

Université de Montréal

La réussite criminelle des participants à la fraude financière en ligne

Par
Mathieu Guillot

École de criminologie, Faculté des arts et des sciences

Mémoire présenté en vue de l'obtention du grade de Maîtrise ès sciences (M.Sc.)
en criminologie

Septembre 2019

© Mathieu Guillot, 2019

Université de Montréal
Faculté des études supérieures et postdoctorales

Le présent mémoire:
La réussite criminelles des participants
à la fraude financière en ligne

Présenté par :
Mathieu Guillot

A été évalué par un jury composé des personnes suivantes :

Benoît Dupont, président-rapporteur
David Décary-Héту, directeur de recherche
Francis Fortin, membre du jury

RESUME

Le carding est un phénomène cybercriminel de par lequel des cyberdélinquants (appelés *carders*) vont compromettre et utiliser frauduleusement des données financières et bancaires. De nombreuses entités privées ou publiques ont mis en évidence l'importance des pertes monétaires occasionnées par ce nouveau type de criminalité. D'un point de vue criminologique, peu de recherches académiques se sont penchées sur l'ampleur de ce phénomène et plus particulièrement sur la réussite criminelle des carders.

Pour combler ce manque de connaissances, ce projet de recherche a pour objectif de comprendre la réussite criminelle des carders en observant l'impact de leurs caractéristiques personnelles et sociales sur leurs revenus criminels. Les différentes variables mobilisées relatent entre autres les activités marchandes ou encore les caractéristiques sociodémographiques des carders interrogés. Pour ce faire, un sondage en ligné, hébergé sur Tor, a été mené. Au total, 49 sondages complets ont été collectés pour être analysés.

En s'attellant à décrire les caractéristiques personnelles et sociales des carders, ce travail a été en mesure de mettre à jour les connaissances préalablement acquises sur les carders et de répondre à des manques de consensus sur certains pans des activités de ces cyberdélinquants. L'ensemble des résultats révèlent que peu de carders affichent une réussite criminelle élevée et qu'une minorité d'entre eux gagnent de forts revenus. La réussite criminelle des carders s'explique par le fait de disposer de compétences spécialisées, de bénéficier d'une bonne expérience, d'utiliser des forums de discussion en ligne ou encore d'occuper des rôles centraux sur les lieux de convergence virtuels. Outre le fait d'apporter des réponses quant à ces prédicteurs sur la réussite criminelle des carders, ce projet de recherche permet de constater les apports et les faiblesses de l'utilisation d'un sondage pour collecter des données dans un écosystème cybercriminel.

Mots-clefs : Réussite criminelle, carding, cybercriminalité, darknet, sondage

ABSTRACT

Carding is a criminal phenomenon which consists of compromising financial data in order to do fraudulent transactions. Several private and public parties highlighted the size of the loss caused by this new form of criminality. From the criminological angle, little research is available in the size and scope of the phenomenon, particularly on the criminal achievement of this kind of online offenders (called carders).

To fill this gap, this research project is aimed at understand the criminal achievement of carders by observing the impact of their personal and social characteristics on their criminal income. Theses variables relate among others to their market activities or their sociodemographic. To do so, an online survey, hosted on Tor, was conducted. A total of 49 completed surveys were collected to do our analysis.

By describing these personal and social characteristics, this work has been able to update our knowledge about carders and to address gaps about certain part of what we known about carding. Overall, the results shown that few carders can claim a good criminal achievement and that a minority of them can earn large amounts of money. Experience, speciliazed skills, the use of online forums or play the role of broker explained the criminal achievement among carders. Apart from the fact that our study brings some answers about those predictors, this project highlights the strengths and weaknesses of using an online survey to collect data from a criminal ecosystem.

Keywords: Criminal achievement, carding, cybercrime, darknet, survey

TABLES DES MATIERES

Résumé.....	i
Abstract.....	ii
Liste des tableaux.....	v
Liste des figures.....	vi
Liste des abréviations	vii
Remerciements	viii
Introduction.....	1
Chapitre 1 - Recension des écrits.....	4
1.1. La réussite criminelle	5
1.1.1. Mesurer la réussite criminelle	5
1.1.2. Les prédicteurs de la réussite criminelle	8
1.2. Le carding.....	12
1.2.1. Définition et ampleur du phénomène.....	12
1.2.2. Les caractéristiques des carders	15
1.2.3. Le script criminel du carding	16
1.2.4. Évolution des lieux de convergences	25
1.3. Problématique.....	29
Chapitre 2 - Données	36
2.1. La constitution du sondage	37
2.2. Les stratégies de promotion	39
2.3. L'échantillon	43
2.3.1. Identification des réponses aberrantes	45
2.3.2. Les données manquantes	51
2.4. Limites	55
Chapitre 3 - Méthodologie.....	56
3.1. Mesurer les revenus criminels des carders	57
3.2. Décrire les caractéristiques personnelles et sociales des cardeurs	58

3.3. Identifier les caractéristiques personnelles et sociales qui expliquent les revenus des	
cardeurs	66
3.4. Limites	71
Chapitre 4 - Analyses et résultats	73
4.1. Mesurer les revenus criminels des carders	74
4.2. Mesurer les caractéristiques personnelles et sociales des carders	75
4.2.1. Activités marchandes	75
4.2.2. Habilités et compétences particulières	79
4.2.3. Expériences de victimisation endogène	80
4.2.4. Fréquence d'utilisation des technologies d'anonymat	82
4.2.5. Contacts	84
4.2.6. Caractéristiques sociodémographiques	85
4.3. Identifier les caractéristiques personnelle et sociales qui expliquent la réussite des carders	
.....	88
Chapitre 5 - Discussion	95
5.1. L'expérience	96
5.2. Activités criminelles.....	100
5.3. Sociabilité	104
5.4. Sociodémographiques.....	105
5.5. Limites	106
Conclusion	109
Bibliographie	113
Annexe I.....	ix
Annexe II	xxi
Annexe III.....	xxiii

LISTE DES TABLEAUX

Tableau 1. Récapitulatif des mesures opérationnalisant la réussite criminelle.....	6
Tableau 2. Identification des prédicteurs ayant un impact sur la réussite criminelle mesurée par les revenus criminels.....	9
Tableau 3. Résumé du script criminel proposé par Hutchings et Holt (2015).....	18
Tableau 4. Sections du sondage et variables à interrogées.....	34
Tableau 5. Indices de tendance centrale et de dispersion pour le temps de passation par page	50
Tableau 6. Distribution des valeurs manquantes pour la base de données des vendeurs	53
Tableau 7. Distribution des valeurs manquantes pour la base de données des acheteurs.....	54
Tableau 8. Dimensions, prédicteurs et modèle empirique	67
Tableau 9. Dimensions et variables contrôles ajoutées	68
Tableau 10. Indices de tendance centrale et de dispersion pour les revenus et les profits	74
Tableau 11. Indice de tendance centrale et de dispersion pour l'année de début des activités et les nombres de produits	76
Tableau 12. Proportions des types de produits, types de lieux de convergence, rôles occupés et moyens de paiement.....	78
Tableau 13. Statistiques descriptives des variables dichotomiques des habiletés et compétences particulières	79
Tableau 14. Statistiques descriptives des mesures autoévaluées des compétences	79
Tableau 15. Fréquences des expériences de victimisation endogène selon les types de lieux de convergence	81
Tableau 16. Fréquences d'utilisation des différentes technologies d'anonymat.....	83
Tableau 17. Indices de tendance centrale et de dispersion des mesures des contacts	84
Tableau 18. Analyses descriptives des caractéristiques sociodémographiques.....	86
Tableau 19. Coefficient de corrélation Rhô de Spearman entre les variables indépendantes et les revenus et les profits des deux échantillons	90
Tableau 20. Tests de U de Mann-Whitney pour les variables Dumps, Forum et Logiciels malveillants pour les vendeurs.....	92
Tableau 21. Tests de U de Mann-Whitney pour les variables Courtier financier et Aucun rôle pour les acheteurs.....	93

LISTE DES FIGURES

<i>Figure 1.</i> Série chronologie du nombre de visites par jour sur le site hébergeant le sondage.	42
<i>Figure 2.</i> Distribution du nombre de visites par pages parcourues	44
<i>Figure 3.</i> Exemple d'insulte reçue sur un cryptomarché lors de la phase de test	46
<i>Figure 4.</i> Exemple d'un IMC - the Blue Dot task (Oppenheimer, Meyvis & Davidenko, 2009)	47

LISTE DES ABREVIATIONS

- CVV : Card Verification Value
- I2P : Invisible Internet Project
- VPN : Virtual Private Network
- MCAR: Missing Completely At Random

REMERCIEMENTS

Tout d'abord, je tiens à remercier mon directeur de recherche, David, pour sa disponibilité, ses précieux conseils et ses encouragements qui m'ont toujours permis d'aller de l'avant. Merci aussi pour toutes ses opportunités que tu as pu me confier depuis que l'on se connaît qui m'ont permis de construire ma méthodologie en tant que chercheur sur des sujets qui me passionnent.

Je tiens aussi à remercier Guillaume et Francis pour m'avoir accordé leurs confiances en tant qu'auxiliaire d'enseignement. Ces postes m'ont permis de continuer à parfaire mes connaissances criminologiques et m'ont permis de travailler dans le monde académique.

Merci aussi au Centre International de Criminologie Comparée pour son soutien financier apportait dans le cadre de ce mémoire mais aussi pour les précédents projets sur lesquels j'ai eu la chance de travailler.

Je voudrais remercier tous mes amis et mes colocataires qui ont su me soutenir dans cette aventure. Mention spéciale à mon *frate*, Igor. Tu es probablement la personne qui connaît le mieux mon sujet de recherche après mon directeur et les discussions qu'on a pu avoir autour de ça m'ont toujours enrichies. Merci mon pote.

Pour finir, je voudrais remercier mon père, ma mère et Roger. Malgré les kilomètres, vous m'avez donné votre soutien indéfectible sur tous les plans depuis le début de ce projet. J'ai énormément de chance de vous avoir et je vous dédie ce travail.

INTRODUCTION

Le concept de réussite criminelle s'inscrit dans le paradigme des carrières criminelles (Lussier, Bouchard & Beauregard, 2016), définies comme une description longitudinale de la séquence de crimes commis par un délinquant (Blumstein, 1986). En s'intéressant aux facteurs qui influencent la durée, l'intensité et les caractéristiques des comportements criminels, l'étude des carrières criminelles permet de mieux comprendre les délinquants les plus persistants qui ont, par conséquent, le plus d'impact sur la société (Piquero, Farrington & Blumstein, 2003). C'est dans ce cadre que la réussite criminelle s'intéresse plus spécifiquement aux bénéfices et aux coûts émanant de différents types de crimes (Ouellet, 2018). Elle se base sur la théorie des renforcements différentiels (Jeffery, 1965) qui compare les renforcements et des punitions vécues. Les délinquants seraient plus enclins à persister dans leur criminalité si la comparaison est favorable.

