il existe donc une lacune importante dans les connaissances scientifiques actuelles à ce sujet.

C'est pourquoi l'objectif de recherche qui a guidé cette étude est de décrire et comprendre le processus d'apprentissage social des pirates informatiques. Cet objectif

s'opérationnalisera à travers deux sous-objectifs, qui s'articulent autour du concept de l'association différentielle et de l'imitation : (1) comprendre le rôle des liens sociaux entretenus par les pirates informatiques, dans le monde « réel » et dans le monde virtuel, ainsi que (2) comprendre le rôle de l'imitation dans leur apprentissage et le développement de leurs compétences.

De plus, à l'heure actuelle, aucune étude cherchant à comprendre les mécanismes de l'apprentissage social ne s'est basée sur des entretiens avec des pirates informatiques toujours actifs. Bien que le questionnaire auto-rapporté ait été l'un des outils de collecte le plus intéressant et populaire en recherche criminologique, notamment en ce qui concerne la victimisation, certains auteurs estiment qu'il s'agit d'un outil qui a été surexploité en sciences sociales, sans qu'on ait tenu compte des limites inhérentes à son utilisation (Champion, 2006; Gauthier, 2010). En effet, une des limites principales liées aux sondages ou aux questionnaires autoadministrés est le niveau de fiabilité des données (Champion, 2006; Gauthier, 2010; Hartley et al., 2020), surtout lorsqu'il est question de demander à des jeunes de déclarer honnêtement des comportements délinquants (Marcum et al., 2014). Pour toutes sortes de raisons, il y a un risque que les participants remplissent le questionnaire de manière erronée, soit parce qu'ils ne comprennent pas réellement le contexte de l'étude et vont fournir des réponses inexactes, ou vont répondre aléatoirement pour terminer le sondage plus rapidement (Champion, 2006; Hartley et al., 2020).

Pour toutes ces raisons, la présente étude propose une méthodologie basée sur des entretiens avec des pirates informatiques. Historiquement, il s'agit d'un type de population qui est assez difficile d'accès puisque les individus sont activement engagés dans des activités criminelles, ils ne veulent donc pas avoir l'attention des chercheurs et des journalistes (Hutchings & Holt, 2018; Jordan & Taylor, 1998; Marion & Twede, 2020). Par contre, cette méthode permettrait de combler les lacunes et les limites présentes dans la littérature existante, puisque du point de vue de la fiabilité et de l'exhaustivité des données, les entretiens semblent présenter un avantage par rapport aux questionnaires remplis par les répondants (Champion, 2006; Hartley et al., 2020). L'une des forces principales de cette méthode de collecte est qu'elle donne un accès direct à l'expérience des individus. Les données sont plus riches en détails et en descriptions (Gauthier, 2010). Cette méthode permet aussi d'être en meilleure posture pour s'assurer que les participants comprennent

bien les questions, ainsi que le contexte de l'étude, afin qu'ils fournissent des réponses appropriées et complètes (Champion, 2006; Gauthier, 2010; Hartley et al., 2020). Les entrevues permettent également une plus grande flexibilité dans le processus d'interrogation, et donc un meilleur contrôle du contexte dans lequel les questions sont posées et les réponses données, un contexte, qui plus est, peut être négocié entre les interlocuteurs (Champion, 2006; Gauthier, 2010).

Dans une optique où cette étude tente de bien comprendre l'expérience et la perspective des participants par rapport à leur processus d'apprentissage, il sera possible adapter le schème d'entrevue pendant son déroulement, afin de tenir compte du discours des participants interviewés (Gauthier, 2010). Sans données qualitatives, il ne serait pas possible de comprendre le phénomène d'apprentissage social en cybercriminalité au-delà des résultats limités, qui peuvent être produits à partir d'études quantitatives d'échantillons d'étudiants, et qui fournissent un aperçu limité du comportement des délinquants (Hutchings & Holt, 2018).

Chapitre 5 – Méthodologie

La présente étude s'est basée sur les données collectées de dix-sept entretiens semi-dirigées avec des pirates informatiques actifs, provenant de trois forums de discussions axés sur le piratage informatique. Les entretiens qualitatifs sont particulièrement appropriés en contexte de recherche exploratoire (Hutchings & Holt, 2018). En effet, dans leur article intitulé « Interviewing Cybercrime Offenders », Hutchings et Holt (2018) ont souligné la nécessité pour les futurs chercheurs d'employer des méthodes qualitatives pour étudier la cybercriminalité, puisqu'ils permettent des analyses approfondies de phénomènes relativement nouveaux, en plus de permettre d'identifier de nouvelles pistes de recherche (Hutchings & Holt, 2018). De plus, puisque nous cherchons à comprendre les processus d'apprentissage social, les entretiens sont également à privilégier pour comprendre des phénomènes au niveau « micro », surtout en ce qui concerne une population difficile d'accès (Hutchings & Holt, 2018). L'Internet est un outil méthodologique particulièrement adapté à la recherche de groupes spécifiques d'internautes, et davantage lorsque la question de recherche implique un phénomène social en ligne. Une force potentielle de la méthode est donc d'effectuer la recherche dans le lieu naturel d'intérêt (O'Connor & Madge, 2021).

5.1 Échantillon

Il a été possible d'obtenir la participation de dix-sept sujets (n=17), provenant de trois plateformes de communautés en ligne différentes. Pour être éligible à participer à cette étude, trois critères d'inclusions ont été retenus. Premièrement, les participants devaient avoir atteint l'âge de la majorité (être âgées d'au moins 18 ans), dans le but de faciliter la prise de consentement, et aussi de s'assurer d'avoir un échantillon plus homogène. Deuxièmement, les participants devaient pouvoir s'exprimer et comprendre la langue française ou anglais, en raison de la limite linguistique de la chercheuse, et afin d'éviter des erreurs d'interprétation. Et finalement, les participants devaient avoir accédé à un système informatisé de façon non autorisée, dans les derniers vingt-quatre mois. La période de vingt-quatre mois a été établie arbitrairement afin de permettre de rejoindre le plus de participants potentiels possible. Aucun critère d'exclusion n'a été prévu dans le cadre de cette étude.

Les entretiens se sont tenus à distance (en ligne), de façon complètement anonyme, et visaient des participants provenant de partout dans le monde. À aucun moment la chercheuse n'a eu accès à l'identité des individus participants à l'entretien. Les entretiens ont été effectués de manière complètement anonyme, puisqu'aucune donnée identifiante n'est nécessaire à la réalisation de l'analyse. Aucun nom de plateforme où le recrutement a été effectué ne sera mentionné dans l'étude, et tous les noms d'usager ont été remplacés par un identifiant numérique aléatoire. Ainsi, aucun nom d'usager de participant n'a été sauvegardé dans les transcriptions d'entretiens. Aucune plateforme de messagerie particulière n'a été imposée aux participants. La chercheuse s'est adaptée à la plateforme sécurisée que le participant estimait qu'elle protégeait son identité de manière suffisamment satisfaisante, afin que le participant se sente à l'aise de procéder à un entretien. Cette mesure a été largement appréciée des participants et a pu mitiger le niveau de méfiance.

Un document d'information et de consentement a été mis à la disposition des participants potentiels, en l'hébergeant sur le site Web du directeur de recherche, le professeur David Décary-Hétu, pour le rendre disponible pour consultation en tout temps. De plus, aucun formulaire de consentement n'a été requis de la part des candidats, et seul un consentement verbal (textuel) a été enregistré en début d'entrevue. Certains éléments personnels dans les propos recueillis ont été modifiés dans la transcription à la demande des participants, afin de respecter leur vie privée. Puisque les entretiens ont été effectués de manière complètement

virtuelle, les sujets ont pu participer à l'étude dans le confort de leur domicile ou tout autre environnement personnel, afin de leur permettre de se sentir plus à l'aise et moins à risque.

Malgré le fait d'avoir clairement communiqué les critères, plusieurs candidats potentiels se sont manifestés alors qu'ils ne correspondaient pas au critère d'âge ou critère technique. Il a toutefois été important de garder un certain rapport amical avec ceux-ci, de manière à ce qu'ils puissent se porter garant auprès d'autres participants potentiels. Ainsi, la chercheuse est entrée en contact avec un nombre considérable de candidats, qui ont pour certains, changé d'idée en cours d'entrevue, ne se sont jamais présentés à la date convenue ou d'autres qui sont simplement complètement disparues de la plateforme, avant d'en arriver à obtenir les 17 entretiens sur laquelle est basée cette étude.

5.2 Collecte

La première étape a été de recenser des plateformes en ligne où les pirates informatiques susceptibles de vouloir apprendre en communauté allaient se retrouver. Un message a été publié dans trois subreddits (https://www.reddit.com/) dédiés au piratage informatique, r/HowToHack, r/Hacking et r/Hacking_Tutorials, pour demander aux membres quelles plateformes ou forums de discussion ils recommandaient pour les personnes désireuses d'apprendre à pirater. Plusieurs d'entre elles ont été mentionnées et la chercheuse a arrêté son choix sur les huit plateformes les plus souvent recommandées.

Un compte a été créé sur ces plateformes, puis un message de sollicitation public, préalablement approuvé par le CER-SC, a été publié dans les sections appropriées, sur chacun des forums de discussion où les règles et politiques n'interdisaient pas ce type de sollicitation. Malgré le fait de ne pas avoir contrevenu à aucune règle de conduite spécifiée sur la plateforme, plusieurs de ces messages ont été supprimés. Il a donc fallu contacter les différents modérateurs pour obtenir leur autorisation de recruter sur leur plateforme, ainsi que les modalités permises, pour éviter que la chercheuse ne soit bannie du forum. Les modérateurs ont affirmé ne pas vouloir tolérer de manière publique la présence de chercheurs sur leur plateforme, ce qui est compréhensible et cela a été respecté. Ce type de réaction a déjà été relevé par d'autres chercheurs par le passé (Hutchings & Holt, 2018; O'Connor & Madge, 2021).

C’est ainsi que la prochaine étape du recrutement s’est mise en marche : en participant aux discussions, en contribuant sur le forum et en faisant connaissance avec les usagers qui le fréquente de façon très régulière. C’est ainsi que, de fil en aiguille, certains participants se sont sentis suffisamment à l’aise et ont accepté de participer au projet de recherche, tantôt par curiosité et parfois dans un esprit de camaraderie. À de rares occasions, il a été possible d’obtenir des participants via références ou contacts, mais il y eu assurément beaucoup de bouche-à-oreille concernant le projet, ce qui a probablement grandement aidé au niveau de la méfiance des participants. Il a été important de demeurer discret quant à la participation, ou non, des usagers qui étaient en contact avec la chercheure. Ainsi, un des principaux obstacles au recrutement a été de gagner la confiance des membres et d’établir une crédibilité en tant qu’étudiante en criminologie pour le projet de recherche, sans être associée à la police (ou au FBI !).

Enfin, dès qu’un membre signifiait un intérêt quelconque envers le projet de recherche, un lien vers le document d’information et de consentement lui a été envoyé. Par ailleurs, aucune compensation n’a été offerte pour la participation à l’étude.

Conduite d’entrevues

Si après avoir consulté le document d’information et de consentement, le sujet manifestait toujours son désir de participer à l’étude, une date et heure était convenue pour réaliser l’entrevue. De plus, chaque participant pouvait choisir la plateforme de messagerie anonymisée et dont les communications sont chiffrées, de son choix, de façon à qu’il se sente en sécurité de répondre aux questions. Les participants ont eu le choix de réaliser l’entrevue par appel vocal (VoIP), ou s’ils le préfèrent, entièrement par clavardage, mais tous les participants ont indiqué préférer procéder par clavardage. Les entretiens en ligne sont de plus en plus appréciés comme méthode de recherche valide et légitime. En effet, les données recueillies par le biais d’entretiens en ligne seraient aussi riches et d’aussi bonne valeur que celles générées lors d’entretiens en personne (O’Connor & Madge, 2021).