La littérature sur le sujet a montré que, comme pour la réussite conventionnelle, la réussite criminelle peut se décliner dans plusieurs dimensions (McCarthy & Hagan, 2001; Morselli & Tremblay, 2004b; Ouellet & Tremblay, 2014). Ces différentes dimensions permettent de couvrir le spectre de la réussite criminelle à la lumière des diverses motivations qui se cachent derrière un acte criminel. Ainsi, la réussite criminelle d'un délinquant motivé par l'appât du gain ne se traduira pas par la même dimension qu'un agresseur sexuel qui souhaite satisfaire ses pulsions.

Dans le cadre de ce mémoire, nous porterons notre attention sur la réussite criminelle d'une forme de cybercriminalité particulière : le *carding*. Ce phénomène est défini comme l'utilisation frauduleuse d'informations de cartes de crédit avec comme but d'acheter des biens et des services (Peretti, 2009). Cette forme de cybercriminalité doit principalement son apparition à la démocratisation des services financiers et commerciaux en ligne (Newman & Clarke, 2003; Wall, 2007; Holt & Bossler, 2014). En effet, ce type de fraude se base en grande partie sur l'exploitation de données financières de nature virtuelles. Alors que les technologies de l'information et de la communication ont permis de faire émerger ce type de données sensibles, elles ont aussi permis à ces criminels, appelés *carders*, de communiquer, de marchander leur savoir-faire et de bénéficier de lieux virtuels où ils pourraient se retrouver pour mener à bien leurs activités criminelles.

Des faits récents ont montré que le *carding* pouvait engendrer des pertes importantes qui nuisent à la fois aux victimes fraudées mais aussi aux entreprises touchées. Bien qu'un certain nombre d'instances privées et publiques aient émis des résultats quant à l'ampleur de ce phénomène, il

demeure que l'étude des montants engrangés par les carders reste relativement peu explorée. En effet, alors que les gains financiers constituent la principale motivation des criminels qui s'adonnent à ce type d'activité criminelle, l'unique étude qui s'est attelée à les mesurer présente des limites méthodologiques (Holt, Smirnova et Chua, 2016). D'une part, les échantillons étudiés se composent de carders évoluant sur un type de lieux virtuels particulier et nous savons aujourd'hui qu'il en existe une multitude qui sont utilisés par ces cyberdélinquants. D'autre part, la manière d'opérationnaliser le calcul des revenus se base sur des indices pouvant être biaisés. Ainsi, ce mémoire aura comme objectif général de comprendre la réussite criminelle différentielle des carders évoluant sur le darknet. Au-delà de fournir des nouveaux résultats quant aux revenus criminels de ces délinquants, cette approche permet à ce projet de s'inscrire dans les travaux réalisés sur la réussite criminelle.

Pour y répondre, ce mémoire de maîtrise se compose de cinq chapitres. Le premier fait une recension de la littérature en présentant le concept de réussite criminelle. Il s'attarde particulièrement à décrire les manières de la mesurer et à mettre en avant les prédicteurs qui l'influencent. Par la suite, une seconde section définit le phénomène de carding qui s'articulera notamment autour de la présentation du script criminel de ce type de fraude. Le second chapitre porte sur les données et explique comment a été constitué et promu le sondage utilisé. Il explique aussi les techniques utilisées pour composer avec le fait que les sondages complétés présentent des réponses aberrantes. Le chapitre de méthodologie qui s'en suit montre comment ont été opérationnalisées les variables ainsi que les stratégies d'analyses qui seront entreprises pour répondre aux objectifs de cette recherche. Finalement, les deux derniers chapitres proposent successivement d'observer les analyses de cette étude et de discuter des principaux résultats.

CHAPITRE 1 - RECENSION DES ECRITS

1.1. LA REUSSITE CRIMINELLE

1.1.1. MESURER LA REUSSITE CRIMINELLE

Les revenus illégitimes forment la dimension la plus étudiée de la réussite criminelle (Wilson & Abrahamse, 1992; McCarthy & Hagan, 2001; Uggen & Thompson, 2003; Morselli & Tremblay, 2004a; Robitaille, 2004; Morselli, Tremblay & McCarthy, 2006; Ouellet & Tremblay, 2014; Rowan, McGloin & Nguyen, 2018). Cette orientation se justifie par le fait que, d'un point de vue rationnel et dans nos sociétés actuelles, une majorité d'individus recherche une certaine réussite financière et que, du point de vue criminel, un gain monétaire constitue la forme la plus palpable de récompense (Morselli & Tremblay, 2004b; Nguyen & Loughran, 2017). Cette recherche de gains monétaires fait écho au fait que les individus cherchent à maximiser leurs revenus pour acquérir un statut social plus prestigieux. En effet, les revenus légitimes supplantent le niveau d'études et le poste occupé lorsqu'il s'agit de juger du statut social d'un individu (Coleman et Rainwater, 1979). Il n'est alors pas étonnant de constater que les crimes motivés par les gains monétaires constituent l'une des formes les plus prégnantes de la criminalité en termes de nombre de commissions, entraînant ainsi d'importantes pertes financières (Baumer & Gustafson, 2007). Naylor (2003) a proposé une typologie de ce type de crime. Il définit les *predatory crimes* comme étant “*a redistribution of existing legally owned wealth from one party to another*”. Cette catégorie peut ainsi regrouper des crimes comme le cambriolage, la fraude ou encore le vol d'automobiles (Morselli, Tremblay & McCarthy, 2006). Cet auteur s'est aussi intéressé aux crimes de marchés qu'il définit comme “*la production ou la distribution de biens ou services illégaux*”. Ainsi, les crimes motivés par l'argent peuvent aussi regrouper des actes comme la vente de drogues, la contrebande, le proxénétisme ou les jeux illégaux (Morselli, Tremblay & McCarthy, 2006).

Plusieurs sources de données peuvent être utilisées pour mesurer cette dimension de la réussite criminelle. Certains chercheurs ont utilisé les pertes moyennes subies par les victimes telles que référencées par les rapports émis par les instances publiques alors que d'autres se sont appuyés sur des travaux passés pour obtenir des estimations des revenus (Reuter, MacCoun & Murphy, 1990; Wilson & Abrahamse, 1992; McCarthy & Hagan, 2001). Dans une autre optique, les données en sources ouvertes présentes sur les marchés noirs en ligne ont aussi permis à d'autres recherches d'estimer les revenus espérés des cyberdélinquants (Holt, Smirnova et Chua, 2016). D'autres auteurs ont pu bénéficier d'un accès à des données présentant moins de limites que les

statistiques officielles et les données en sources ouvertes. En effet, Levitt et Venkatesh (2000) ont pu obtenir les livres de comptes tenus par un leader de gang impliqué dans le trafic de drogue. Ces livres étaient mis à jour chaque mois par un des hommes de main et ont offert aux chercheurs une fenêtre inédite de quatre ans sur l'évolution de la réussite financière d'une telle organisation. En allant du simple revendeur au leader du gang, il était possible de distinguer la réussite financière relative en fonction des rôles occupés au sein d'une organisation criminelle, mais aussi d'un point vu longitudinal (Levitt et Venkatesh, 2000; Gundur, 2019).

Tableau 1. Récapitulatif des mesures opérationnalisant la réussite criminelle

Dimensions de la réussite	Opérationnalisation
Les revenus criminels	Pertes moyennes des victimes
	Résultats émis par des travaux passés
	Livres de comptes de délinquants
	Sondage avec revenus auto-rapportés
Accès aux opportunités	Liens non redondants dans un réseau criminel
Évitement des coûts	Ratio confrontant la durée de la carrière et la gravité des délits commis aux peines reçues

Ainsi, la technique d'opérationnalisation des revenus criminels la plus communément utilisée repose sur l'utilisation de sondages interrogeant directement les criminels sur leurs revenus (Tremblay & Morselli, 2000; Morselli & Tremblay, 2004a; Morselli & Tremblay, 2004b; Thompson & Uggen, 2012; Ouellet, 2018; Rowan, McGoin & Nguyen, 2018). Cette démarche s'appuie bien souvent sur des échantillons de détenus (Wilson & Abrahamse, 1992; Tremblay & Morselli, 2000; Morselli & Tremblay, 2004b; Morselli, Tremblay & McCarthy, 2006; Charest & Tremblay, 2009; Bouchard & Ouellet, 2011; Ouellet & Tremblay, 2014; Ouellet, 2018). De prime abord, cette technique peut laisser perplexe. Plusieurs raisons laissent penser que les délinquants pourraient se laisser aller à un élan de vantardise et surestimer leurs revenus (Wilson & Abrahamse, 1992). Malgré cela, une récente étude a montré que les revenus autorapportés des délinquants étaient consistants avec la réalité (Nguyen & Loughran, 2017). En effet, il existe plusieurs stratégies visant à assurer la fiabilité et la validité de ce type de données. L'une d'entre elles consiste à interroger les détenus sur des éléments contextuels à leurs histoires de vies délinquantes pour s'assurer que les estimations fournies soient

consistantes avec ces récits (Morselli & Tremblay, 2004a; Ouellet, 2018). Une autre technique consiste à appliquer une fonction logarithmique sur les revenus autorapportés. Ceci permet de réduire l'effet des écarts extrêmes entre les délinquants et de normaliser la distribution des revenus tout en contingentant l'effet néfaste des déclarations étant surestimées (Ouellet & Tremblay, 2014). En réduisant les écarts extrêmes, l'effet d'une augmentation de revenus de même nature aura un impact plus prononcé pour les délinquants présentant moins de revenus que pour ceux se trouvant dans le haut du panier.

Les revenus criminels ne constituent pas la seule mesure utilisée pour attester de la réussite criminelle des délinquants. Comme le présente le tableau 1, il existe d'autres dimensions et mesures de la réussite criminelle. L'une d'entre elles est l'accès à des opportunités. Pour la mesurer, plusieurs travaux se sont intéressés aux réseaux sociaux des délinquants se positionnant comme intermédiaires dans un réseau criminel (Morselli, 2000; Morselli & Tremblay, 2004b; Décary-Héту et Leppänen, 2013; Calderoni & Superchi, 2019). À titre d'exemple, une des méthodes consistait à utiliser une version modifiée d'un questionnaire étant destiné à l'origine à des employés d'entreprises légitimes. Ainsi, il était demandé aux répondants de préciser le nombre relations qu'ils entretenaient avec d'autres délinquants (les chercheurs avaient fixé un seuil maximum de 15 connexions) et de qualifier la force de chaque relation. Par la suite, les auteurs ont utilisé une matrice pour chaque répondant et ont appliqué des mesures d'analyse de réseaux pour découvrir la redondance dans ces réseaux (Morselli & Tremblay, 2004b).