Les entrevues se sont donc tenues entre le 28 mai 2021 et le 12 juillet 2021. Un total de dix-sept entretiens semi-dirigés ont été menés, d’une durée totale cumulée de 35,7 heures. Les entrevues ont duré en moyenne 2 heures, et la durée d’une entrevue a varié entre 1 heure et 4 heures.

Avant le début de chaque entretien, les modalités de participation détaillée dans le document d'information ont été rappelée à chaque participant afin de s'assurer d'obtenir son consentement éclairé.

Ensuite, après l'obtention de son consentement, chaque participant a été soumis à une question générale d'ouverture, qui était : « Quelles sont les trois compétences qui sont cruciales dans votre carrière criminelle et comment les avez-vous apprises ? ». Pour étudier les sous-objectifs de recherche, la chercheure s'est également assurée d'aborder les thématiques suivantes : le rôle des relations sociales dans la « vraie vie » et dans le monde virtuel, ainsi que le rôle de l'imitation dans le processus d'acquisition de ces compétences.

L'interactivité en temps réelle et l'utilisation d'une technologie avec laquelle les participants sont déjà familiers, dans un environnement sécurisant font partie des avantages de l'entretien par clavardage relevés par d'autres auteurs (Hutchings & Holt, 2018; O'Connor & Madge, 2021).

Transcriptions

Puisque les entrevues se sont toutes déroulées dans des plateformes de messageries différentes, il a fallu exporter la conversation et sauvegarder la transcription dans un fichier Microsoft Word. Ces fichiers ont ensuite été classés dans des dossiers archivés protégés par mot de passe (.zip). Pour assurer l'anonymat et la confidentialité des entretiens dans les transcriptions, toutes les mentions de nom d'utilisateur ou de plateforme à l'intérieur des transcriptions ont été caviardées, et chaque participant a reçu un identifiant numérisé aléatoire pour l'identifier. La chercheuse et le directeur de recherche sont les seuls à avoir accès aux données brutes collectées.

5.3 Analyse

La question de recherche guidant le présent travail est de nature plutôt exploratoire, puisqu'elle vise un thème qui été peu analysé dans la littérature. L'objectif étant de comprendre le processus d'apprentissage social des pirates informatiques qui s'introduisent dans des systèmes informatisés de façon non autorisée est donc de nature inductive. Des données qualitatives d'entretiens semi-dirigées avec 17 pirates informatiques présentement actifs ont été collectées dans le but de tirer une description riche de leurs processus

d'apprentissage individuel, ainsi que des différentes composantes l'ayant influencé, tel que le rôle qu'ont joué les pairs et le rôle de l'imitation. Ce qui est visé ici n'est pas nécessairement d'établir une causalité linéaire, mais surtout de comprendre et donner un sens à ces évènements de vie tels qu'ils ont été perçus et vécus par les participants (Gauthier, 2010).

Pour en faciliter la démarche, les transcriptions ont été téléversées dans le logiciel QDA Miner, qui a permis la gestion, la codification et l'analyse des données qualitatives obtenues. Les entretiens ont été examinés à l'intérieur du logiciel et une codification par thème de recherche a été appliquée aux extraits qui les traitaient : les compétences importantes pour la réussite, l'influence de l'entourage et rôle de l'imitation. De plus, pour chaque nouveau type de compétence, un nouveau code a été créé. L'arborescence de codification des variables s'est opérationnalisée de la façon suivante :

- **Compétences importantes**
  - Compétence 1
  - Compétence 2
  - Compétence 3
  - ....
  - Explications quant à l'acquisition de compétences
- **Mention d'un entourage/amis/influence**
  - Monde réel
  - Monde virtuel
  - Mention d'un mentor
- **Question de l'imitation**
  - Imitation importante
  - Imitation non importante

Une analyse thématique a ensuite permis de faire ressortir les éléments les plus mentionnés et pertinents à l'étude, et de départager ceux plus marginaux et d'importance moindre.

Chapitre 6 – Résultats

6.1 Compétences cruciales pour la réussite

Une question d'ouverture a été posée aux participants (n= 17) pour débuter chacune des entrevues, à savoir quelles compétences les pirates informatiques considéraient comme étant importantes dans leur réussite et comment ils les avaient acquises. Tous les participants ont répondu à cette question et plusieurs éléments sont ressortis, mais seules celles ayant été mentionnées par au moins 4 participants ont été retenues pour l'analyse.

Ces derniers ont pu être classés en deux catégories : (1) **les compétences techniques** et (2) **les compétences personnelles**. Les compétences techniques sont en lien avec des connaissances ou habiletés spécifiques à l'informatique, tandis que les compétences personnelles représentent surtout des traits de personnalités ou des aptitudes générales (*voir Tableau 2*).

Tableau 2. – Tableau des compétences mentionnées en entrevue, selon le type de compétence

	Compétence mentionnée
Compétences techniques	Connaissances en informatique / réseautique
	Programmation informatique (codage)
Compétences personnelles	Compétences sociales / Ingénierie sociale
	Patience / Persistance
	Pensée créative

Dans les sous-sections suivantes seront détaillées les compétences qui ont été citées dans les entretiens comme étant importantes dans la réussite des pirates informatique.

Connaissances en informatique et en réseautique

Cette compétence englobe de façon générale l'importance d'avoir des connaissances de base des fondements entourant l'informatique et de la réseautique, et que ceux-ci soient relativement variées (n= 12 ; 71%). Les exemples qui ont été cités concernent notamment le fonctionnement des pares-feux pour savoir les contourner, maîtriser les systèmes

d'exploitation pour savoir où se trouvent les répertoires d'intérêt, bien connaître les applications, ou même les services infonuagiques spécialisés.

Ces deux citations ont été choisies pour illustrer ces propos :

> "Well, definition of hackers kinda relates to hacking things, or in general words, tryna break things. [...] so to know how to break a thing, you probably wanna know how it was built [...]."
>
> – Participant ID #2086
>
> "When you successfully break into the server of a website, and you don't know your way around the terminal, you will most likely get caught before you can do any damage/download the data you want [...]."
>
> – Participant ID #2056

L'importance d'avoir des connaissances en informatique et en réseautique a été justifiée de plusieurs façons. D'abord, il semble évident que pour savoir comment exploiter une vulnérabilité, il est essentiel de comprendre les principes de bases qui régissent le contexte au sein duquel elle se trouve. Souvent, ces « connaissances de base » telles qu'explicitées par les participants se sont avérées être des connaissances en réseautiques. En effet, la maîtrise des concepts de base des réseaux informatiques peut s'avérer essentielle à toutes phases d'une attaque, que ce soit à l'étape de la compromission d'un système, de l'exploitation de la vulnérabilité, ou au moment de l'évasion pour éviter la détection. De plus, plusieurs ont mentionné que la réseautique constitue une excellente base sur laquelle bâtir et développer d'autres connaissances plus avancées.

En dehors des connaissances générales en informatique et en réseautique, parfois les pirates informatiques se trouvent confrontés à des défis spécifiques à leur cible, auquel cas, les pirates informatiques se doivent de consulter de la documentation technique concernant les technologies qui composent l'infrastructure qu'ils tentent de compromettre.

Finalement, il serait impensable de ne pas connaître quelques principes fondamentaux de la sécurité opérationnelle, des outils et techniques d'anonymisation qui sont primordiaux pour minimiser les traces de leurs activités sur un réseau, ainsi que les traces pouvant mener à leur identification.

Programmation informatique (codage)

Une autre compétence technique à avoir été très souvent citée est la capacité de programmer dans au moins un langage informatique (n=11 ; 65%). Plusieurs ont mentionné l'utilité de pouvoir analyser l'envers du décor d'une interface, que ce soit au niveau du système d'exploitation ou au niveau du Web, mais également le côté pratique de pouvoir coder leurs propres outils (*script*) – ou ne serait-ce que d'avoir les connaissances de base pour savoir adapter les scripts existants à leurs besoins.

> "To successfully compromise a target, you don't need to be able to write a program from scratch, but you absolutely need to be able to read the code which builds a program and understand each individual function. You must be able to understand what makes code malfunction, what could make it function better, why, and how these improvements or malfunctions can occur. It is entirely possible for a "successful hacker" to never have written a piece of code on their own so long as they have a fundamental understanding of programming."
>
> – Participant ID #2001
>
> "[...] most of the OS [operating systems] are written in C and also due to that, exploit codes are also written in C...it directly relates to more technical aspects like developing your own malwares or even exploits, they're all on native C language."
>
> – Participant ID #2086

Ici, il est surtout question de savoir déterminer de quel(s) langage(s) informatiques est constituée la plateforme ou l'application que les pirates informatiques ont dans leur mire, notamment au niveau de la couche du code source (*back end*). En génie logiciel, les termes *front-end* et *back-end* font référence aux deux types de préoccupation lors de la conception d'un logiciel ou d'une application : l'interface graphique (couche de présentation, ou *front-end*) et la couche où les données de l'infrastructure du logiciel se trouvent (*back-end*). Il ne serait pas forcément nécessaire de maîtriser totalement le langage utilisé par la plateforme ciblée, mais surtout d'en avoir une compréhension suffisante pour en distinguer les différents éléments et fonctions de manière individuelle, et comment ils interagissent entre eux pour assurer le fonctionnement de la plateforme. Il faut également être en mesure de comprendre ce qui pourrait faire dysfonctionner le programme, ou au contraire, comment se servir de ses fonctionnalités à son avantage.

Les connaissances en programmation peuvent également servir à créer des outils pour automatiser les processus d'exploitation, permettant d'attaquer plusieurs sites Web en même temps, par exemple, ou à lire et modifier les outils/scripts d'exploitation qui existent déjà, de manière à les adapter à leurs besoins.

Certains langages informatiques semblent être plus polyvalents, puisqu'ils peuvent être employés dans la plupart des champs du développement logiciel, tels que Python, tandis que d'autres sont fondamentaux dans la compréhension des systèmes d'exploitation embarqués, tels que les langages systèmes C et Rust. Quoiqu'il en soit, de se familiariser avec au moins un langage de programmation permet d'intégrer une logique qui peut servir de base à la compréhension des autres langages par la suite.

Pour la plupart des participants, la meilleure façon d'apprendre à programmer est simplement de programmer, en apprenant par soi-même et en s'aidant, au besoin, de vidéos YouTube, en recherchant des exemples de morceaux de codes disponibles sur Internet ou des forums et de les adapter. Certains ont mentionné avoir commencé à s'intéresser à la programmation puisqu'ils étaient intrigués par la conception de logiciels malicieux, ou maliciels (*malware*).

Étant donné la diversité du paysage d'Internet des langages de programmation qui le composent, il est plus ou moins possible de dépendre d'outils ou d'une méthodologie préétablie. Le processus manuel est donc important pour demeurer adaptatif. Un pirate qui n'apprendra jamais aucun langage de programmation serait donc voué à rester un « skid », ou *script kiddie* (pirate novice).

Compétences sociales et ingénierie sociale

Une des compétences personnelles à avoir été citée le plus souvent sont les compétences sociales, telles que des habiletés en communication et en réseautage, avec les gens ou des pairs délinquants (n=9 ; 53%). En contexte de sécurité informatique, l'ingénierie sociale englobe des techniques de manipulation psychologique visant à obtenir des informations confidentielles ou privilégiées, dans le but de frauder ou compromettre un système

> "Most hacking can be replaced with social engineering. Works better. Call someone or send them an email and u can get whatever u want XD."

– Participant ID #2070

> "You'd be surprised how far this gets you, social skillset plays a huge role into how you can social engineer in a long run, especially if you're a black hat. [...] People are aware of social engineering, and many corporates/companies take great effort to mitigating this, but these secure practices don't work when you're actually on a 1:1 talk with someone at an event or a meet up yknow? [you know]. "

– Participant ID #2086

Un des participants a également relevé la pertinence de posséder cette compétence en vue d'apprendre en communauté et potentiellement collaborer sur des projets :

> "Communication is also important if you work with a crew or are trying to cooperatively learn in a forum setting. [...] there's a lot of different kinds of people in the hacker community, and if you want to work with them there is a certain way of talking to them depending on their personality, same goes for an open source software project, if you want to build a big toolkit you might want to recruit some talented developers to help out, it ties into human nature, which ties into persuasion, which then leads in to the concept of social engineering as an attack vector in cyberattacks. So, as you can see communication is key in a lot of things."

– Participant ID #2062

Tel que mentionné par plusieurs participants, l'humain demeurera toujours l'élément le plus vulnérable dans la sécurité d'une infrastructure, puisque même en mettant en place les mesures de sécurité informatique les plus robustes, l'humain derrière un écran peut toujours commettre une erreur. Après tout, ce sont des humains qui sont derrière la conception, la gestion et le maintien des infrastructures. Le but des techniques en ingénierie sociale est de manipuler une personne de façon à l'amener à faire une action ou divulguer de l'information, dans l'intention de s'en servir de façon malicieuse. L'ingénierie sociale exploite donc un type de vulnérabilité qu'il n'est pas possible de corriger : les vulnérabilités humaines.

Il semblerait qu'en dégageant suffisamment d'assurance, il serait possible de faire faire pratiquement « n'importe quoi, à n'importe qui », comme par exemple, cliquer sur un lien, exécuter un fichier malicieux, révéler des informations confidentielles, en se faisant passer pour une personne dans son entourage ou un collègue de travail, notamment via un courriel

d'hameçonnage. Une méthode plus agressive consisterait à faire chanter une personne en menaçant de révéler de l'information compromettante qui a été trouvée à son sujet si elle ne s'exécute pas.

Les organisations sont au fait que de telles attaques existent et tentent tant bien que mal de s'en prémunit en effectuant de l'éducation et de la sensibilisation, mais selon les participants, ces concepts demeurent du domaine de l'abstrait lorsqu'ils sont confrontés à certaines situations qui requièrent leur intervention. Ce type d'attaque fonctionnerait si bien que, selon un participant, pratiquement toutes les tactiques attaques pourraient être remplacées par des techniques d'ingénierie sociale, puisqu'il serait beaucoup plus facile de simplement convaincre la bonne personne de poser une action.

Toutefois, les techniques d'ingénierie sociale n'impliquent pas forcément de la tromperie. Selon un des participants, être sympathique de façon consistante avec certains employés de bars ou de cafés, peut amener ces derniers à baisser leur garde et révéler des informations précieuses pour les pirates informatiques. D'autres fois, il s'agit de repérer des employés insatisfaits ou frustrés et de leur faire miroiter la possibilité de se venger de leur patron ou leur milieu de travail.

De manière plus générale, les compétences sociales peuvent également être utiles dans un contexte où un collectif de pirates informatiques doit travailler en équipe. Il existerait plusieurs types de pirates informatiques fréquentant les communautés et la bonne entente dépend parfois de compétences sociales, telles que la communication et le réseautage.

Au final, les compétences sociales demeureront toujours essentielles puisque dans plusieurs types de situations, les pirates informatiques auront affaire à des êtres humains. Plus ils maîtriseront les caractéristiques de leurs cibles et leurs vulnérabilités, et plus ils augmentent leurs chances de succès, ce que les pirates informatiques font généralement durant la phase de reconnaissance, l'étape qui précède une attaque.

Patience et persistance

La patience et la persistance sont des aptitudes qui ont également été rapportées à de nombreuses reprises par les participants (n=8 ; 47%). La plupart des explications font état de

processus itératifs qui demandent énormément de patience et de persévérance avant de pouvoir trouver une vulnérabilité ou un point d'entrée :

> "There are times where I audited software for days and I didn't find anything, different time I have found a lot of bugs. I am fully conscious that I can turn nothing in that audit, but I need to be patient and keep searching for those vulnerabilities. [...] Persistence? well, I think that will start to come to people when they realize they can't just be a hacker overnight and it takes time and dedication to learn how to code, writing exploits etc. that takes time to learn, and once people realize that things aren't instantaneous when it comes to hacking, they will slowly develop and improve their own persistence."
>
> – Participant ID #2033

La patience et la persistance ont souvent été employées de manière interchangeable pour exprimer l'importance d'être disposé à demeurer constant dans la poursuite de leurs efforts, d'être répétitif et insistant si nécessaire et de ne pas abandonner.

De manière générale, l'univers du piratage informatique est vaste et nécessite de la persévérance pour apprendre certaines connaissances de base et à programmer pour écrire un *exploit*, c'est-à-dire un logiciel ou morceau de code qui faire intervenir une série de commandes qui vont exploiter un bogue ou une vulnérabilité dans le but d'exécuter une action voulue, généralement malicieuse.

Parfois, une cible peut représenter un nouveau défi pour le pirate informatique, et il doit donc effectuer de nouveaux apprentissages, ainsi qu'essayer de nouvelles techniques, ou même se familiariser avec langue de la cible.

Pendant une des phases initiales d'une attaque, l'audit pour tenter de trouver un point d'entrée via un bogue ou une vulnérabilité, la patience et la persistance sont essentielles dans le processus, car il peut aisément se passer des heures et des jours avant qu'une des tentatives ne réussisse. Il serait alors facile pour un pirate inexpérimenté de se laisser décourager, alors qu'en fait, il faut savoir qu'il existe toujours une faille à exploiter. Ce principe s'appliquerait en revanche à toutes les phases d'une attaque informatique.

Pensée créative

Un certain état d'esprit (*thinking outside the box*) ainsi qu'une façon créative d'aborder les défis auxquels sont confrontés les pirates informatiques seraient des aptitudes importantes pour plusieurs raisons (n= 7 ; 41%). Premièrement, effectuer un audit de sécurité à l'aveuglette, sans avoir d'information sur l'infrastructure ni les mesures de sécurité mises en place par la cible, requiert un esprit imaginatif. Il existe bien sûr un certain nombre d'attaques standards, mais celles-ci deviennent rapidement inutiles lorsqu'il est question de s'attaquer à des cibles de niveau supérieur. Parfois, la sécurité d'une infrastructure peut paraître très robuste, et c'est là que la créativité intervient, car il existe toujours une faille à exploiter. Finalement, développer de nouveaux vecteurs d'attaque permet également de s'attaquer à de nouvelles cibles de façon insoupçonnée.

> "I believe the second skill is probably creativity; a lot of times, you must think outside the box, and act independently. There is no one-size-fits-all approach that can be applied in every situation."
>
> – Participant ID #2079

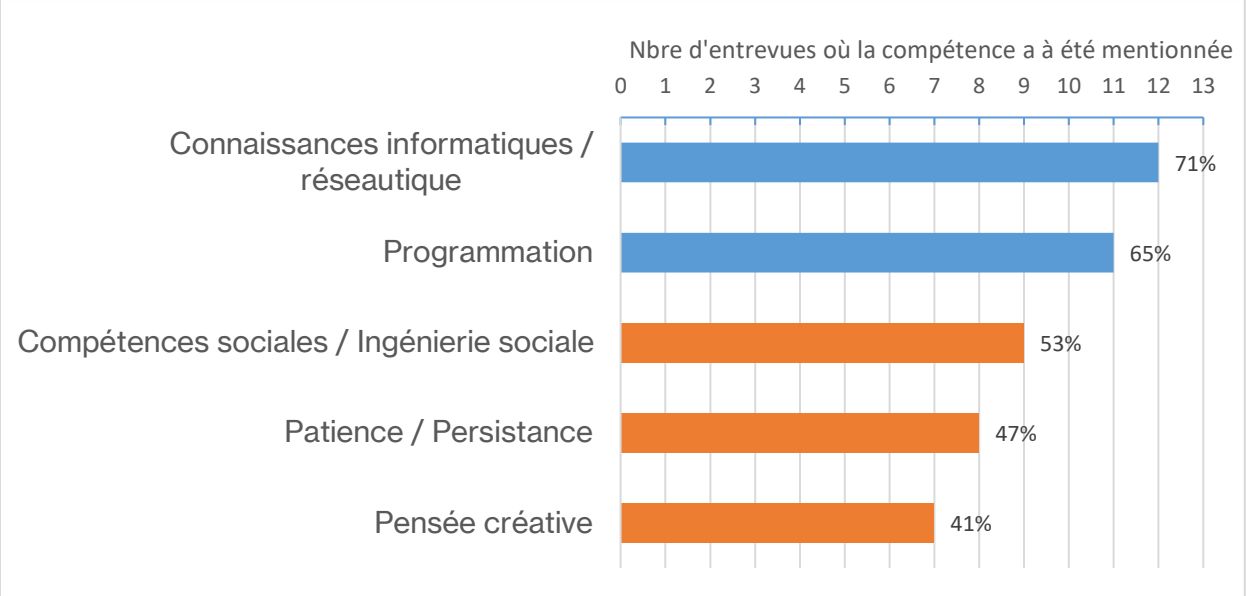
Il a été mentionné à quelques reprises qu'il n'existait pas de manuel d'instruction qu'il était possible de suivre pas à pas pour mener une attaque réussie à tout coup. Il n'est pas possible d'anticiper à l'avance toutes les sortes d'embûches qui se retrouveront au travers de la route lors d'une opération de piratage informatique. Il serait donc important d'être capable d'aborder un problème d'un point de vue unique, de sortir des sentiers battus, de penser à des moyens de réussir qui ne seraient pas conventionnels et de trouver des solutions originales à des problèmes imprévus.

Ce n'est pas en employant des techniques partagées à outrance dans les forums et déjà utilisées par d'autres qu'il sera possible de réussir une attaque. De plus, si une vulnérabilité a été largement exploitée par d'autres pirates informatiques et qu'elle a été répertoriée, il y a davantage de chances que celle-ci ait été corrigée, réduisant les chances de réussite d'une attaque. La créativité entre également en compte lorsqu'il est nécessaire de créer ou modifier un outil/script spécialisé et personnalisé pour qu'il soit adapté à la situation.

Ainsi, la patience, la persistance et la créativité sont souvent invoquées ensemble comme étant des aptitudes primordiales, des facteurs de réussite, pour aborder la résolution de problèmes lors d'attaques informatiques. De manière générale, chaque attaque informatique serait aussi unique que la personne qui mène l'attaque ainsi que la personne qui a élaboré le système sous attaque. Sans ces qualités, les chances de voir ses tentatives d'attaques réussir diminuent drastiquement. En effet, face à des problèmes, il est important de trouver des solutions qui peuvent ne pas être conventionnelles, et il est important de ne pas baisser les bras face à de nouveaux défis.