Pour certaines formes de criminalité, les revenus criminels et l'accès à des opportunités ne peuvent pas s'appliquer en tant que dimension de la réussite criminelle. Dans ce genre de cas, il est plus pertinent de prendre en compte l'évitement des coûts (Lussier et Mathesius, 2012). Cette dimension se définit comme la capacité et l'habilité à éviter tout contact avec le système de justice et peut se décliner en plusieurs sous-dimensions comme l'évitement de sanctions pénales, l'évitement de la détection ou une moindre probabilité d'arrestations (Shover & Thompson, 1992; McCarthy & Hagan, 2001; Kazemian & Le Blanc, 2007; Bouchard & Nguyen, 2010; Fader, 2016; Blokland, 2017; Boccio, Beaver & Schwartz, 2018). Ces dimensions sont particulièrement pertinentes lorsqu'il s'agit de se questionner sur la réussite criminelle des délinquants sexuels (Lussier, Bouchard & Beauregard, 2011; Lussier &

Mathesius, 2012) mais peuvent être aussi mobilisées pour se pencher sur la résilience de groupes criminels face à la détection policière (Bouchard & Nguyen, 2010; Blokland, 2017).

1.1.2. LES PREDICTEURS DE LA REUSSITE CRIMINELLE

L'ensemble des travaux sur la réussite criminelle ayant porté sur les revenus illégitimes a mis en lumière l'impact de prédicteurs pouvant être associés à la fois aux caractéristiques du délinquant ou à son réseau social. Le tableau 2 présente un récapitulatif des prédicteurs et de leurs impacts. Au niveau des caractéristiques personnelles, l'expérience criminelle a un impact positif sur la réussite criminelle. En effet, les gains criminels augmentent en fonction de l'âge des délinquants et du nombre de condamnations passées (Robitaille, 2004; Ouellet & Tremblay, 2014). Cette dernière observation illustre la place qu'ont les institutions carcérales en tant qu'« universités » du crime permettant aux délinquants de bénéficier d'apprentissages auprès de leurs congénères (Kazemian & Le Blanc, 2007). Ces apprentissages, qui peuvent se traduire en compétences et habiletés particulières, auront eux aussi un impact positif sur la réussite (McCarthy et Hagan 2001; Morselli et Tremblay 2004; Morselli, Tremblay et McCarthy 2006; Ouellet & Tremblay, 2014; Ouellet, 2018). Cet aspect d'expérience peut aussi s'observer au travers de l'établissement de tactiques avant la commission de l'acte (Robitaille, 2004) et au travers de la spécialisation des criminels dans un type de délinquance (Tremblay & Morselli, 2000) qui ont tous deux des impacts positifs sur la réussite des délinquants. Une autre composante personnelle ayant un impact positif est la fréquence de consommation de drogues (Robitaille, 2004). D'autres auteurs ont souligné ce phénomène en soutenant que cette augmentation s'opérait lors de périodes de consommation d'héroïne ou de cocaïne (Uggen & Thompson, 2003). Ceci s'expliquant par le fait que les consommateurs de drogues sont dans une recherche perpétuelle d'argent pour assouvir leurs dépendances (Thompson & Uggen, 2012). En termes de déplacement, les recherches montrent qu'à la fois le fait de passer du temps dans la rue (Rowan, McGloin & Nguyen, 2018) et le fait d'être mobile (Morselli & Royer, 2008) ont un effet positif sur la réussite criminelle. La fréquence des activités criminelles est elle aussi corrélée positivement avec la réussite (Tremblay & Morselli, 2000; Robitaille, 2004). Néanmoins, il est à noter que les criminels les plus prolifiques génèrent qualitativement moins de revenus pour chaque acte que ceux ayant restreint leurs actions criminelles (Tremblay & Morselli, 2000). Finalement, les délinquants affichant un plus faible contrôle d'eux-mêmes présentent une meilleure réussite, même si ce lien n'a pas été validé pour la criminalité de marché (Morselli & Tremblay, 2004)

Tableau 2. Identification des prédicteurs ayant un impact sur la réussite criminelle mesurée par les revenus criminels

Dimension	Prédicteurs et variations identifiés	Impact sur la réussite
Expérience	↑ Nombre de condamnations	↑
	↑ Compétences	↑
	↑ Habiletés particulières	↑
	↑ Établissement de tactiques	↑
	↑ Spécialisation	↑
Activités criminelles	↑ Fréquence de consommation de	↑
	↑ Déplacement(s)	↑
	↑ Fréquence des activités	↑
	↑ Périodes d'inactivité criminelle	↓
Sociabilité	↑ Présence de co-délinquants lors	↓
	↑ Nombres de pairs délinquants	↑
	↑ Propension à collaborer	↑
	↑ Présence d'un mentor	↑
	↑ Liens redondants	↑
	↑ Place de leader	↑
Sociodémographiques	↑ Activité légitime	↓
	↑ Consommation d'alcool	↓
	↓ Contrôle de soi	↑
	↑ Stabilité de la vie affective	↓

D'autres prédicteurs de la réussite criminelle sont à placer dans un contexte de co-délinquance. D'un point de vue général, un accroissement du nombre de pairs délinquants augmente les revenus (Rowan, McGloin & Nguyen, 2018). Plus spécifiquement, la propension à collaborer avec d'autres délinquants a été soulignée comme facteur ayant un impact positif sur la réussite criminelle ainsi que sur l'accès à des opportunités lucratives (Tremblay & Morselli, 2000; Descormiers, Bouchard & Corrado, 2011). Cet effet est particulièrement observé lorsque le délinquant a pu bénéficier de l'expérience d'un mentor au cours de sa carrière, celui-ci lui permettant de se doter de compétences entrepreneuriales et d'avoir un meilleur capital criminel réduisant ainsi les peines d'emprisonnement dont il peut faire l'objet (Morselli, Tremblay &

McCarthy, 2006). Ces habiletés entrepreneuriales peuvent d'ailleurs se traduire par le fait d'avoir des liens non redondants dans son réseau social qui augmentent significativement la réussite criminelle (Morselli & Tremblay, 2000; Morselli & Tremblay, 2004a; Morselli & Tremblay, 2004b). Notons tout de même que cette observation demeure plus probante pour les délinquants se tournant vers une criminalité de marché (Tremblay & Morselli, 2004a). Pour finir, dans le contexte d'une organisation criminelle, occuper une place de leader garantit une meilleure réussite dans la mesure où un gradé obtiendra des gains plus élevés que ses subalternes (Levitt & Venkatesh, 2000).

À l'inverse, d'autres prédicteurs ont un impact négatif sur la réussite criminelle mesurée au travers des revenus. Dans les années 90, l'un des premiers constats a été de noter que le fait d'effectuer des vols ou des cambriolages ne pouvait pas générer des revenus conséquents comparativement au salaire moyen (Wilson & Abrahamse, 1992). En ajoutant à cela le fait de devoir composer avec les risques d'arrestations, il est suggéré que les criminels de ce type n'ont pas connu une carrière réussie. En logique opposition avec le fait que la fréquence des activités criminelles soit corrélée positivement avec la réussite, l'augmentation de la fréquence des périodes d'inactivités a l'effet inverse (Ouellet & Tremblay, 2014). D'autres travaux ont suggéré que la co-délinquance pouvait diminuer la réussite criminelle. En effet, bien que les revenus globalement générés lors de vols soient plus importants lorsque la commission s'effectue en groupe, il semble que les revenus que va tirer chaque individu du groupe soient moins importants que s'ils l'avaient commis seuls (Tillyer & Tillyer, 2015). Cette observation fait écho aux résultats d'un des modèles de Rowan, McGloin et Nguyen (2018) qui montrent que la présence de co-délinquants réduit la réussite criminelle. Bien qu'il ait été souligné que la consommation de drogue a un effet positif sur la réussite financière, d'autres recherches suggèrent que la consommation problématique d'alcool aurait un impact négatif sur cette dernière (Robitaille, 2004). Pour finir, et en accord avec la théorie des contrôles sociaux de Laub et Sampson (1995), plusieurs auteurs ont montré que le fait d'avoir une activité légitime ainsi qu'une vie affective stable réduisait la propension à obtenir plus de revenus (Robitaille, 2004; Thompson & Uggen, 2012; Rowan, McGloin & Nguyen, 2018).

Bien entendu, la place des revenus illégitimes comme mesure de la réussite criminelle doit être mise en perspective. Certains criminels vont préférer recevoir des récompenses matérielles plutôt que monétaires. Ce constat s'illustre, par exemple, au travers du fait que des voleurs

pourraient préférer conserver le fruit de leurs méfaits ou que des consommateurs de drogues préféreraient obtenir de quoi entretenir leurs dépendances (Maher, Dixon, Hall & Lynksey, 2002; Rowan, McGloin & Nguyen, 2018).

Un autre pan de la recherche s'est penché sur les prédicteurs ayant un effet sur l'évitement des coûts. Cette dimension se traduit par l'évitement de la détection policière ou de sanctions pénales. Corroborant les précédentes affirmations évoquées, la littérature a montré que les délinquants plus âgés évitent mieux les sanctions pénales que les plus jeunes (Ouellet & Tremblay, 2014) et que le fait d'être spécialisé dans un type de criminalité sexuelle réduit la lourdeur des peines attribuées par le système de justice (Lussier, Bouchard & Beauregard, 2011). Ce dernier constat peut particulièrement bien s'illustrer au travers des délinquants sexuels s'attaquant à des victimes plus jeunes dans la mesure où cette criminalité a un taux de reportabilité plus faible, les jeunes victimes étant moins promptes à dénoncer leurs victimisations (Lussier & Mathesius, 2012). Kazemian et Le Blanc (2007) ont fourni un profil type du délinquant ayant réussi à éviter des coûts. Leurs résultats suggèrent tantôt des prédicteurs ayant des effets similaires que ceux invoqués dans le cadre des revenus criminels (comme le fait de bénéficier d'un large réseau social), tantôt des prédicteurs rentrant en contradiction avec les résultats émis sur ces mêmes revenus (comme le fait de consommer de la drogue ou d'occuper une activité légitime). De plus, la recherche de prédicteurs sur cette dimension a permis de mettre en évidence l'impact de certaines caractéristiques d'ordre psychologique. En effet, il a été montré qu'un plus grand quotient intellectuel (QI) prédit une meilleure capacité à éviter d'être arrêté (Beaver et al., 2013; Boccio, Beaver & Schwartz, 2018) et qu'un degré de psychopathie élevé ou moyen est positivement associé à la réussite criminelle, bien qu'un faible score à la composante émotionnel puisse contribuer à un certain manque d'empathie qui entraînerait une plus forte propension à être détecté (Aharoni & Khiel, 2013).

Cette revue de littérature a mis en lumière que les recherches sur la réussite criminelle s'attachent particulièrement à l'étudier sous l'expression de formes de criminalités traditionnelles. Il demeure que peu de recherches se sont attelées à étudier la réussite criminelle de nouvelles formes de délinquance comme la cybercriminalité. Wall (2005) a spécifié les impacts que pouvait avoir l'avènement des technologies de l'informations sur les opportunités criminelles. Alors que ces technologies ont pu bénéficier à des types de délinquances traditionnelles en accroissant les opportunités, d'autres types de délinquance sont tout

bonnement nées de ces innovations technologiques. Ces constats soulèvent bien entendu les différences qui existent dans la conceptualisation de la réussite criminelle. En effet, les cyberdélinquants n'évoluent pas dans un espace physique et doivent généralement posséder des compétences techniques au-dessus de la moyenne de la population pour commettre leurs offenses. Ces caractéristiques remettent donc en question la pertinence d'utiliser certaines variables de la réussite criminelle traditionnelle lorsque l'on se penche sur la réussite des cyberdélinquants.