La figure ci-dessous illustre la proportion de compétences mentionnées dans les entretiens. L'axe gradué au-dessus représente le nombre de participants l'ayant cité, tandis que l'étiquette au bout des barres indique la même information, mais sous forme de pourcentage. De plus, les compétences techniques ont été signifiées en couleur bleue, tandis que les compétences personnelles ont été indiquées en couleur orangée, afin d'en faciliter la distinction au niveau visuel (*voir Figure 1).*

Figure 1. – Compétences cruciales en piratage informatique par le nombre de participants les ayant cités



Légende :

- Compétences techniques
- Compétences personnelles

Il est possible de constater d'un rapide coup d'œil au graphique que le nombre de compétences dites « personnelles » rapportées par les pirates informatiques est plus important que le nombre de compétences de type technique. En effet, seulement 2 types de compétences ont pu être considérées comme des compétences techniques, tandis que 3 aptitudes mentionnées ont pu être classifiées comme des compétences personnelles.

Par contre, parmi les trois compétences les plus mentionnées par les participants (n total de 17), deux se retrouvent à être des compétences techniques, à savoir, les connaissances en informatique et en réseautique (n=12 ; 71%) et la compétence en programmation (n=11 ; 65%). La troisième compétence la plus mentionnée est la compétence sociale et ingénierie sociale (n=9 ; 53%).

Les autres compétences et traits de personnalité qui ont été mentionnés par les participants et qui n'ont pas été représentés dans le graphique sont (en ordre de mention) :

- **Curiosité** (n=4 ; 24%) : Pour les participants ayant cité la curiosité comme un élément important auquel ils attribuent leur succès en tant que pirates informatiques, il s'agit surtout d'un état d'esprit qui est à la fois, à la source de ce qui les mène dans cette voie, et un moteur perpétuel.
- **Rétro-ingénierie** (n=3 ; 18%) : La rétro-ingénierie appliquée aux systèmes logiciels ou matériels est le processus d'analyse des composants, soit dans le but d'en permettre la création d'une conception entièrement reproduite, ou d'en comprendre la conception à partir des informations extraites. Pour un expert en sécurité, elle sera utilisée pour comprendre comment fonctionnent les programmes malicieux (*malware*), mais pour un attaquant, elle peut servir à connaître les vulnérabilités d'un système.
- **Sécurité opérationnelle** (n=3 ; 18%) : Cette compétence est liée aux pratiques de sécurité opérationnelle (OPSEC). La sécurité opérationnelle est un ensemble de processus de sécurité et de gestion des risques qui empêchent les informations sensibles de tomber entre de mauvaises mains. Évidemment, du point de vue des pirates informatiques, il s'agit d'anonymiser ou d'obfusquer au maximum toutes les traces ou informations pouvant être liées à son identité ou ses activités.
- **Capacité de recherches** (n=3 ; 18%) : Une bonne capacité de recherche peut s'avérer importante pour certains pirates informatiques. En effet, pour ceux qui ont mentionné cette compétence, elle leur permettait de retrouver des solutions à des défis qui ont

déjà été surmontés par d'autres, plus rapidement et efficacement que de tenter de les résoudre par soi-même. Elle permet également de trouver de la documentation en lien avec des organisations, des technologies ou des systèmes qu'ils ont dans leur mire.

- **Enthousiasme** (n=3 ; 18%) : L'enthousiasme, parfois même la passion pour l'informatique, a été mentionné par quelques participants, qui considèrent qu'il s'agit, tout comme la curiosité, d'un élément inhérent au fait d'être un pirate informatique et de toujours vouloir en apprendre davantage au sujet des technologies.
- **Pensée logique ou critique** (n=2 ; 12%) : Deux participants ont indiqué que pour eux, le fait d'adopter une pensée « logique » et la capacité d'avoir un esprit « critique » est ce qui leur a permis d'être un pirate informatique ayant du succès, surtout lorsqu'il s'agit de reconnaître les possibilités d'exploitation ou de couvrir ses traces.
- **Discipline** (n=1 ; 6%) **et Humilité** (n=1 ; 6%) : Finalement, la discipline et l'humilité ont chacune été mentionnées par un participant puisqu'elle la discipline lui permettait de demeurer systémique, tant dans ses processus d'apprentissage, que ceux impliqués dans sa sécurité opérationnelle, et que l'humilité jouait un rôle important dans le fait dans ne pas se faire prendre par les autorités.

6.2 Rôle et influence des pairs dans l'apprentissage

Les participants ont aussi dû répondre à une question quant à savoir s'ils considèrent avoir eu des personnes dans leur entourage qui ont joué un rôle dans leur initiation ou leur apprentissage du piratage informatique, et si ces personnes faisaient partie de leur entourage dans la vraie vie ou s'il s'agissait de personnes rencontrées en ligne.

Tous les 17 participants (100%) ont indiqué que des pairs en ligne ont joué un rôle dans leur apprentissage ou initiation dans le monde des pirates informatiques, contre seulement 7 participants (41%) qui ont aussi souligné l'influence de personnes qui faisaient partie de leur vie dans le monde réel.

6.2.1 Les pairs dans le monde réel

Un nombre minoritaire de participants ont affirmé avoir eu des personnes dans leur entourage de la vie réelle, qui ont joué un rôle dans leur apprentissage (n= 7 ; 41% des participants).

Certains (n=3) ont affirmé avoir eu de l'influence familiale, et même l'opportunité d'être initié à l'informatique à un jeune âge grâce à un parent.

> "[...] but I did get my interest in computers from my dad, it's thanks to him that I started with computers at a young age. [...] Well, he is very tech savvy and always let me experiment with the computer, which created a very good environment to experiment."
>
> – Participant ID #2056

D'autres (n=2) ont eu la chance de rencontrer un ami, qui les a initiés à la programmation ou qui avait des connaissances de base en réseautique, à travers des connaissances en communs.

> "Yes, he basically gave me a push, just recommended it to me [...] my only friend with basic knowledge of it all [...] it was vague, more of a 'yeah we know each other', held normal conversations, and didn't bring up any of it due to being an unnecessary risk factor [but] it was nice knowing you had someone you could share your ideas, etc, with."
>
> – Participant ID #2063

Pour 3 participants, leur parcours académique ou professionnel dans un domaine connexe à l'informatique leur a permis de rencontrer des individus avec des centres d'intérêt similaires.

> "Yes! I met some cool people in school and some conferences."
>
> – Participant ID #2030
>
> "My family, the people I encountered in [redacted – work related] and in my first job out of uni [university] have been pivotal."
>
> – Participant ID #2072
>
> "With how I attend conferences and other networking events, I would NOT be shocked if I have met a few people I have brushed shoulders with online and not even known it."
>
> – Participant ID #2001

Finalement, quelques participants ont insisté sur le fait de maintenir leurs activités et leur vie virtuelle, séparés de leur vie dans le monde réel, principalement pour des raisons de sécurité opérationnelle, tel que l'illustrent les citations ci-dessous :

> "I am mistrusting to meet people in real life, I try not to link my virtual friendships in my personal life"
>
> – Participant ID #2011
>
> "Not really [...] I also keep that illegal stuff away from my personal life"
>
> – Participant ID #2045

6.2.2 Les pairs dans le monde virtuel

Puisque tous les participants ont été recrutés dans des communautés en ligne, il n'a pas été surprenant de constater qu'ils ont tous mentionné avoir des pairs dans le monde virtuel (n=17 ; 100%), qui ont joué un rôle, à des niveaux variables, dans leur évolution et leur réussite en tant que pirate informatique.

Pour la plupart (n=10 ; 58,8%), l'impact qu'ont eu les pairs rencontrés dans le monde virtuel a été très concret, et a pu prendre différentes formes. Pour certains, il a d'abord été une question de rechercher des pairs qui avaient les mêmes intérêts envers la technologie, que ce soit pour socialiser et avoir des discussions stimulantes, ou comme certains ont mentionnés, simplement pour avoir des « contacts » et réseauter dans une communauté ayant les mêmes affinités.

Pour plusieurs (n=7), ces échanges leur ont permis d'étendre leurs connaissances et élargir leurs horizons, d'obtenir des opportunités leur permettant d'affiner leurs compétences, et même de se mesurer à d'autres et mettre en perspective leurs capacités.

> "Yes. In fact, I think you will find a lot of this on [redacted: name of forum]. People coming for one reason and deciding to stay to improve on their skills, or maybe even foster a skillset they have yet to realize they are geared toward."
>
> – Participant ID #2001
>
> "I think chatting and being involved with people of various levels of experience, some less knowledgeable, some the same level as me, some

> way ahead of me, it really helped to have a view of where I was, concerning my skills and abilities, so I wouldn't get ahead of myself and think I'm hot shit or something [...]."
>
> – Participant ID #2074

Parmi ces participants, certains (n=3) ont souligné l'importance de faire partie d'une communauté dans leur apprentissage, car cela leur a apporté de l'inspiration et des encouragements pour persévérer leur apprentissage dans cette voie, malgré les difficultés.

> "Well, they pushed me to learn more, they gave me inspiration and ideas. I learned a lot because of them, and I am sure the feeling is mutual [...]. They pushed me to become better and I did the same for them. Even a conversation about Command Injection assisted me in remembering what I learned about it and allowed it to stick in my brain."
>
> - Participant ID #2033

Il a également été intéressant d'avoir des participants (n=2) indiquer clairement que ces associations virtuelles leur ont permis d'apprendre d'autres pirates informatiques qui se sont fait prendre, et qui partagent leurs erreurs avec les autres, ainsi que comment éviter les écueils.

> "Well, a great example of that would be how I didn't know all the best practices in operational security and I wouldn't know them if it wasn't for members of the [redacted: forum name] community who have either been caught by authorities and provided me with insight into their mistakes and how to avoid them, and talking to members who have not been caught and why they haven't been caught."
>
> – Participant ID #2074
>
> "[...] On forums we saw ppl [people] getting caught, so we learned from their mistakes."
>
> – Participant ID #2052

Bien sûr, les communautés en ligne s'entraident à résoudre des défis et trouver des réponses à des questions situées dans différents champs d'expertises de l'informatique.

> “Also, it's not like I know all there is to know now, if I have a challenging problem, I will go to my favorite hacking forum and discuss it with the members there.”
>
> – Participant ID #2062

Cependant, l’essentiel de ces communautés servirait surtout à donner des indices sur les chemins à emprunter et les différentes possibilités qui sont à portée de la main, plutôt qu’un lieu où l’apprentissage s’effectuerait en tant que tel. Certains (n=4) ont même fait référence à une philosophie d’apprendre par soi-même, et que le principal de l’apprentissage s’effectue, de toute façon, majoritairement par le biais d’essais et erreurs.

> “Learn different things, see what other people do, try what they do, change it up a bit, see what works. It's just trial and error in my opinion.”
>
> - Participant ID #2026

Un autre élément intéressant a également été relevé par différents participants (n=6). Il subsisterait au sein des communautés, malgré tout, une certaine méfiance, ou parfois un esprit de compétition, qui limiterait le partage des connaissances tous azimuts et de façon publique. Oui, les différents membres se retrouvent en communauté pour rencontrer des pairs, socialiser et se bâtir une certaine réputation, mais les échanges de méthodes et techniques s’effectueraient surtout au sein de cercles restreints et d’amitiés formées sur ces forums. Ceux-ci migrent ensuite vers des plateformes de messageries privées pour réellement effectuer leurs échanges.

> “However, if you develop online friendships, they are more inclined to share. So, you would become friendly with someone, or a group, then PM [private message] them your jabber for example and discuss from there. People are more inclined to share on an individual basis. Not everybody thinks, wow let's just post everything on the fucking internet.”
>
> – Participant ID #2079
>
> “Maybe small groups up to 5 in [redacted] chats where we discussed hacking and opsec [...] but not necessarily for the reason of it being a secret or something that has to be kept hush hush. It's more often than not due to the more seasoned members only talking about these kinds of things to people who have proven their worth and that they aren't just talking out of

> their ass to look cool on the internet. We like to keep to like-minded people who share our knowledge and views."
>
> – Participant ID #2074

Par ailleurs, dans l'échantillon collecté, il semble y avoir eu 5 participants qui étaient davantage orientés vers l'aspect des « affaires » et gagnaient leur vie avec leurs activités en ligne. Ils ont pu fournir une perspective un peu différente du rôle que jouent ces communautés dans leur évolution en tant que pirate informatique. En effet, pour ces derniers, il a rarement été question de socialiser et former des amitiés au sein des communautés en ligne, mais surtout de trouver, soit des pairs avec qui s'associer, soit trouver des clients potentiels parmi les usagers, pour leurs services ou les bases de données qu'ils vendent. Ce type de membre est également peu enclin à partager ses connaissances avec d'autres, à moins qu'il s'agisse d'un échange de service, et demeure très méfiant à l'égard des autres.

Ces trois citations ont été sélectionnées parmi d'autres pour illustrer ces propos :

> "Yeah, but what you have to understand is that there are trust issues during criminality. You can't get close to a lot of people, because you are criminal and they are a criminal, do you see the inference? [...] I used to deal with a lot of people on a daily basis. It's bad to call them friends, they were associates. They were criminals."
>
> – Participant ID #2079
>
> "To be successful in the hacking community though, you need to be good at exploiting people, stealing from them, being better than others, to be on top. Send adversaries to prison. Steal their data. Manipulate them. Spread lies about them, defame them, make them unwanted so they have to create a new identity and start over with zero reputation. It's all competitive, not a friendly place."
>
> – Participant ID #2026
>
> "Actually, I don't want to share my knowledge. [...] I know people from forum. Then I contact them from "their contact method". I only have strong relationships with those people who knows stuff."
>
> – Participant ID #2045

L’analyse des résultats au sujet du rôle et de l’influence des pairs nous amène donc à comprendre que, de côtoyer des pairs ayant les mêmes centres d’intérêt, tournant autour de la technologie, ses applications ainsi que ses vulnérabilités et ses possibles avenues d’exploitation, permet d’élargir ses connaissances en discutant de ce qui est possible. Puisque les différents domaines de l'Internet requièrent des connaissances et des compétences différentes, il n’est pas possible d’en maîtriser tous les aspects et que lorsqu’on débute à s’intéresser à un nouvel aspect, il y aura toujours quelqu’un d’autre qui aura déjà maîtrisé cet aspect avant nous et de qui on peut apprendre. Ils peuvent discuter de ce qui est possible de réaliser, ce qui ne l’est pas, se faire suggérer des avenues qu’ils n’auraient peut-être pas envisagées, en apprendre sur des sujets qui peuvent s’avérer utile un jour, et développer des connaissances en informatiques qui sont pragmatiques de façon générale.

En dehors des connaissances qu’ils peuvent mutuellement s’apporter, les participants ont mentionné l’importance d’obtenir de la rétroaction de la part de leurs pairs, de partager des outils, s’encourager mutuellement à devenir meilleurs et se garder à jour des dernières nouvelles et techniques. Par ailleurs, d’entendre certains individus partager leurs exploits avec les autres peut les pousser à vouloir mesurer leurs propres capacités et compétences en essayant de reproduire ces exploits, dans un élan de vouloir se prouver à eux-mêmes et aux autres.

Les membres de ces communautés qui rencontrent d’autres membres qui sont doués ou avec qui ils ont des affinités finissent par former des cliques ou des groupes, et vont migrer leurs échanges sur des plateformes de messageries privées, à l’extérieur du cadre du forum. Aussi, parfois, les connaissances au sein d’un groupe d’amis particulier peuvent atteindre une certaine limite, et c’est là qu’appartenir à une communauté en ligne peut devenir intéressant. Par contre, il est également important d’apprendre et développer des méthodes uniques par soi-même, qui ne sont pas déjà partagées partout sur les forums et qui n’auront pas été utilisées à outrance par d’autres pirates informatiques.

6.2.3 Mention d’un mentor

À la question quant à savoir si les participants ont pu bénéficier de la présence d’un mentor quelconque au cours de leur parcours d’apprentissage, 7 participants sur les 13 qui ont

répondu à cette question, ont mentionné avoir eu un au moins une personne ayant joué un rôle similaire dans leur vie. Ils les ont inspirés et guidés, les ont encouragés à aller plus loin dans leurs apprentissages, les ont aidés à trouver des solutions, et les ont amenés à un niveau supérieur dans leur compétence en leur montrant ce qui était possible.

Il est à noter que dans le cas de 4 entretiens sur un total de 17, la question n'a pas pu être posée, pour différentes raisons, ou elle n'a pas été répondue.

> "Sure, I do have someone I called him "Sensei" [...] a cybersec instructor who is doing trainings to faculties, companies, armies and he is well experienced, always giving me things to learn and improve myself to better, every time I felt weak and can't handle anything, I contact him. He will give me all the recourses that I need. I [was] always inspired by him."
>
> – Participant ID #2090

Parfois, il s'agissait surtout d'une influence indirecte :

> "Yes, there are many people I admired. I saw them as these sort of mythical figures... how was it possible for them to be so smart? How can they do it? It seemed impossible. Now, I am as skilled as them, even more skilled than some."
>
> - Participant ID #2026

Sur les 13 participants ayant répondu à cette question, 6 ont affirmé ne jamais vraiment avoir eu de mentor pour les assister dans leur cheminement.

> "Nah not really like that, just being part of the community kinda did the trick for me."
>
> – Participant ID #2086
>
> "Maybe some are lucky enough to have their "hacking sensei" but most often nada."
>
> – Participant ID #2001

6.3 Rôle de l'imitation dans l'apprentissage

La dernière thématique à avoir été abordée avec les participants a été se savoir si l'imitation avait joué un rôle dans leur apprentissage. Malheureusement, 6 participants, sur le total de 17, n'ont pas répondu à la question, pour diverses raisons (entretiens qui se sont terminés avant d'aborder le thème ou question contournée, par exemple). Sur les 11 participants qui ont répondu à cette question, la presque totalité (n=10) a admis que l'imitation représente un bon moyen de démarrer l'apprentissage et comprendre certains outils ou processus, surtout dans les débuts.

> "Well I suppose it's a bit like: someone invents a method, shares it, then other people copy. Really, you want to be the person inventing the method, not copying, but sure, it can be useful. I suppose that's how I learned."
>
> – Participant ID #2079
>
> "For me, hacking is a science and replicating some stuff could help you to understand how something works."
>
> – Participant ID #2030
>
> "I think it takes a huge place in learning. [It] can differ from person to person but it does make things easier. [Your] goals [are] out of what is trendy, or out of the general scope, then will be different, but yeh [and] u can see in forums, [people] mostly imitate. People who are in search of results would keep doing that as much as possible [and] they might learn during that process."
>
> – Participant ID #2052

En effet, la plupart s'entendent pour dire qu'il s'agit d'un bon moyen d'apprendre dans les débuts, mais plusieurs participants (n=6) ont tenu à y apporter quelques nuances, comme en témoigne la citation suivante :

> "You can't simply completely imitate what other people are doing, unless it's just you, learning from your friend, so you're the only ones doing it. Because if you just do something that everyone else knows how to do, it's pointless, useless. Sure, it helps you understand some things better, but it only helps for learning. At some point, you need to try doing things on your own, not copying from others. You're using some script from GitHub? Delete it, make your own better version, then, think of how you could copy it for other uses, so you can do something unique. Sure, imitation can work for learning, but in terms of being practical, you need to be unique."
>
> - Participant ID #2026

Quelques exemples d'apprentissage à travers l'imitation ont été relevés dans les entretiens, notamment lorsqu'il est question de créer un outil/script personnalisé. Les participants ont souvent eu recours à des scripts préexistants, trouvés via un moteur de recherche ou sur des forums spécialisés, en en trouvant un qui corresponde à peu près à ce que le pirate informatique recherchait et en le modifiant pour l'adapter, ou en combinant plusieurs scripts ensemble pour arriver à un résultat désiré. À force d'en faire, une certaine maîtrise se développe et peut être réappliquée pour d'autres situations. Évidemment, tel qu'il a été mentionné précédemment, pour réellement devenir compétent, il faut vraiment apprendre à maîtriser au moins un langage et créer ses propres outils.

6.4 Acquisition

Jeux vidéo

Bien que le thème de l'influence des jeux vidéo ne figurait pas parmi mes sous-objectifs de recherche, il s'est imposé de lui-même dans les entretiens qui ont été effectués. En effet, 7 participants sur les 17 (41%) ont mentionné les jeux vidéo en parlant du processus qui les a amenés à s'intéresser au piratage, à leurs tous débuts.

La plupart des témoignages racontent comment le fait de jouer à des jeux vidéo compétitifs avec d'autres joueurs en ligne les a amenés à vouloir rechercher un avantage déloyal sur les autres joueurs. Pour certains, cela est passé par le fait d'apprendre à programmer pour modifier certains éléments du jeu, pour d'autres, une démarche qui a les mené à trouver exploiter des défauts de conceptions (*bug*) ou vulnérabilités dans le programme du jeu, ou même trouver des façons de profiter du système de devises (monnaie du jeu) pour s'offrir des objets ou de l'équipement octroyant un certain avantage au personnage du jeu.

Dans un cas, le participant relate qu'il téléchargeait des jeux piratés et avait été fasciné par la façon de s'y prendre, alors il s'est mis à se renseigner sur la façon de contourner les mécanismes de gestion des droits numériques (*digital rights management,* ou *DRM labels*) mis en place par les fabricants de jeux vidéo.

En effectuant leurs recherches, de fil en aiguille, les participants seraient tombés sur des forums de discussion où les discussions ne tournaient pas uniquement autour des jeux vidéo.

C’est ainsi qu’ils se seraient familiarisés avec des concepts utilisés en piratage informatique et à plusieurs autres sujets convergents.

> “Jess, it's a very complicated thing to answer. When I was about 13 years ago, I use to play MMO's and thought to myself one day, wow I wonder if there's an easy way to cheat on this game. I started doing various searches and found forums. Created a profile, spent months lurking and looking at how other people cheated. I saw other discussions taking place, relating to website development, got curious, fucked around with website development for a bit [...].”
>
> – Participant ID #2079

Sinon, il semble y avoir un consensus à l’effet qu’il n’existe pas de chemin tout tracé pour apprendre à devenir un pirate informatique. Il s’agit surtout de processus itératifs, au cours duquel plusieurs aptitudes et connaissances, provenant de domaines variés, finissent par s’entrecroiser et coconstruire un tout cohérent, et le pirate informatique passionné le devient parfois un peu par « accident ».

Les novices peuvent commencer par ce qu’ils veulent avoir l’air « cool » et être respectés parmi les autres membres, mais une fois cette phase se termine et si l’intérêt et la curiosité envers l’informatique demeure, vient un moment où le pirate se rend compte qu’il a concrètement développé des compétences pratiques pour le piratage. Mais ces connaissances et compétences se développent graduellement au fil du temps, et en côtoyant des pairs qui ont les mêmes centres d’intérêt et en échangeant avec ces derniers. SI un individu est passionné et persévérant, cela le poussera toujours à rechercher des réponses à ses questions, à comprendre comment les ordinateurs fonctionnent et communiquent. Il aura soif d’en apprendre davantage plus à propos de domaines connexes et repousser les limites.