Ainsi, la seconde section de ce chapitre présente le phénomène criminel d'intérêt de ce projet : le carding. Très largement motivé par l'appât de gains financiers, l'étude de ce phénomène entre en résonance avec le cadre théorique développé au cours de cette section.

1.2. LE CARDING

1.2.1. DEFINITION ET AMPLEUR DU PHENOMENE

La démocratisation d'internet a permis aux délinquants de disposer de moyens facilitant la commission de crimes de nature traditionnelle, mais aussi de permettre l'émergence de nouvelles formes de criminalités (Newman & Clarke, 2003; Wall, 2007; Holt & Bossler, 2014). Appelées cybercrimes, ces nouvelles expressions de la criminalité peuvent se définir comme « l'utilisation d'ordinateurs ou tout autre équipement électronique qui, de par leur capacité à accéder à un réseau d'ordinateurs, vont faciliter la commission d'une infraction » (McQuade, 2006). Du point de vue des utilisateurs légitimes, ce nouveau médium a soutenu l'apparition d'un mode de consommation en ligne de par la prolifération de sites marchands et via la facilitation des achats en ligne (Newman & Clarke, 2003; James, 2005). Ces configurations entraînées par l'innovation procurée par l'internet ont permises à certains cyberdélinquants de se nourrir de nouvelles opportunités criminelles pour constituer, entre autres, le phénomène de carding.

Le carding se définit par « l'utilisation non autorisée d'informations financières liées à des cartes de crédit ou de débit pour acheter frauduleusement des biens ou des services » (Perretti, 2009). Bien que certains auteurs aient mis en évidence que ce type de fraude puisse être utilisé pour revendiquer des aspirations *hacktivistes* (Vasiu & Vasiu, 2015), une large majorité des

fraudeurs (appelés *carders*) a pour principale motivation l'appât de gains financiers ou matériels (Kshetre, 2010; Moore, Clayton & Anderson, 2009). Pour approfondir cette définition généraliste, il est important de mentionner que cette motivation peut s'exprimer à différents niveaux dans le cadre de cette fraude. En effet, la typologie en trois catégories proposée par Naylor (2003) pour définir les crimes motivés par les gains financiers confirme que le carding se place sous l'égide de ce type de crime. Néanmoins, étant donné que l'accomplissement de cet acte se décompose en une série d'étapes, chacune d'entre elles se rattache à l'une des trois catégories, à savoir : *predatory* pour le vol d'informations financières, *market-based* pour leurs reventes sur un marché en ligne et *commercial* pour l'utilisation frauduleuse des informations financières.

Dans un souci de présentation de ce phénomène, son ampleur sera illustrée au travers de trois différentes visions offertes par des milieux distincts. En effet, plusieurs domaines proposent d'étudier de près ou de loin l'ampleur de ce type de cybercriminalité en termes de pertes financières engendrées, de gains pour les délinquants ou encore de victimes touchées. Une partie de ces résultats émanent d'entités privées travaillant généralement dans le secteur de la sécurité informatique. Ainsi, on observe une croissance du nombre d'informations personnelles dérobées dans le cadre de failles dans les systèmes informatiques contenant ce type de données (Symantec, 2017). Bien entendu, une part importante de ces données personnelles concerne des données financières. De plus, on observe que, bien que le nombre de failles ait stagné, le nombre de données personnelles dérobées a quant à lui considérablement augmenté en passant de 536.8 millions en 2016 à près d'1.1 milliards en 2017 (Symantec, 2017). Ce constat coïncide avec la découverte faite par 4iQ à la fin 2017 qui mit à jour la présence d'1.4 milliards de données d'identification disponibles sur le Darknet. Dans le même registre, une croissance du nombre de victimes de fraudes à l'identité a été observée entre 2015 et 2016 ayant mené à des pertes annuelles évaluées 16 milliards de dollars (Javelin Strategy & Research, 2017). Cette observation se retranscrit bien au travers des nombreuses brèches évoquées dans les médias. À titre d'exemple, la chaîne de restauration rapide Sonic Drive-In a été victime en 2017 d'une seconde attaque ayant mené à la compromission de près de 5 millions de cartes de crédit ou débit (KrebsOnSecurity, 2017). Au-delà de la compromission des données personnelles des clients, ce type d'attaque engendre des conséquences néfastes sur la réputation de l'entreprise qui peut se traduire par une baisse significative du cours de ses actions en bourse (CompariTech,

2017). En moyenne, une victime ayant vu ses données bancaires compromises perd un montant de 722\$ (Ilyin, 2014).

Au niveau des instances publiques, les décisions rendues par le système de justice peuvent renseigner sur le degré de vigueur qu'accorde la société face à cette problématique. À l'automne 2017, les autorités américaines ont accusé 36 individus impliqués dans le forum de carding InFraud (Department of Justice, 2018¹). Les accusations ont mené à une évaluation des montants compromis par les participants qui pouvaient atteindre plusieurs centaines de millions de dollars. Néanmoins, il est peu probable que ces mêmes individus aient pu engendrer de telles sommes. En effet, chaque cour de justice est libre d'appliquer son propre calcul des montants compromis (Vasiu & Vasiu, 2015). Ainsi, pour assurer des peines plus sévères et vraisemblablement une plus forte dissuasion, il est possible que certaines d'entre elles majorent les montants compromis par les accusés. Quand bien même, ces constats permettent d'illustrer la forte répression envers le carding (Bylieva, Lobatyuk & Rubtsova, 2018). Il n'est donc pas étonnant de constater la portée des pertes mises à jour par diverses entités travaillant étroitement avec les législateurs. L'Australian Payments Network a observé une augmentation de 7,8% entre juillet 2017 et juin 2018 des fraudes liées aux paiements en ligne utilisant des cartes constituant désormais près de 85% des fraudes mobilisant des cartes bancaires pour un montant total compromis de 478 millions de dollars (AusPayNet, 2018) et Europol a mis à jour l'existence d'une organisation criminelle ayant compromis près 130,000 cartes de victimes provenant de 29 pays pour des pertes de 8 millions d'euros (Europol, 2017).

Il est important de préciser que les résultats de ces deux domaines doivent être pris avec prudence dans la mesure où ces derniers peuvent avoir une forme d'intérêt à grossir les traits de l'ampleur du phénomène ; en particulier les entreprises privées qui souhaitent accroître l'intérêt pour leurs produits (Dupont, 2014). Ainsi, l'emphase sera mise ici sur les résultats émis par les travaux universitaires. Franklin et ses collaborateurs (2007) ont étudié une salle de clavardage soutenant le phénomène de carding. Leurs résultats suggèrent que les montants générés sont comprise entre 37 et 93 millions de dollars sur une période de sept mois. La même année, Moore et Clayton (2007) ont montré que les pages de *phishing* pouvaient compromettre

¹ Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than \$530 Million in Losses from Cybercrimes, 2018. Repéré au: <https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible>

annuellement et minimalement près de 350 millions de dollars. En étudiant l'impact de logiciels malveillants, Holz, Engelberth et Freiling (2009) ont soutenu que la valeur d'un ensemble de données compromises sur une période de sept mois était comprise entre près de 800,000 et près de 16,6 millions de dollars. Dans un autre registre, Bulakh et Gupta (2015) ont soutenu que les revenus générés sur des marchés virtuels où s'échangent des données financières peuvent osciller entre près de 6,000 et 9,000 dollars par jour. Plus récemment, Holt, Smirnova et Chua (2016) ont proposé des estimations de revenus engendrés par les participants de 13 forums. Leurs résultats suggèrent que les vendeurs d'informations financières ont généré entre près d'un et 2 millions de dollars dépendamment du nombre de produits offerts et que les acheteurs peuvent avoir acquis entre plusieurs millions de dollars en monétisant ses informations financières.

1.2.2. LES CARACTERISTIQUES DES CARDERS

Le cybercrime en tant que nouvelle forme de criminalité peut mettre à mal les conceptions traditionnelles des délinquants. Bien que certains auteurs aient mentionné que les carders n'aient pas nécessairement besoin de disposer de connaissances techniques en informatique (Thomas & Martin, 2006; Franklin et al., 2007; Décary-Héту & Leppänen, 2013), d'autres recherches suggèrent tout de même qu'une majorité des cyberdélinquants se compose de jeunes relativement éduqués (Kshetri, 2006) et qu'il est nécessaire d'avoir certaines compétences pour participer aux activités marchandes (Décary-Héту, Mousseau & Vidal, 2018). Ce constat est appuyé par une étude qui mentionne que cette population se caractérise par une moyenne d'âge relativement jeune (30 ans) et est majoritairement composée d'hommes (77%) (Hutchings, 2014). Malgré tout, la démonstration de compétences techniques confère un avantage certain, car elle est un vecteur de crédibilité et de reconnaissance au sein des communautés de cyberdélinquants (Lusthaus, 2012).

Bien que l'on puisse douter de l'implication de groupes provenant crime organisé 'traditionnel' (Lusthaus, 2018), plusieurs recherches suggèrent que les carders constituent une forme de criminalité organisée (Sullivan, 2010). Cette forme d'organisation se traduit par une division du travail et la spécialisation de certains participants (Herley & Florêncio, 2010), par la capacité de mener des actions coordonnées (Wehinger, 2011) ou bien par la constitution d'un système

de messagerie sécurisé (Kirk, 2007a). Cette composante est aussi importante pour assurer une gestion de la confiance et tenir à l'écart les participants souhaitant frauder d'autres participants (Yip, Webber & Shadbolt, 2013), en ce sens que le fait de s'accorder avec d'autres délinquants favoriserait les apprentissages et le partage de connaissances (Hutchings, 2014, Kwon & Shakarian, 2018). De plus, une organisation peut conférer une plus grande adaptabilité aux communautés pour composer avec les mesures prises par les forces de l'ordre (Décary-Héту & Leppänen, 2013, Kwon & Shakarian, 2018). Néanmoins, cette organisation n'est pas conditionnelle à l'accomplissement de ce type de délinquance. En effet, certains fraudeurs peuvent opérer seuls et certains groupes n'opèrent pas en ligne (Hutchings, 2014). Ces caractéristiques auraient d'ailleurs comme bénéfice de réduire les risques de sanctions (Hutchings, 2014).