Un autre thème à avoir été souvent mentionné est le fait que l’apprentissage s’effectue inévitablement en expérimentant, à coup d’essais et erreurs, en passant énormément de temps sur un ordinateur. Un individu curieux ira se renseigner sur un sujet, et cherchera simplement à appliquer ses connaissances. Il tentera donc par divers moyens d’en tester les différentes applications. Beaucoup de recherches, de lectures et de pratiques sont impliquées dans l’apprentissage du piratage informatique. De plus, il semblerait qu’il s’agit d’un

apprentissage solitaire, même s'il est utile de discuter avec des pairs, partager des points de vue et des astuces, ne seraient-ce que pour mieux ancrer leurs connaissances en mémoire.

Chapitre 7 – Discussion & intégration

En premier lieu, à la lumière des entretiens réalisés et des résultats obtenus, il est possible d'affirmer que la théorie de l'apprentissage social, telle qu'élaborée par Akers, a constitué un cadre théorique solide pour l'opérationnalisation des questions de recherche. Il est apparu de manière évidente que les composantes de l'apprentissage social, telles que l'association différentielle, l'intégration de définitions favorables, le renforcement différentiel, ainsi que l'imitation, sont tous des éléments qui ont été mentionnés, à divers degrés d'importance, par les participants lorsque questionnés au sujet de leur processus d'acquisition de compétences et au sujet des facteurs auxquelles ils attribuent leur réussite en tant que pirates informatiques. Cela confirme ce que d'autres études similaires ont rapporté dans leurs études (Décary-Hétu, 2013a; Higgins et al., 2007; Higgins & Makin, 2004; Higgins & Wilson, 2006; Hinduja & Ingram, 2009; Holt et al., 2010, 2012; Holt & Copes, 2010; Marcum et al., 2014; Montégiani, 2017; Morris & Higgins, 2010; M. K. Rogers, 2001; Skinner & Fream, 1997).

En revanche, la limite qui subsistait dans la littérature actuelle concernant l'apprentissage social des pirates informatiques est qu'aucune étude ne s'est basée sur des entretiens effectués avec des pirates informatiques toujours actifs et qui s'introduisent dans des systèmes informatisés de façon non autorisée. Tous les chercheurs qui se sont intéressés de proche ou de loin à la cyberdéviance sous la lunette de l'apprentissage social ont, soit étudié le phénomène du téléchargement illégal chez des étudiants, soit analysé des questionnaires auto-rapportés, des publications de forums ou des canaux de clavardages. Ce que les entretiens directs avec les pirates informatiques a permis de faire ressortir est la différence fondamentale de parcours, de perception et de processus d'apprentissage chez les pirates informatiques qui se servent du piratage comme moyen de faire de l'argent, et ceux qui piratent comme une fin « en soi ».

Les entretiens ont en effet permis de constater que le rôle des communautés en ligne, du mentorat et de l'imitation sont perçus et vécus de manière radicalement différente chez les pirates motivés par le gain financier. Ces derniers semblent se servir des communautés de

manière accessoire, soit pour se trouver des associés compétents pour mener leurs activités à bien, ou trouver des clients potentiels auprès de pirates à la recherche de services ou de bases de données en particulier. Dupont et al. (2016) avaient également relevé que les *hackers* malveillants profitaient de la division du travail entre différents associés aux compétences avancées. Il semble aussi y avoir davantage de mentorat et d'imitation chez ce type de pirates informatiques, moins préoccupés par le principe « d'apprendre par soi-même » et moins intéressés à « perdre du temps » à maîtriser des compétences secondaires, pour lesquelles ils peuvent simplement embaucher un autre pirate compétent pour faire la besogne.

Il avait déjà été relevé dans la littérature que les pirates motivés par le profit financier, tels que le délinquant adaptatif et le pirate criminel professionnel, possèdent des niveaux d'habiletés techniques modérés à élevés, et qu'ils ont tendance à se spécialiser davantage vers les compétences qu'ils considèrent spécifiques à leur activité criminelle (S. Hald & Pedersen, 2012; M. Rogers, 1999; M. K. Rogers, 2006). De plus, ces pirates n'auraient pas forcément d'intérêt généralisé envers la technologie outre que ce qu'elle peut leur rapporter. Il serait donc raisonnable d'avancer que leur processus d'apprentissage soit différent des autres types de pirates informatiques.

Évidemment, avec un échantillon restreint à n=17, il est difficile d'en tirer une conclusion en tant que telle. Bien que la littérature ait créé des typologies de pirates informatiques selon leurs motivations, aucune de s'est questionnée à savoir si la motivation exerçait une influence sur le parcours d'apprentissage, ou inversement, et de prendre ces différents éléments en compte dans l'étude de ces concepts. Les résultats de cette étude suggèrent qu'il s'agirait d'une avenue de recherche prometteuse à explorer.

En guise de question d'ouverture, les participants ont dû révéler les compétences qu'ils considéraient qu'elles avaient joué un rôle dans leur réussite tant que pirate informatique, et comment ils les avaient acquises. L'analyse thématique du contenu de ces entretiens a démontré que des connaissances de base en informatique et en réseautique (cités par 12 participants sur 17) et une compréhension d'un langage de programmation (cité par 11 participants sur 17) étaient considérées comme cruciales. La troisième compétence la plus importante est le fait d'avoir des aptitudes sociales et en ingénierie sociale (cités par 9 participants sur 17). En effet, bien que la plupart des compétences mentionnées puissent

davantage être considérées comme des aptitudes personnelles, les compétences techniques de base se retrouvent tout de même en tête des compétences primordiales à maîtriser.

Les sous-objectifs de cette étude visaient justement à comprendre l'importance des pairs, dans le monde réel et virtuel, ainsi que le rôle de l'imitation dans l'acquisition de ces compétences.

7.1 Rôle et influence des pairs

La littérature décrit abondamment la pertinence de la théorie de l'apprentissage social pour étudier le phénomène de criminalité informatique (Boman & Freng, 2017; Morris & Higgins, 2010; Steinmetz & Nobles, 2018), dont celui du principe de l'association différentielle en lien avec la cybercriminalité (Décary-Hétu, 2013a; Higgins & Wilson, 2006; Holt et al., 2010; Marcum et al., 2014) (Holt and Bossler, 2014).

De plus, l'étude de Baillargeon-Audet (2010), de Montégiani (2017) et de Zhang et al. (2019), ont démontrés que les communautés de *hackers* représentaient des communautés d'apprentissage, où la méritocratie règne. Les résultats de la présente étude vont dans le même sens, sachant que 100% des participants ont mentionné le fait que les pairs rencontrés au sein de communautés en ligne avaient joué un rôle dans leur processus d'apprentissage. Pour plusieurs, les échanges ont permis d'étendre leurs connaissances, trouver réponse à leurs questions et élargir leurs horizons, mais également pour y trouver de l'inspiration et des encouragements de la part d'autres membres, face à une courbe d'apprentissage qui peut parfois être rude à surmonter. D'autres ont même mentionné y avoir appris des erreurs commises par d'autres membres qui s'étaient fait prendre par les autorités. Cela correspond aux conclusions auxquelles étaient arrivés Holt et Copes (2010), qui ont passé en entrevue 34 individus qui s'adonnaient au téléchargement illégal. Ils ont trouvé que la participation à des forums en ligne et les interactions avec d'autres membres avaient permis aux pirates d'améliorer leurs compétences.

Par contre, il ne faudrait pas croire pour autant que ces plateformes servent à partager des connaissances tous azimuts, à n'importe quel membre inscrit. Ce qui est partagé et accessible de façon publique ne représente que la pointe de l'iceberg en ce qui a trait aux interactions d'apprentissage et d'échange de connaissances. Plus souvent qu'autrement, les membres y forment des cliques et des amitiés en cercles restreints, où ils discuteront en privés de

méthodes et de sécurité opérationnelle. Ainsi, les connaissances intéressantes sont partagées en privé, parmi des individus ayant certaines affinités et ayant surtout démontré leur valeur ou leur utilité au sein d'une communauté. Cela confirme certaines conclusions de l'étude intitulée « Information exchange paths in IRC hacking chatrooms », menée par Décary-Hétu (2013a), à l'effet que les pirates informatiques ont tendance à se rassembler et former des groupes restreints et intimes pour échanger.

Ces résultats viennent donc limiter la portée des études sur l'apprentissage social des pirates informatiques, qui sont strictement basées sur des analyses de publication publiques, partagées sur des forums publics.

De plus, bien que la totalité des participants ait discuté de l'influence significative des pairs rencontrés dans les communautés virtuelles dans leur apprentissage, certains ont tout de même tenu à rappeler l'importance et le respect que les pirates informatiques accordent au principe d'apprendre et se développer « par soi-même ».

Dans le cadre de cette entrevue, seulement 7 participants (41%) ont indiqué avoir subi une influence quelconque de pairs provenant du monde réel dans leur apprentissage. Parmi ceux-ci, une minorité avait été initiée à la technologie à un jeune âge par un parent, mais les autres ont surtout côtoyé des pairs dans le monde réel parce qu'ils ont eu l'opportunité d'en rencontrer durant leur parcours académique ou professionnel, lié à l'informatique. En revanche, chez les participants qui étaient motivés par le gain financier, il était très clair qu'ils ne mêlaient pas leurs activités en ligne à leur vie personnelle.

Ces résultats contredisent légèrement ceux recensés dans la littérature. En effet, les personnes interrogées par Holt et Copes (2010) ont indiqué ne pas uniquement s'identifier comme étant des « pirates informatiques », et maintenaient des liens étroits avec d'autres groupes d'amis du monde réel. Hinduja et Ingram (2009) ont également étudié l'influence des pairs en ligne et hors ligne et leurs résultats ont démontré que les étudiants qui étaient associés à d'autres personnes dans la vie réelle, qui soutenaient ce type d'activité, avaient des scores de piratage plus élevés. Par contre, il semble important de spécifier que ces deux études se sont penchées sur le sujet du téléchargement de contenu numérique illégal. Des conclusions divergentes peuvent s'expliquer par le fait que le téléchargement illégal est un type de criminalité banalisé par les jeunes (Navarro & Marcum, 2019a).

Par ailleurs, plusieurs auteurs ont souligné le manque de littérature en lien avec l'influence des pairs « terrestres » et ceux en ligne pour expliquer l'engagement dans la cybercriminalité (Boman & Freng, 2017; Navarro & Marcum, 2019b; Steinmetz & Nobles, 2018). Il pourrait d'agir d'une autre voie à explorer pour mieux cerner le phénomène propre aux pirates informatiques qui s'introduisent dans des systèmes de façon non autorisée.

À ce sujet, Holt et Copes (2010) ont fait remarquer un point intéressant dans leur étude, par rapport au fait qu'il existe une certaine facilité d'interaction dans les communautés en ligne, de manière générale, en comparaison avec les interactions en face à face. Ces participations à des communautés en ligne, ne nécessitant qu'un engagement minimal de la part d'un individu, permettent la transmission de comportements déviants vers des individus qui ne sont pas nécessairement engagés dans une trajectoire criminelle. Autrement dit, des groupes déviants créent des communautés en ligne, où la participation à des comportements déviants peut s'étendre à des populations qui ne sont pas forcément criminelles. Cette réalité a pu être observée par la chercheuse au sein des plateformes étudiées. Par conséquent, de futures études menées au sein de communautés de pirates informatiques, qui ne font pas la distinction entre ceux deux types d'individus, ne permettront pas d'identifier les caractéristiques uniques et propres aux pirates informatiques réellement criminalisés.

En ce qui concerne la présence de mentors, 7 participants sur le 13 ayant répondu à cette question (53%) ont affirmé avoir pu bénéficier d'une telle influence durant leurs parcours. Ceux-ci les ont aidés à naviguer dans le vaste univers des connaissances liées à l'informatique et la réseautique, trouver des pistes de solutions lorsque confrontés à des obstacles, ou même concernant la sécurité opérationnelle. De manière plus abstraite, certains ont mentionné que ces mentors ont servi de modèle, les ont inspirés, stimulés et encouragés à persévérer dans leur apprentissage, et sans cesse repoussé les limites de leurs compétences. À la question quant à savoir s'ils seraient devenus des pirates informatiques si ces mentors n'avaient pas croisé leur chemin, ils sont unanimes : oui, la passion était déjà présente. Cependant, ils reconnaissent qu'ils ne se seraient pas rendus aussi loin dans leurs acquis sans ce coup de pouce.

Certains auteurs ont mentionné l'importance du mentorat dans les communautés de pirates (Rogers, 2001), aussi baptisés « hacker gurus » dans l'étude de Zhang et al. (2017), où des usagers plus expérimentés partagent leurs connaissances, leurs techniques, leurs

perspectives et leurs définitions, avec les pirates informatiques novices. De plus, les analyses de réseaux de pirates informatiques effectués par Décary-Hétu (2013a) et ceux de Montégiani (2010), qui ont respectivement analysé des canaux de clavardage et des publications publiques d'un forum, pointent vers l'existence de groupes restreints, favorables à l'apparition de mentors et d'apprentis.

Cependant, pour les 6 autres participants dans l'échantillon, ceux-ci affirment ne pas avoir eu la chance d'avoir un mentor à leur portée pour les aider à évoluer, et que de faire partie d'une communauté leur a suffi. Des recherches supplémentaires sont nécessaires pour approfondir le contexte qui amène ces groupes à se former.

7.2 Rôle de l'imitation

Peu d'études se sont concentrées sur le rôle de l'imitation dans la perpétration de cybercrimes, mais ceux qui y sont intéressés ont souligné l'importance de l'imitation dans le processus d'apprentissage social, insistant sur la nécessité de prendre cet aspect en compte dans les études liés aux crimes informatiques (Holt et al., 2010; Navarro & Marcum, 2019b; Sharma, 2007; Skinner & Fream, 1997).

Dans le cadre de cette étude, il subsiste une certaine limite quant aux résultats liés à cette question puisque seulement 11 participants sur les 17 y ont répondu, mais la presque totalité a admis que l'imitation représente un bon moyen de démarrer l'apprentissage et comprendre certains outils ou processus, surtout dans les débuts.

En effet, bien qu'ils étaient presque tous prêts à reconnaître qu'au niveau des méthodes et la réplication des outils d'autres pirates informatiques était un peu inévitable dans les débuts de l'apprentissage, plusieurs ont insisté sur le fait que développer des techniques et des outils uniques jouait un rôle clé dans la réussite et l'évasion de détection à des niveaux plus avancés.

Ces résultats sont consistants avec les travaux de Skinner et Fream (1997), qui ont observé un plus haut taux de prévalence chez les individus qui fréquentaient des babillards électroniques dédiés au piratage informatique. L'étude de Holt et al. (2010), a également fait ressortir que l'imitation jouait un rôle essentiel dans le processus d'apprentissage.

Cela peut s'expliquer par la nécessité de maîtriser des compétences techniques suffisantes pour mener à bien des opérations de piratage informatique, des habiletés qui ne sont pas, de

prime abord, accessibles pour tous. L'imitation s'impose donc comme une façon de faire et d'apprendre de manière rapide et efficiente.

Fait important à noter, il a été observé une certaine perception ou connotation négative de l'imitation dans la sous-culture des pirates informatiques. Cette pratique est associée aux pirates novices (*script kiddies*, ou *skid*). Il pourrait donc s'avérer judicieux pour de futures études qui souhaitent observer cette composante de sélectionner un certain vocabulaire ou une approche qui ne heurte pas leur sensibilité à ce niveau, pour éviter d'obtenir des données faussées.

7.3 Intégration criminalistique

Lorsqu'il est question d'étudier un type de criminalité aussi complexe et évolutif que la criminalité informatique, une approche multidisciplinaire, comme la traçologie, serait à privilégier (Bécue & Décary-Hétu, 2016). La traçologie est définie comme étant la combinaison de la criminologie et de la criminalistique, articulée autour de l'étude des traces. La trace forensique est généralement une marque, un signe ou un objet apparent, ou invisible à l'œil nu, qui est le vestige d'une présence et/ou d'une action à l'endroit de cette dernière, et résulte donc d'une activité (Margot, 2014).

Dans le contexte qui nous intéresse, il serait question de traces numériques, ou de manière plus spécifique, de traces internétiques (laissées sur Web et accessibles via Internet) (Rossy & Décary-Hétu, 2017). Dans leur article, Bécue et Décary-Hétu (2016) argumentent que les traces liées aux activités criminelles peuvent désormais être trouvées en ligne, notamment dans les marchés illicites, les canaux de clavardage et les forums de discussion.

L'analyse des discussions, en tant que traces internétiques, permettrait de mieux comprendre la psychologie, les comportements et les processus des délinquants (Bécue & Décary-Hétu, 2016). Par contre, il est essentiel de souligner que l'analyse seule des traces pour comprendre un phénomène criminel comporte des limites, puisque les traces seules ne fournissent pas toujours à l'analyste le contexte nécessaire à leur interprétation (Rossy & Décary-Hétu, 2017). Par conséquent, bien que l'analyse des discussions en ligne puisse nous en apprendre sur certains aspects de la criminalité informatique, de pouvoir les coupler ces données à des données d'entrevues, permettraient d'obtenir une compréhension globale du phénomène étudié.

En ce qui concerne la présente étude, une approche qui aurait été novatrice et qui aurait permis d'observer de manière concrète la façon dont s'effectue l'imitation entre pirates informatiques, ainsi que son ampleur, aurait été d'adopter l'approche de traçologique, c'est-à-dire en combinant des données criminologiques qualitatives à des données de criminalistiques informatiques. Autrement dit, en comparant des données d'entrevue, à des techniques d'attaques répertoriées par des analystes en sécurité informatique, ou comparer la composition d'outils ou de scripts similaires disponibles en ligne. Malheureusement, il s'agit d'un projet de recherche un peu trop ambition dans le cadre d'un travail de maîtrise.

7.4 Limites de l'étude

Les données de cette étude ont produit des résultats intéressants, mais il est important de prendre en compte les limites méthodologiques suivantes, principalement liées à l'échantillon ainsi qu'à la méthode de collecte.

En effet, il peut être argumenté qu'un « n » de dix-sept entretiens représente un échantillon plus ou moins restreint. De plus, il est important de noter que les participants d'un des forums sont surreprésentés dans l'échantillon. Le fait qu'il s'agisse d'un échantillon principalement composé de volontaires est réellement ce qui pourrait affecter sa représentativité. Certains auteurs invoquent le fait que les volontaires partagent généralement des caractéristiques psychologiques particulières, comme la volonté de plaire, le désir de connaître, besoin de régler des problèmes, etc. et que par conséquent, toute généralisation des résultats devient hasardeuse (Gauthier, 2010). Cependant, compte tenu de la nature sensible du sujet à l'étude, il est fréquent d'utiliser un échantillon composé de volontaires puisque l'objet d'étude rend difficile la sélection et l'interrogation d'individus sur des thèmes considérés comme étant délicats, et de leur imposer une expérimentation potentiellement embarrassante, voire dangereuse pour leur sécurité (Gauthier, 2010).

Le dernier élément à potentiellement affecter la validité externe de l'étude est le biais de désirabilité social, qui est incontournable avec une méthode de collecte telle que les entrevues. En effet, il appert que lorsque les participants se savent observés, ils recherchent naturellement à adopter un comportement ou un discours qu'ils s'imaginent recherché par l'intervieweur (Gauthier, 2010). Pour toutes les raisons explicitées ci-haut, il peut subsister un déficit affectant le niveau de généralisabilité des résultats.

Pour ce qui est de la validité interne de l'échantillon, les sujets ont tous été recrutés sur des forums de discussions, et sont anglophones. Par contre, au fil des entrevues, il a été observé que les participants n'étaient pas tous motivés par les mêmes facteurs, affectant leurs réponses quant à leurs intérêts, et du même coup, influencer le processus d'apprentissage qui y est lié. Cet élément s'est avéré important au moment de l'analyse et peut affecter la solidité du lien dans les résultats.

Conclusion

L'objectif principal de cette étude était de comprendre le processus d'apprentissage des pirates informatiques, à l'intérieur du cadre de la théorie de l'apprentissage social. Les sous-objectifs retenus pour les analyses étaient de comprendre l'influence des pairs dans le monde réel, ceux dans le monde virtuel, ainsi que le rôle de l'imitation dans l'apprentissage de ces pirates informatiques. Pour ce faire, il a été possible de recruter 17 participants, provenant principalement de trois communautés dédiées au piratage informatique.

L'analyse de ces résultats a permis d'apprendre que les pirates informatiques débuteraient initialement leur apprentissage soit par curiosité ou intérêt envers l'informatique, soit à travers un intérêt connexe, comme les jeux vidéo, les menant vers des espaces de convergence tels que les forums de discussion spécialisés pour obtenir des réponses à leurs interrogations et rencontrer des pairs ayant les mêmes centres d'intérêt. C'est surtout au sein de telles communautés que les usagers vont, de fil en aiguille et en discutant avec d'autres membres, en apprendre au sujet de divers autres domaines informatiques connexes, élargir leurs horizons, apprendre et développer des techniques et potentiellement internaliser des définitions favorables à la participation à des activités considérées comme étant déviantes ou criminelles. L'imitation jouerait également un rôle important dans l'apprentissage initial de techniques et l'élaboration d'outils/scripts adaptés, puisque les activités de pirate informatique nécessitent une certaine maîtrise de base d'un langage de programmation et que cet apprentissage peut s'effectuer aisément en modifiant les scripts des autres, trouvés sur des plateformes spécialisées. S'ils sont chanceux, ils trouveront un mentor qui les prendra sous son aile et qui les aidera à aller plus loin dans leurs apprentissages et surtout progresser

plus rapidement. Par ailleurs, peu de participants ont affirmé avoir eu des personnes dans leur entourage dans le monde réel ayant contribué à leurs apprentissages.

À la lumière des entretiens, il a également été possible de comprendre qu'il existait une perspective différente et donc un cheminement d'apprentissage fondamentalement différent chez les pirates passionnés par l'informatique et ceux opportunistes, qui rechercheraient le profit avant tout, mais que ces deux catégories n'étaient pas pour autant mutuellement exclusives chez les pirates informatiques. Pour ceux-ci, les communautés représentent surtout d'un terrain fertile pour recruter des associés ou dénicher des clients potentiels à qui offrir leurs services.

Au final, il n'existerait pas de chemin préétabli pour devenir un pirate informatique. Chacun aura un parcours unique, en lien avec ses intérêts et motivations. Par contre, tous ces individus peuvent converger vers une même communauté, que ce soit pour trouver de l'information ou des outils, développer de nouvelles techniques et se tenir à jour, rencontrer des pairs, des clients ou des associés, ainsi que s'encourager et se mesurer les uns aux autres. L'évolution d'un pirate informatique serait, quant à elle, un chemin en solitaire, pavé d'essais et erreurs, au fil du cheminement poursuivi, ainsi que des compétences et des aptitudes personnelles qu'il sera en mesure de développer.