Cependant, il y a certains avantages à retirer d'une éventuelle association avec des co-délinquants au niveau individuel. En effet, le nombre de contacts est corrélé positivement avec le nombre de transactions (Motoyama et al., 2011). Ainsi, un réseau bien construit peut mener à plus d'opportunités criminelles et donc espérer de meilleurs revenus (Décary-Héту & Leppänen, 2013). Ce constat est d'ailleurs soutenu par les analyses de Lu et ses collaborateurs (2010) et de Yip et ses collègues (2012) qui précisent que les participants jouant le rôle d'intermédiaire sont plus rares et ont une position plus avantageuse. Ce constat fait d'ailleurs écho au fait qu'une minorité des vendeurs de données financières est responsable de la majorité des ventes sur les marchés en ligne (Motoyama et al., 2011) et qu'une majorité des participants a une présence éphémère au sein des communautés en ligne (Décary-Héту & Leppänen, 2013)

1.2.3. LE SCRIPT CRIMINEL DU CARDING

La théorie des scripts criminels (Cornish, 1994) affirme que les crimes ne sont pas des événements isolés et que ces derniers devraient être compris comme des actes faisant parti d'une séquence de plusieurs événements qui, mis ensemble, constituent un phénomène criminel. À titre d'exemple, le trafic d'automobiles volées peut se décomposer en différents actes (le vol, le maquillage, le recel, etc.) (Tremblay, Talon & Hurley, 2001). Bien que l'on puisse considérer une multitude de scripts du carding compte tenu de la malléabilité de cette théorie (Soudijn & Zegers, 2012), le carding fait lui aussi référence à une chaîne d'acteurs et de comportements qui se spécialisent dans le vol d'informations financières, dans la revente d'informations ou encore dans leur monétisation. Deux travaux ont mis en évidence des scripts criminels du carding. En

utilisant un échantillon de 25 tutoriaux de carding mis gratuitement en ligne sur des forums, Hardeveld, O'Hara et Webber (2016) ont séquencé le phénomène de carding en 6 étapes. Cependant, contrairement à la vision du script fourni par Hutchings et Holt (2014) résumée dans le tableau 3, Hardeveld, O'Hara et Webber (2016) n'ont pas inclus un acteur central, le vendeur, qui acquiert les données financières pour ensuite les vendre à d'autres. Cette omission s'explique par le fait que les données à leur disposition étaient des tutoriaux destinés à d'aspirants carders. Ainsi, dans un souci de présenter le phénomène de manière exhaustive nous aborderons le script criminel du carding tel qu'élaboré par Hutchings et Holt (2014). Cette approche nous permet de distinguer les différentes compétences nécessaires lors de chaque étape du script pour apprécier les différents types de carders qui composent cette chaîne d'acteurs.

Au cours de la première étape de *Préparation* les carders devront se doter d'un ensemble de comptes et de logiciels leur permettant de communiquer et d'échanger avec les mêmes moyens que ceux faisant consensus dans leur communauté. Tout d'abord, ils devront trouver le ou les marchés sur lesquels d'autres carders échangent des produits du carding². Ils devront ensuite se constituer une nouvelle identité au travers d'un pseudonyme (Soudijn & Zegers, 2012). Destiné à protéger leurs identités réelles, utiliser ce pseudonyme de manière constante assurera aux carders de maintenir leurs relations de confiance avec les autres (Lusthaus, 2012). Cette étape du script criminel soulève le paradoxe du pseudonymat. Bien qu'il fournisse une forme d'anonymat, il peut aussi mener à la possibilité d'être plus ciblé lorsqu'il bénéficie d'une forte réputation (Lusthaus, 2012).

Ainsi, pour faire pencher la balance en leurs faveurs, ces délinquants devront réduire la traçabilité de leurs activités en utilisant des technologies d'anonymat. Bien qu'une mauvaise utilisation de certaines d'entre elles puisse accroître les risques de victimisation, il existe un vaste choix de techniques et outils permettant une meilleure sécurité (Hardeveld, Webber & O'Hara, 2017). À titre d'exemple, les serveurs mandataires sont parmi les outils les plus plébiscités. Ils permettent d'éviter la détection en masquant l'adresse IP originale par une autre qui n'est pas reliée à leur identité (Décary-Héту & Leppänen, 2013; Hardeveld, Webber & O'Hara, 2017). Pour soutenir cette étape, des tutoriaux et discussions sont généralement

² Le fonctionnement et l'architecture de ces différents marchés sera détaillée dans la section suivante.

présents sur les marchés et assurent aux nouveaux venus du matériel à étudier pour leur permettre de comprendre et utiliser correctement ces outils (Yip, Webber & Shadbolt, 2013; Hardeveld, Webber & O'Hara, 2016; Hardeveld, Webber & O'Hara, 2017).

Tableau 3. Résumé du script criminel proposé par Hutchings et Holt (2015)

Étapes du script universel	Principaux résultats
1 - Préparation	Recherche des marchés ; Création de comptes ; Mesures concernant l'anonymat et la sécurité ; Apprentissage spécialisé
2 - Entrée	Apprentissage de la sous-culture
3 - Pré-condition	Obtention de produits (ex. : logiciels malveillants)
4 - Pré-condition instrumentale	Mise en marché de produits ou services ; Vérification des produits par les modérateurs
5 - Initiation instrumentale	Échange d'informations sur les forces de l'ordre ; Négociations
6 - Actualisation	Envoi ou réception du paiement
7 - Passage à l'acte	Emballage ou envoi électronique du produit
8 - Post-condition	Réputation ; Echanges de devises
9 - Sortie	Blanchiment de l'argent

C'est lors de l'étape de *Pré-condition*, que les informations financières sont dérobées. Les carders spécialisés dans cette étape peuvent mobiliser différentes techniques menant à des collectes quantitativement différentes. Tout d'abord, le vol ou l'extorsion peuvent permettre à obtenir des données financières (Sullivan, 2010; Patil & Dange, 2016). Néanmoins, ces actes ne revêtent pas la définition d'un cybercrime. Aucun moyen électronique ou technologique n'est obligatoirement nécessaire pour assurer la commission. Ainsi, nous développerons plus en détails les techniques relevant de cette définition qui, par la même, peuvent permettre aux délinquants de colliger un plus grand nombre d'informations.

Le *skimming* consiste à implémenter un dispositif électronique (un *skimmer*) capable de soustraire et d'enregistrer les informations d'une carte bancaire lorsque celle-ci est insérée dans un lecteur de carte (Peretti, 2008). Une petite caméra ou un clavier numérique permet d'obtenir

le code PIN de la carte. Ces dispositifs de skimmer sont offerts entre 1,200 et 5,000 dollars et demeurent réservés à un groupe restreint d'individus (Holt & Lampke, 2010). En effet, la mise en place d'un tel dispositif est difficile et risquée. Le criminel devra disposer de contacts et d'informations pour bénéficier d'un accès aux cartes et pourra, par exemple, soudoyer un employé pour installer l'appareil sur un guichet. Une autre forme de skimmer a récemment vu le jour et permet de transmettre plus rapidement l'information au carder en faisant appel au Bluetooth. En plaçant ce dispositif au sein d'un système de paiement, le carder pourra recevoir sur son smartphone toutes les informations d'une carte qui a été glissée dans le lecteur ainsi que les informations tapées sur le clavier numérique grâce à une communication en Bluetooth émise par le dispositif (Jensen, Gouda et Qiu, 2016; Mehrnezhad et al., 2016).

Le *phishing* a été défini par Lastdrager (2014) comme « [a] scalable act of deception whereby impersonation is used to obtain information from a target ». Dans le cadre du carding, le phishing est l'envoi d'un faux courriel d'une institution bancaire demandant à la victime un certain nombre d'informations personnelles. Cette dernière sera priée de cliquer sur un lien hypertexte conduisant à un faux site de la banque (Holt & Bossler, 2016). Une fois sur le site, la victime est invitée à y inscrire son nom d'utilisateur et son mot de passe. Ces informations seront consignées sur le serveur hébergeant le site web frauduleux et demeureront à la disposition du carder (James, 2005; Wall, 2007).

Une autre technique consiste à mobiliser des *logiciels malveillants* pour extraire des données financières et personnelles en infectant l'ordinateur de la victime. Ces logiciels malveillants peuvent se spécialiser dans l'extraction de données financières comme les identifiants de connexions à des comptes bancaires en ligne (Symantec, 2017) ou de *keyloggers* qui permettent d'intercepter les frappes entrées sur le clavier de l'utilisateur (Holz, Engelberth & Freiling, 2009; Europol, 2015). Dans un registre similaire, l'*infection de points de ventes* s'attaque directement à des terminaux de paiements présentant des failles sécuritaires (Bulakh & Gupta, 2015). Ce logiciel extrait les informations sensibles des clients transitant par la mémoire vive du système de paiement (Vasiu & Vasiu, 2015). Cette technique peut permettre de récolter un grand nombre de données, car les points de ventes sont en général reliés au système financier central du magasin dont ils dépendent (Sullivan, 2010; Symantec, 2015). Des exemples récents d'infections de points de ventes ont démontré que cette technique pouvait mener à la compromission des informations bancaires de dizaines de millions de victimes (Green & Stavins, 2016; Chakraborty et al., 2016; Kashmiri, Nicol et Hsu, 2016; Manworren, Letwat et

Daily, 2016; Ferell, 2016).

Finalement, nous mentionnerons les cas de *data breach* définis comme « un incident dans lequel des données sont dérobées ou supprimées par un tiers n'ayant pas reçu l'autorisation d'accéder à ce contenu » (Sherstobitoff, 2008). Ce type d'attaque peut mener à la compromission d'un nombre considérable de données personnelles et financières de clients et s'opère principalement lorsque les bases de données contenant ses informations n'ont pas vu leurs remparts sécuritaires mis à jour.

Il est intéressant de mentionner que les concepteurs de ces logiciels malveillants peuvent être réticents à les utiliser eux-mêmes et préférer les vendre pour plusieurs centaines de dollars à d'autres carders qui ont les compétences de les utiliser (Holt & Lampke, 2010). Cela leur permet de tirer un bénéfice plus marginal que s'ils les avaient utilisés, mais réduit aussi leur sentiment de culpabilité car ils ne sont pas à l'origine de l'infection (Brenner, 2008). Cela peut aussi s'expliquer par le fait que les carders qui dérobent des informations financières sont peu intéressés ou peu efficaces pour monétiser les informations qu'ils collectent (Dupont, 2012). Ainsi, une fois les données collectées, ces types de carders peuvent les mettre en vente sur des lieux de convergence en ligne lors de l'étape de *Pré-Condition instrumentale* (Perretti, 2009) pour que d'autres fraudeurs spécialisés dans l'achat et la monétisation des données puissent les acheter. Bien qu'une foule de produits et de services, reliés ou pas au carding, peuvent aussi être vendus sur les mêmes plateformes en ligne (Sullivan, 2010), nous nous concentrerons sur les produits phares du carding émanant de l'étape précédente. Différents produits sont disponibles en fonction de la quantité d'informations qu'ils fournissent (Wehinger, 2010).

Les *dumps* contiennent les informations nécessaires à la contrefaçon d'une carte. Il s'agit des données présentes sur la bande magnétique d'une carte soit le numéro de la carte, le nom et le prénom du détenteur, le mois et l'année d'expiration, les chiffres composant le cryptogramme visuel et une suite numérique relative à l'institution émettrice (Peretti, 2008; Holt & Lampke, 2010). Selon certains auteurs, ce type de produit est le plus populaire sur les marchés (Thomas & Martin, 2006; Franklin et al., 2007; Du et al., 2018) avec un prix moyen de 56\$ (Holt & Lampke, 2010). D'autres auteurs stipulent que les dumps ont perdu en popularité et se vendent relativement moins chers (Haslebacher, Onalopo & Stringhini, 2016). Cette absence de consensus s'illustre bien au travers des fortes variations de prix en fonction de la qualité des produits (Holt & Lampke, 2010). Il est à noter qu'en plus de cet achat, des coûts annexes devront être ajoutés pour pouvoir extraire l'argent de ses données. En effet, pour constituer une

carte de contrefaçon il est nécessaire de disposer de cartes vierges, d'appareil permettant l'impression des données contenues dans le dumps ou encore d'hologrammes pouvant ajouter quelques centaines de dollars supplémentaires (Mativat & Tremblay, 1997; Bulakh & Gupta, 2015).

Les *fullz* (diminutif de « *full information* ») contiennent des informations bancaires et personnelles des victimes. Ils incluent le nom complet de la victime, son adresse postale, son numéro de téléphone, son numéro d'assurance sociale, son numéro de carte bancaire, la date d'expiration de la carte, un historique de crédit, le nom de jeune de fille de la victime et sa date de naissance (Peretti, 2009; Holt & Lampke, 2010). Les *fullz* sont avant tout utilisés pour faire des achats frauduleux en ligne. Selon certaines études, ces produits se vendent en moyenne moins chère que les dumps (46\$) avec une variation de prix plus limitée (entre 5\$ et 260\$) (Holt & Lampke, 2010).

Le *credit card verification value* (CVV ou CVV2) est une version plus réduite du *fullz* et ne contient que le nom de la victime, son adresse postale, son adresse courriel, le numéro de la carte, la date d'expiration et les chiffres composant le cryptogramme visuel (Holt & Lampke, 2010). Les CVV sont utilisés pour faire des achats en ligne (Clarke & Newman, 2003; Peretti, 2009; Hutchings & Holt, 2014) et se vendent en moyenne encore moins chers, soit 3\$ l'unité selon Holt et Lampke (2010) avec une variation allant de 1\$ à 14\$. Ces résultats sont cependant différents d'observations récentes qui stipulent que les CVVs se vendent en moyenne pour une dizaine de dollars (Haslebacher, Onaolopo & Stringhini, 2016). Finalement, les *comptes en ligne* qui comportent les identifiants de connexion pour accéder à un compte bancaire en ligne ou PayPal par exemple (Holt & Lampke, 2010). Comme pour les précédents produits, le prix est peu élevé (environ \$10) et fluctue de \$4 à \$50 en fonction du solde et qualité des informations fournies (Holt & Lampke, 2010), bien que d'autres auteurs aient suggéré que ce type de produit soit plus cher (Perretti, 2009).

De manière générale, il est relativement difficile d'avoir des estimations constantes des prix des produits qui fluctuent dépendamment de leur fraîcheur, des montants pouvant être retiré, de leur pays de provenance, de la taille du lot ou même d'éventuelles réductions offertes par les vendeurs (Holt & Lampke, 2010; Herley & Florêncio, 2010; Haslebacher, Onaolope & Stringhini, 2016). De plus, ce processus de mise en vente des produits n'est pas accessible à n'importe quel participant. En effet, certains lieux de convergence ne rendent accessible la section des ventes qu'aux membres ayant fait preuve d'une activité soutenue et qui sont intégrés

dans communauté (Motoyama et al., 2011; Décary-Héту & Leppänen, 2013). Si tel est le cas, les carders qui vendent les données devront fournir des détails sur leurs offres en précisant, par exemple, les modalités de paiement, la description du ou des produits offerts ainsi que ses coordonnées pour être contacté par messagerie privée.

Une fois les produits mis en vente sur les lieux de convergence virtuels ils feront l'objet d'une vérification par l'équipe administratrice pour assurer leur bonne qualité. Cette vérification prendra la forme d'évaluations qui seront par la suite visibles par l'ensemble de la communauté (Holt & Lampke, 2010; Holt et al., 2015). Ce processus peut prendre plusieurs jours avant d'être avalisé par un vérificateur et le refus d'obtempérer à une vérification peut mener à une exclusion (Hutchings & Holt, 2014).

Avant de se lancer dans une transaction les participants vont se renseigner les risques que comportent leurs activités frauduleuses et négocier avec les vendeurs lors de l'étape de l'*Initiation instrumentale*. Ce comportement peut se traduire par l'actualisation des cas d'arrestations ou de disparitions soudaines de membres anciennement actifs (Hutchings & Holt, 2014). La littérature a mis en évidence que lorsqu'un acheteur déclare son intérêt pour un produit des négociations peuvent prendre place entre ce dernier et celui qui le vend. Faisant écho aux facteurs dynamisant les fluctuations des prix des produits, les négociations prennent place lors de discussions privées n'impliquant que les deux parties (Franklin et al., 2007; Motoyama et al., 2010).

Quand une entente a été trouvée, les deux parties vont pouvoir s'envoyer leurs dus lors de l'étape de l'*Actualisation instrumentale*. Différents moyens de paiements ont été mis à jour dans la littérature. Les plus utilisés demeurent les moyens de paiements électroniques permettant des transferts rapides (Wehinger, 2011). Certaines recherches ont souligné l'utilisation de Western Union, Liberty Reserve, Web Money, e-Gold, Yandex, et PayPal (Franklin et al., 2007; Holt & Lampke, 2009; Motoyama et al., 2013; Holt & Smirnova, 2014; Holt et al., 2015). Bien que d'autres recherches suggèrent que leurs utilisations soient rares dans le cadre du carding (Mikhaylov & Frank, 2016), il n'existe pas de consensus à savoir si les cryptomonnaies sont couramment utilisées (Portnoff et al., 2017). Néanmoins, ces dernières peuvent constituer un moyen de paiement très apprécié des cyberdélinquants en raison de leurs vertus sécuritaires (Aldridge & Décary-Héту, 2014). Étant donné les risques inhérents de victimisation endogène entre délinquants (et plus particulièrement dans le cadre de la cybercriminalité où les

délinquants n'ont pas nécessairement à entrer en contact physique), les carders désirant acheter des produits peuvent faire appel au service d'un *courtier financier* (Lusthaus, 2018). Moyennant un coût supplémentaire à la transaction, ce service d'intermédiaire permettra de vérifier la qualité du produit avant de le transmettre à l'acheteur et d'envoyer son paiement au vendeur (Herley & Florêncio, 2010; Aldridge & Décary-Hétu, 2014; Holt et al., 2015). Cependant, ce moyen n'est pas infaillible, car cet intermédiaire peut dérober les dus des deux parties pour en tirer bénéfice (Hutchings & Holt, 2014; Barratt & Aldridge, 2016).

Le vendeur disposera de différents moyens pour envoyer son dû à l'acheteur lors de l'étape du *Passage à l'acte*. Bien que la majorité des produits revêtent un caractère virtuel, l'utilisation de dumps nécessite des équipements spécifiques pour permettre l'utilisation des données (Mativat & Tremblay, 1997). Les carders doivent donc mobiliser des techniques permettant de faire transiger du matériel physique. Par exemple, ils peuvent s'échanger des colis de matériel illégal en profitant de l'effervescence des périodes de fêtes pour tenter d'éviter la détection (Hutchings & Holt, 2014). Dans d'autres cas, les acheteurs peuvent faire appel à d'entreprises privées opérant dans un cadre légal gris (Thomas & Martin, 2006). Ce type de service permet de contourner les mécanismes de protection de plusieurs sites qui refusent de livrer des colis en dehors de certains pays occidentaux, mais peut être assez dispendieux et exiger des frais allant jusqu'à 50% de la valeur du bien envoyé (Thomas & Martin, 2006). Certains carders préfèrent alors plutôt faire livrer leurs colis dans des maisons abandonnées ou chez des individus qui acceptent de servir de point de livraison (Hutchings & Holt, 2014).

Concernant les envois de produits virtuels, les transferts de marchandises peuvent s'opérer grâce à des moyens de communication privée. À titre d'exemple, le système de communication cryptographique *Pretty Good Privacy* (PGP) permet aux utilisateurs de communiquer entre eux sans crainte que leurs échanges soient interceptés et surveillés. De plus, la nature virtuelle des produits permet un envoi et une réception rapide (Franklin et al., 2007; Herley & Florêncio, 2010; Holt & Lampke, 2010).

Lors de l'étape de *Post-condition*, et une fois le produit reçu, l'acheteur est en mesure d'en vérifier la qualité s'il n'est pas passé par un *courtier financier*. Cette vérification peut se faire par l'entremise d'un don minime à une association caritative (par exemple \$1) pour s'assurer que les données sont utilisables (Franklin et al., 2007). Si la carte n'est pas fonctionnelle, certains vendeurs offrent un service après-vente en proposant de remplacer le produit

(Hutchings & Holt, 2015). Ce service permet aux vendeurs de gérer leur réputation afin de conserver leurs clients et d'en attirer de nouveaux. Par la suite, les acheteurs posteront des évaluations positives ou négatives quant à la qualité du service fourni. Ce mécanisme est essentiel à la constitution d'un système de réputation et de confiance (Holt, 2013a; Cherqi et al., 2018). De plus, il permet d'améliorer l'identification des vendeurs malhonnêtes qui pourront être tenus à l'écart des marchés (Hutchings & Holt, 2015).

Lorsque les produits achetés sont de bonne qualité, les acheteurs vont pouvoir les utiliser afin d'en extraire l'argent. Pour monétiser les informations financières, les carders ayant acheté des produits peuvent utiliser deux stratégies. Le *carding en magasin* consiste à utiliser une fausse carte bancaire ou de crédit pour faire des achats dans un magasin physique (Sullivan, 2010; DeFilippi & Michael, 2016). Cette stratégie implique la présence physique du carder dans le magasin et la capacité à produire des cartes de contrefaçon à partir de dumps. Les carders achèteront des biens ou des cartes cadeaux qu'ils revendront par la suite à plus bas prix (Peretti, 2009; Hardeveld, Webber et O'Hara, 2016). Le caractère anonyme des cartes cadeaux est à la fois apprécié par les carders qui évitent toute traçabilité, mais aussi à l'acheteur potentiel qui pourra effectuer des achats à moindre coûts (Pastrana et al., 2018).

La seconde stratégie de monétisation est le *carding en ligne* (Sullivan, 2010). Cette stratégie fait référence à l'achat de biens et services en ligne et nécessite l'utilisation de fullz ou de CVV. Il n'existe pas de consensus à savoir si les grands sites, dans lesquels il est plus facile de passer inaperçu, reçoivent plus de commandes des carders (Hardeveld, Webber et O'Hara, 2016). En effet, les grands sites disposent souvent de systèmes de paiement plus sécuritaires en utilisant, entre autres, les services de validation d'identité de Visa et MasterCard. De plus petits détaillants en ligne peuvent donc être pris pour cibles, mais il est alors plus facile de détecter une activité frauduleuse et le choix de biens proposés peut être moins étendu. Lorsque des biens physiques sont achetés, les carders peuvent à nouveau faire appel aux stratégies d'envoi physique mentionnées lors de l'étape du *Passage à l'acte*.