Cette étude a aussi permis de dégager de nouvelles avenues de recherches qui pourraient permettre d'en apprendre plus sur ce sujet peu étudié. Premièrement, il pourrait être intéressant de pousser cette recherche qualitative plus loin en étudiant le processus d'apprentissage social des pirates informatiques en lien avec leurs motivations. En effet, les résultats suggèrent que ce parcours diffère. Ensuite, de pouvoir combiner les données qualitatives à des traces internétiques dans l'optique d'effectuer une analyse traçologique permettrait d'avoir une compréhension plus globale et complète du phénomène d'apprentissage des pirates informatiques. Finalement, il pourrait également être pertinent de différencier les membres des communautés de pirates qui commettent des actes déviants, de ceux qui sont réellement engagés dans une trajectoire de vie criminelle, afin d'en distinguer les différences et potentiellement identifier les caractéristiques propres aux pirates informatiques réellement criminalisés.

Références bibliographiques

Akers, R. L. (2009). *Social learning and social structure : A general theory of crime and deviance*. Transaction Publishers.

Akers, R. L., Sellers, C. S., & Jennings, W. G. (2017). *Criminological Theories : Introduction, Evaluation, & Application* (7th éd.). Oxford University Press.

Akers, R. L., Sellers, C. S., & Jennings, W. G. (2021). *Criminological Theories : Introduction, Evaluation, and Application* (8th éd.). Oxford University Press.

Bachmann, M. (2010). *The Risk Propensity and Rationality of Computer Hackers*. *4*(1), 14.

Baillargeon-Audet, K. (2010). *Étude de cas d'un réseau de pirates informatiques au Québec* [Non-publié]. Université de Montréal.

Bécue, A., & Décary-Hétu, D. (2016). Traceology – Fusing Forensic Science And Criminology For Security. *Security Journal*, *29*(4), 539-542. https://doi.org/10.1057/sj.2015.28

Boman, J. H., & Freng, A. (2017). Differential Association Theory, Social Learning Theory, and Technocrime. Dans K. F. Steinmetz & M. R. Nobles, *Technocrime and Criminological Theory* (p. 55-65). Taylor & Francis Group. http://ebookcentral.proquest.com/lib/umontreal-ebooks/detail.action?docID=5056434

Brenner, S. W. (2001). *Cybercrime Investigation and Prosecution:* 40.

Champion, D. J. (2006). *Research Methods for Criminal Justice and Criminology* (3rd éd.). Pearson Education.

Cullen Francis T. & Pamela Wilcox. (2012). *The Oxford Handbook of Criminological Theory*. /z-wcorg/.

De Leeuw, E. D. (1992). *Data Quality in Mail, Telephone and Face-to-Face Surveys* [Thèse de doctorat]. Vrije Universiteit.

Décary-Hétu, D. (2013a). Information exchange paths in IRC hacking chatrooms. Dans *Crime And Networks* (Morselli, Carlos, p. 18). Routledge.

Décary-Hétu, D. (2013b). Le piratage Informatique. Dans *Cybercriminalité—Entre inconduite et crime organisé* (Fortin, Francis). Presses internationales Polytechnique. https://daviddhetu.openum.ca/files/sites/39/2016/05/Le-piratage-informatique-1.pdf

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 129-151. https://doi.org/10.1080/17440572.2016.1157480

Edwards, G. (2020). *Cybercrime Investigators Handbook* (1re éd.). Wiley. https://doi.org/10.1002/9781119596318

Franklin, P., Adams, R., & Henry, C. (2019). *What the hack is a hacker?* James Madison University.

Gauthier, B. (Éd.). (2010). *Recherche Sociale : De la problématique à la collecte de données*. Presses de l'Université du Québec.

Gendarmerie Royale du Canada. (2016). *Stratégie de lutte contre la cybercriminalité de la Gendarmerie Royale du Canada.* https://www.rcmp.gc.ca/wam/media/1089/original/e1a9d988ea543658c8ea1463d588c6b0.pdf

Goode, S., & Cruise, S. (2005). What Motivates Software Crackers? *Journal of Business Ethics*, *65*(2), 173-201. https://doi.org/10.1007/s10551-005-4709-9

Graham, R. S., & Smith, S. K. (2019). Cybercriminology. Dans *Cybercrime and Digital Deviance* (1st edition, p. 196-214). Routledge.

Hald, S. L. N., & Pedersen, J. M. (2012). *An updated taxonomy for characterizing hackers according to their threat properties*. 6.

Hald, S., & Pedersen, J. (2012). An updated taxonomy for characterizing hackers according to their threat properties. *2012 14th International Conference on Advanced Communication Technology (ICACT)*, 81-86.

Hartley, R. D., Ellis, L., & Walsh, A. (2020). *Research Methods for Criminology and Criminal Justice*. Rowman & Littlefield Publishers. http://ebookcentral.proquest.com/lib/umontreal-ebooks/detail.action?docID=6361233

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2007). Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States. *Social Science Computer Review*, *25*(3), 339-357. https://doi.org/10.1177/0894439307299934

Higgins, G. E., & Makin, D. A. (2004). *Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy? 2*(2), 22.

Higgins, G. E., & 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. https://doi.org/10.1057/palgrave.sj.8350002

Hinduja, S., & Ingram, J. (2009). Social learning theory and music piracy : The differential role of online and offline peer influences. *Criminal Justice Studies*, *22*, 405-420. https://doi.org/10.1080/14786010903358125

Holt, T. J. (2007). subcultural evolution ? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171-198. https://doi.org/10.1080/01639620601131065

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, *37*(3), 378-395. https://doi.org/10.1007/s12103-011-9117-3

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance : Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61. https://doi.org/10.1080/0735648X.2010.9721287

Holt, T. J., & Copes, H. (2010). Transferring Subcultural Knowledge On-Line : Practices and Beliefs of Persistent Digital Pirates. *Deviant Behavior*, *31*(7), 625-654. https://doi.org/10.1080/01639620903231548

Hutchings, A., & Holt, T. J. (2018). Interviewing Cybercrime Offenders. *Journal of Qualitative Criminal Justice & Criminology*. https://doi.org/10.21428/88de04a1.1fdab531

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, *46*(4), 757-780. https://doi.org/10.1111/1467-954X.00139

Junger, M. (2019). Cyber-offenders versus traditional offenders : An empirical comparison. *Tijdschrift Voor Criminologie*, *61*(1), 103-108. https://doi.org/10.5553/TvC/0165182X2019061001005

Kizza, J. M. (2013). Cyber Crimes and Hackers. Dans J. M. Kizza, *Guide to Computer Network Security* (p. 107-132). Springer London. https://doi.org/10.1007/978-1-4471-4543-1_5

Larribeau, A. (2019). Du bidouilleur amateur à l'informaticien, apprendre le détournement : Une étude de la socialisation au hacking informatique. *Sociologies pratiques*, *N° 38*(1), 59-70.

Lavoie, P.-É., Fortin, F., & Tanguay, S. (2013). Problèmes relatifs à la définition et à la mesure de la cybercriminalité. Dans F. Fortin (Éd.), *Cybercriminalité : Entre inconduite et crime organisé*. Presses internationales Polytechnique et Sûreté du Québec.

Leman-Langlois, S. (Éd.). (2008). *Technocrime : Technology, crime and social control*. Willan.

Madarie, R. (2017). *Hackers' Motivations : Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers*. *11*(1), 20.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in High School : Cybercrime Perpetration by Juveniles. *Deviant Behavior*, *35*(7), 581-591. https://doi.org/10.1080/01639625.2013.867721

Margot, P. (2014). Traçologie : La trace, vecteur fondamental de la police scientifique. *Revue internationale de criminologie et de police technique et scientifique*, *67(1)*, 72-97.

Marion, N. E., & Twede, J. (2020). *Cybercrime : An Encyclopedia of Digital Crime: Vol. First edition*. ABC-CLIO; eBook Collection (EBSCOhost). https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2634295&lang=fr&site=ehost-live

McBrayer, J. (2014). Exploiting the digital frontier : Hacker typology and motivation [M.S., The University of Alabama]. Dans *ProQuest Dissertations and Theses* (1562270477). ProQuest Dissertations & Theses Global. https://www.proquest.com/dissertations-theses/exploiting-digital-frontier-hacker-typology/docview/1562270477/se-2?accountid=12543

Montégiani, C. (2017). *L'apprentissage social chez les pirates informatiques : Analyse de l'influence des relations d'entraide et de conflit sur le processus d'apprentissage* [Travail dirigé]. Université de Montréal.

Morris, R. G., & 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. https://doi.org/10.1016/j.jcrimjus.2010.04.016

Navarro, J. N., & Marcum, C. D. (2019a). Deviant Instruction : The Applicability of Social Learning Theory to Understanding Cybercrime. Dans T. J. Holt & A. M. Bossler, *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (p. 1-20). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-90307-1_18-1

Navarro, J. N., & Marcum, C. D. (2019b). Deviant Instruction : The Applicability of Social Learning Theory to Understanding Cybercrime. Dans *The Palgrave Handbook of*

International Cybercrime and Cyberdeviance (p. 1-20). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_18-1

Oliver, D., & Randolph, A. B. (2020). Hacker Definitions in Information Systems Research. *Journal of Computer Information Systems*, 14. https://doi.org/10.1080/08874417.2020.1833379

Rogers, M. (1999). *Psychology of Hackers : Steps Toward a New Taxonomy* [University of Manitoba]. http://homes.cerias.purdue.edu/~mkr/hacker.doc

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior : An exploratory study.* University of Manitoba (Winnipeg).

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, 6.

Rossy, Q., & Décary-Hétu, D. (2017). Internet traces and the analysis of online illicit markets. Dans Q. Rossy, D. Décary-Hétu, O. Delémont, & M. Mulone (Éds.), *The Routledge International Handbook of Forensic Intelligence and Criminology* (1re éd., p. 249-263). Routledge. https://doi.org/10.4324/9781315541945-21

Salisbury, E. J. (2012). Social Learning and Crime. Dans F. T. Cullen & P. Wilcox (Éds.), *The Oxford Handbook of Criminological Theory*. Oxford University Press.

Seebruck, R. (2015). A typology of hackers : Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36-45. https://doi.org/10.1016/j.diin.2015.07.002

Sharma, R. (2007). Peeping into a Hacker's Mind : Can Criminological Theories Explain Hacking? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1000446

Skinner, W. F., & 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. https://doi.org/10.1177/0022427897034004005

Steinmetz, K. F. (2015). Becoming a Hacker : Demographic Characteristics and Developmental Factors. *Journal of Qualitative Criminal Justice & Criminology*. https://doi.org/10.21428/88de04a1.af131ffc

Steinmetz, K. F., & Nobles, M. R. (2018). *Technocrime and Criminological Theory* (Vol. 1-1 online resource (1 volume)). Routledge; WorldCat.org. https://doi.org/10.4324/9781315117249

Summers, T. C. (2013). *How hackers think : A study of cybersecurity experts and their mental models*. 34.

Sutherland, E. H., & Cressey, D. R. (1966). *Principes de criminologie*. Ed. Cujas; WorldCat.org.

Tremblay, P. (2010). *Le délinquant idéal : Performance, discipline, solidarité*.

Viano, E. C. (Éd.). (2017). *Cybercrime, Organized Crime, and Societal Responses*. Springer International Publishing. https://doi.org/10.1007/978-3-319-44501-4

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, *17*(6), 1239-1251. https://doi.org/10.1007/s10796-015-9567-0