Finalement, lors de la dernière étape *Sortie*, Hutchings et Holt (2015) stipulent que peu de discussions évoquent les moyens pour blanchir l'argent du carding, bien que certains participants proposent des services de blanchiment en prenant un pourcentage d'autant plus élevé que le montant à blanchir est bas.

1.2.4. ÉVOLUTION DES LIEUX DE CONVERGENCES

Le carding nécessite l'implication de toute une chaîne d'acteurs. L'organisation de la collaboration entre ces acteurs repose sur des lieux de convergence où les activités de carding peuvent être discutées et où des produits et services illicites sont offerts et achetés (Leukfeldt, 2014; Caines et al., 2018). Depuis les années 1990, ces lieux de convergence ont pris la forme de forums de discussion sur internet et de salles de clavardage sur l'*Internet Relay Chat* (IRC). Au cours des 5 dernières années, une nouvelle génération de marchés illicites en ligne a vu le jour de par le réseau Tor (Martin, 2014). Cette section décrit le fonctionnement de ces deux générations de lieux de convergences en précisant le rôle des acteurs clefs qui régulent et soutiennent ces marchés. Nous observerons dans quelles mesures les marchés de la seconde génération améliorent le socle structurel sur lequel s'étaient reposés les marchés de première génération.

L'IRC est un service de messagerie instantanée qui permet à ses utilisateurs de s'échanger des messages en temps réel au travers de conversations publiques ou privées (Décary-Hétu & Dupont, 2012; Bernard et al., 2018). L'IRC est divisé en centaines de serveurs qui hébergent chacun un très grand nombre de salles de clavardages avec chacune son propre sujet de discussion et ses propres règles de participation (Franklin et al., 2007). L'IRC a facilité l'émergence d'un véritable réseau social entre les carders en favorisant leurs rencontres et en proposant un espace où les vendeurs peuvent placer des annonces pour leurs produits et services illicites en lien avec le carding (Thomas & Martin, 2006). Des applications comme ICQ ou Telegram proposent un service similaire tout en encryptant les communications les rendant très prisées par les carders (Holt & Lampke, 2010; Yip, Shadbolt et Webber, 2013)

Les forums de discussions constituent un autre type plateforme virtuelle où des utilisateurs peuvent converser sur divers sujets. Les forums sont divisés en fils de discussion ; chaque fil de discussion peut à son tour héberger un grand nombre de discussions (Holt, 2007; Holt & Lampke, 2010; Motoyama et al., 2011). Contrairement à l'IRC, les discussions sur les forums sont asynchrones; tous les acteurs ne doivent donc pas être en ligne en même temps pour pouvoir participer aux conversations (Yip, Webber & Shadbolt, 2013). Ceux-ci peuvent plutôt consulter une archive de tous les messages publics lorsqu'ils se reconnectent à nouveau au forum. Les forums possèdent aussi une messagerie privée pour permettre aux utilisateurs d'échanger sans être visibles du reste des participants (Yip et al., 2013). Dans le cadre du

carding, les forums servent de lieux de convergence en ce sens qu'ils fournissent un support social aux carders et forment de véritables lieux de marchandage (Décary-Héту & Leppänen, 2013; Yip et al., 2013), et ce dans de nombreux langages (Motoyama et al., 2011; Haslebacher, Onaolopo & Stringhini, 2016). Au-delà d'être des marchés, les forums sont aussi des communautés organisées autour de normes et de valeurs (Jordan & Taylor, 1998; Motoyama et al., 2011; Afroz et al., 2013) qui jouent un rôle de facilitateur pour les activités des carders (Yip, Shadbolt et Webber, 2010).

Les acteurs qui prennent place sur les marchés se distinguent de par les rôles et les statuts qu'ils occupent. Yip, Shadbolt et Webber (2010) indiquent que les acteurs peuvent jouer différents rôles qui ne sont pas mutuellement exclusifs (Franklin et al., 2007; Holt, 2013). Au sommet de la pyramide se trouvent les *administrateurs* et les *modérateurs* dont la fonction est d'assurer la gestion globale des forums (Dupont et al. 2016). Cela passe par la mise à l'écart de participants ne respectant pas les règles, en se positionnant comme *courtier financier* pour faciliter les transactions entre les participants ou encore en tant que *vérificateur* des produits (Holt et al., 2015).

S'ajoutent à cela les *évaluateurs* qui sont responsables du système de réputation des *vendeurs*. Ceux-ci peuvent, à n'importe quel moment, exiger un échantillon de la marchandise d'un vendeur pour en tester l'authenticité et la qualité, et ainsi fournir une évaluation de son contenu pour conférer un statut spécial au vendeur (Lusthaus, 2018). Finalement, le dernier type d'acteur est le *membre régulier*. Celui-ci peut être aussi bien un acheteur qu'un vendeur, mais ne bénéficie pas du sceau de confiance attribué par les évaluateurs. Décary-Héту et Eudes (2015) rajoutent à cette typologie un sixième rôle : le *courtier financier*. Ces acteurs se positionnent comme des intermédiaires très prisés par les acheteurs, car ils constituent un moyen important de lutte contre la victimisation. L'IRC s'appuie aussi sur une structure semblable.

Les forums et l'IRC ont tout pour fournir à leurs utilisateurs des lieux de convergence efficaces pour échanger et vendre des données financières (Franklin et al., 2007; Fallman, Wondracek et Platzer, 2010). Le système d'enregistrement de compte permet aux utilisateurs de masquer leurs identités réelles et de créer autour d'un pseudonyme un vrai réseau de relations marchandes qu'ils pourront entretenir sur différentes plateformes (Franklin et al., 2007; Lusthaus, 2018; Pastrana et al., 2018). De plus, l'inscription peut se faire exclusivement grâce une invitation ou au parrainage d'un membre déjà établi pour éviter que des indésirables n'arrivent à s'inscrire

(Holt, 2007; Markham, 2011; Holt & Dupont, 2018; Lusthaus, 2018b). Les utilisateurs inscrits ont ainsi accès à un vaste bassin de contacts potentiels et peuvent aisément transiger avec des acteurs dont l'historique de transactions est conservé dans les archives. Évidemment, les participants peuvent à tout moment changer de pseudonyme et ainsi se dissocier de leur mauvaise réputation (Lusthaus, 2018). Il semble d'ailleurs que cela soit relativement fréquent (Décary-Héту & Dupont, 2012). Ce type de comportement est associé aux *rippers* (Herley & Florêncio, 2010). Ces derniers arnaquent les autres en fournissant des produits de mauvaise qualité ou en ne livrant pas la marchandise après avoir été payés (Motoyama et al., 2010). Ce type d'acteur est le principal problème qui affecte les marchés illicites en ligne (Herley & Florêncio, 2010) et pour les combattre, les administrateurs et les modérateurs ont développé diverses techniques. Parmi elles, nous retrouvons, comme expliqué précédemment, le système de vérification de la marchandise qui peut tout aussi bien se faire de manière sporadique ou systématique (Décary- Héту & Leppänen, 2013; Holt & Lampke, 2010). Une autre technique consiste à exiger un paiement avant de pouvoir annoncer ses produits et services en ligne afin d'augmenter les coûts liés à cette victimisation endogène (Hutchings & Holt, 2014). Ainsi, un vendeur qui voudrait blanchir sa réputation devrait à nouveau déboursier des frais d'inscription.

Malgré ces dispositions, les travaux d'Harley et Florêncio (2010) relèvent que les *rippers* amènent l'imposition d'une taxe sur toutes les ventes. Les marchés illicites en ligne devraient ainsi être considérés comme des marchés de tacos (Akerlof, 1970). Sur certains marchés, où il est impossible d'attester de la qualité des produits vendus, les acheteurs ne voudront effectivement pas payer un prix élevé pour un produit étant donné le risque de tomber sur un bien de mauvaise qualité. Les vendeurs proposant des produits de bonne qualité n'auront d'autre choix que de quitter le marché ou bien de vendre leur marchandise à bas prix. À terme, les bons vendeurs se retrouveront mis sur la touche et le marché sera saturé en biens de piètre qualité. Malgré cette constatation, une étude récente a permis de nuancer les propositions d'Herley et Florêncio (2010). En effet, dans le cadre du désavantage que peut représenter le système d'enregistrement (qui peut conduire les fraudeurs à se recréer une identité), Décary-Héту & Eudes (2015) ont montré que peu de participants utilisent cette stratégie et que les modérateurs semblent contrôler correctement la régulation de leurs plateformes.

Finalement, nous pouvons dire qu'il n'y a pas de réel consensus sur le fait que les lieux de convergences de première génération soient ou non efficaces pour supporter des marchés illicites en ligne. Alors que certains auteurs ont suggéré que les marchés soutenus sur l'IRC

pouvaient être des lieux de convergences efficaces (Franklin et al., 2007; Fallman, Wondracek et Platzer, 2010), d'autres ont postulé que le risque de victimisation endogène en faisait des lieux trop risqués pour supporter des marchés illicites en ligne (Herley & Florêncio, 2010). L'équilibre entre les avantages et les désavantages de ces plateformes est un phénomène subtil à saisir étant donné la variété de forums et de salle de clavardage qui ont émergées pour soutenir le phénomène de carding. Il est aussi important de noter que ces types de lieux de convergence ne sont pas les seuls où les carders s'organisent et échangent. En effet, les réseaux sociaux traditionnels comme Facebook hébergent aussi d'importantes communautés de carders qui, malgré les dispositions prises par les équipes administratrices, restent relativement résilientes en se recomposant rapidement (KrebsOnSecurity, 2019). Néanmoins, nous verrons dans la partie suivante que ce sont les lieux de convergence décrits plus tôt qui ont posé la base pour assurer leur propre mutation vers des plateformes plus élaborées.

Un darknet se réfère à un réseau encrypté dont le but est d'assurer l'anonymat de ses utilisateurs. En effet, ce réseau de proxies semi-décentralisé permet à ces utilisateurs d'établir une connexion avec un site web en passant par différents nœuds du réseau qui mobiliseront différentes adresses IP rendant ainsi difficile l'identification de la personne ayant fait une requête sur le réseau (Christin, 2013; van Buskirk et al., 2016). Ce type de réseau a largement attiré des individus désirant faire des activités criminelles (Bancroft & Reid, 2015; Dong et al., 2018). Bien que le réseau Tor soit le plus populaire, d'autres logiciels permettent d'accéder à d'autres darknets, comme l'*Invisible Internet Project* (I2P) (Kwon & Shakarian, 2018). Ce type de réseau est connu pour notamment faciliter divers types d'activités criminels mais permet aussi à d'assurer la liberté d'expression en offrant un espace virtuel loin de tout contrôle étatique. Dans le cadre de cette section, nous nous pencherons plus en détail sur les types de lieux de convergence soutenant des marchés de carding qui ont pris place et ont émergé de concert avec l'apparition de ce type de réseau.

Autant présents sur l'internet traditionnel que sur le darknet, les *carding shops* opèrent en tant que marché virtuel pour les carders désirant vendre des données financières (Benjamin et al., 2015). En proposant un système convivial (création de compte, moteur de recherche pour les produits, navigation par catégories, utilisation de cryptomonnaies), les cardings shops se distinguent par le fait qu'ils sont spécialisés dans la vente de produits relatifs à la fraude financière en ligne (Bulakh & Gupta, 2015; Smirnova & Holt, 2017). Ils permettent à un carder, ayant une bonne réputation sur les autres types de lieux de convergences, de canaliser ses offres

sur son propre site et ainsi de réduire grandement les interactions entre vendeurs et acheteurs grâce à un système de commande automatisé (Europol, 2017).

L'utilisation du darknet a permis aux cyberdélinquants de bénéficier d'un nouveau type de lieux de convergence amenant innovation et sophistication aux marchés illicites en ligne. Appelé *cryptomarché*, ce type de lieu de convergence a été conçu par Ross W. Ulbricht (Olson, 2013) et sa plateforme *Silk Road* (SR1). Lancé en février 2011, SR1 visait principalement la vente de drogues illicites, mais facilitait aussi la vente de produits licites comme des vêtements et du matériel informatique (Devine, Egger-Sider et Rojas, 2015). Cette innovation criminelle a su profiter de l'émergence du réseau Tor ainsi que des cryptomonnaies comme le Bitcoin, permettant à la fois aux délinquants de bénéficier d'un anonymat de leurs activités et de leurs transactions (Barratt & Aldridge, 2016, Penny, 2016). Ces caractéristiques ont d'ailleurs permis aux cryptomarchés d'être relativement résilients face aux opérations policières (Soska & Christin, 2015). Le fonctionnement et la facture visuelle des cryptomarchés sont très largement inspirés des grands sites marchands comme eBay et Amazon (Broséus et al., 2016; Décary-Héту & Giommoni, 2016). Un système automatisé de réputation permet aux acheteurs d'évaluer l'expérience et la fiabilité des vendeurs. En cas de conflit, les acheteurs peuvent demander réparation aux administrateurs. Ces derniers jouent un rôle important dans les conflits, car la plupart des paiements doivent transiter par eux étant donné qu'ils jouent aussi le rôle de *courtier financier* (Christin, 2013). En forçant les acteurs à utiliser leurs services, les administrateurs se garantissent des commissions importantes et peuvent poser des garanties sur le niveau de service des vendeurs. Les cryptomarchés fournissent un environnement relativement sécuritaire pour leurs membres et il n'est donc pas étonnant d'observer croître leur popularité (Custer, Pool & Cornelisse, 2018; Décary-Héту, Mousseau & Vidal, 2018)

1.3. PROBLEMATIQUE

Le carding représente un phénomène inquiétant qui engendre d'importantes pertes monétaires. Il est donc important d'en approfondir la compréhension et d'en accroître les connaissances. Cependant, malgré le caractère alarmiste des chiffres émis par les entreprises privées et le système de justice, ces dernières restent empreintes de limites. En effet, les entreprises privées peuvent tourner à leur avantage les chiffres émis afin de grossir les traits de la menace pour augmenter leur bassin de clients. Cette volonté se traduit d'ailleurs par le fait qu'elles ne soient pas transparentes avec leur méthodologie (Leukfeldt, 2015). Ce manque de consistance

méthodologique est aussi valable pour les chiffres émanant du système de justice dans la mesure où chaque court est libre d'appliquer son propre calcul des dommages causés par les carders (Vasiu & Vasiu, 2015). Ajouté à cela le fait que le système de justice puisse vouloir grossir les traits des dommages causés afin d'augmenter les sanctions pénales et ainsi de renforcer la dissuasion, il demeure important d'accorder d'avantages de crédit aux travaux académiques pour avoir une meilleure idée de l'ampleur du phénomène et plus particulièrement ici, de la réussite criminelle des carders.

Cependant, l'étude de la réussite criminelle des carders demeure relativement peu explorée et il est important de combler ce manque de connaissances. À ce jour, deux études ont étudié ce cybercrime sous le prisme de la réussite criminelle (Décary-Héту & Leppänen, 2013; Holt, Smirnova & Chua, 2016). En analysant les réseaux criminels Décary-Héту et Leppänen (2013) ont permis de mettre à jour l'application de la théorie des signaux de Gambetta (2009) dans un contexte de communautés de carders. Cependant, ce travail s'est intéressé exclusivement à la dimension d'accès à des opportunités criminelles et non pas aux revenus illégitimes. Ainsi, il est nécessaire d'interroger cette dimension clef de la réussite criminelle car le carding est un cybercrime orienté vers l'appât du gain (Naylor, 2003). Sur ce sujet, Holt, Smirnova et Chua (2016) ont estimé les revenus et les profits générés par les carders sur des forums. En s'intéressant à 1,889 fils de discussions provenant de 13 forums accessibles via l'internet traditionnel, leurs résultats suggèrent que les vendeurs ont généré entre 1 et 2 millions de dollars dépendamment du nombre de produits offerts dans les lots vendus et du fait que les acheteurs peuvent avoir acquis entre plusieurs millions de dollars en les monétisant. En effet, fonction du type de forums sur lesquels les ventes prennent place et de la quantité et la qualité des produits, les vendeurs peuvent espérer gagner des sommes allant jusqu'au million de dollars. Néanmoins, leurs résultats peuvent être sujets à critiques et nous permettent d'évoquer deux principales limites inhérentes à leur méthodologie.

Dans un premier temps, ces auteurs se sont concentrés uniquement sur des forums de discussions accessibles via l'internet traditionnel alors que beaucoup de cyberdélinquants ont transposé leurs activités sur le réseau Tor pour bénéficier d'une meilleure sécurité. Ce constat peut d'ailleurs très bien s'illustrer par l'apparition récente d'une seconde génération de lieux de convergence exclusivement basés sur ce réseau (Aldridge & Décary-Héту, 2014; Décary-Héту & Giommoni, 2016). Entre autres, il est aussi important de noter qu'il existe des différences

entre les forums quant à leur degré d'insularité (Haslebacher, Onaolopo & Stringhini, 2016). Exit le fait que ces derniers prennent place sur le réseau Tor ou l'internet traditionnel, certains d'entre eux sont plus ou moins ouverts et contingentent ainsi la qualité des participants pouvant accéder à leur communauté (Holt, 2007; Markham, 2011; Holt & Dupont, 2018; Lusthaus, 2018). Bien que cette différence puisse être négligeable lorsque l'on s'intéresse à ces communautés d'un point de vue structurel (Holt et al., 2015), elle peut mener à des différences échantillonales lorsque l'on se questionne sur la réussite criminelle de ces participants. En effet, les marchés dont les inscriptions sont ouvertes au public peuvent attirer des participants désireux d'arnaquer les autres (Franklin et al., 2007; Herley & Florêncio, 2010). Ainsi, l'utilisation de forums ouverts peut mener à échantillonnage limité lorsque l'on s'intéresse à la réussite criminelle des carders dans la mesure où ceux-ci ne sont pas les seuls représentants du phénomène. Cette hypothèse est d'ailleurs appuyée par les travaux de certains auteurs qui stipulent que ces marchés ne sont pas viables car ces fraudeurs de fraudeurs y pulluleraient. Appelés *rippers*, ces vendeurs vont fournir aux acheteurs des produits de mauvaise qualité (des comptes bancaires expirés par exemple) ou ne rien fournir du tout après avoir été payés (Herley & Florêncio, 2010; Motoyama et al., 2010). Ainsi, une première limite relève de limites méthodologiques liées à l'échantillon.

La seconde limite identifiée, quant à elle, se réfère à la manière dont les revenus des carders ont été évalués. Les travaux ayant tenté de fournir un estimé des revenus criminels des carders utilisaient principalement deux indices pour le calculer : le prix ainsi que le nombre d'évaluations reçues par le vendeur (Holt, Smirnova & Chua, 2016). La difficulté pour rendre un estimé des revenus fiables repose principalement sur deux problèmes reliés à ces éléments. Tout d'abord, l'utilisation des prix des produits peut souffrir de certains problèmes dans la mesure où le prix affiché sur une annonce ne reflète pas le prix final. En effet, il a été vu que des processus de négociations prenaient place lors des transactions (Holt & Lampke, 2010; Motoyama et al., 2010; Holt, 2013b; Holt & Smirnova, 2014). De plus, la présence de certains intermédiaires qui s'assurent de la qualité des produits (comme les *courtiers financiers*) vient aussi enlever une part du revenu potentiel (Holt & Lampke, 2010; Holt et al., 2015; Holt, Smirnova & Hutchings, 2016; Leukfeldt, Kleemans & Stol, 2017). À cela peut s'ajouter le fait que des réductions peuvent être offertes lorsqu'un acheteur souhaite acquérir un grand nombre de produits (Franklin et al., 2007; Herley & Florêncio, 2010; Holt & Lampke, 2010; Holt,

2013a). Ainsi, l'utilisation des prix affichés par les vendeurs ne peut refléter le prix final qui sera déboursé par l'acheteur et rétribué au vendeur.

La seconde sous-limite se réfère aux évaluations. Les évaluations peuvent être laissées par les acheteurs lorsque ces derniers viennent d'entériner une transaction. Elles constituent l'une des pierres angulaires qui soutiennent les systèmes de confiance et de réputation essentiels à ces communautés en ligne (Holt & Lampke, 2010; Holt, 2013a; Décary-Héту & Laferrière, 2015; Holt et al., 2015; Haslebacher, Onaolopo & Stringhini, 2016; Holt, Smirnova & Hutchings, 2016). Les calculs précédemment effectués les ont utilisés en tant que variable proxy des ventes. Bien que plusieurs travaux ayant porté sur les cryptomarchés aient utilisé les évaluations comme témoignage qu'une vente a été effectuée (Christin, 2013; Barratt & Aldridge, 2016), l'utilisation de ce proxy sur des données émanant de forums de discussions soulève des limites. Tout d'abord, ce ne sont pas tous les acheteurs qui laissent une évaluation après une vente. Étant donné que ce n'est pas obligatoire, certaines pourraient préférer limiter leurs communications dans un souci de protection de leur identité (Holt et al., 2015). De plus, il est possible que certains vendeurs génèrent de fausses évaluations pour bonifier leur réputation afin d'attirer plus de clients. En effet, dans une optique de marchés de tacos et étant donné que les rôles occupés par les participants ne sont pas mutuellement exclusifs (un administrateur peut tout aussi bien être un vendeur), il est envisageable de remettre en question la véracité de certaines évaluations (Haslebacher, Onaolopo & Stringhini, 2016).

Deux types de limites méthodologiques ont été abordées au cours de cette section. La première porte sur le choix du type de lieu de convergence mobilisé pour récolter des données afin de mesurer les revenus des carders. Bien que l'utilisation d'observations provenant de forums peut présenter des limites, il est important de signaler que le phénomène de carding n'a jamais été étudié sous l'angle du darknet. Il est donc important de questionner ce phénomène sur les types de marchés virtuels hébergés sur le réseau Tor. De plus, nous avons mis à jour les limites que soulève l'utilisation d'un calcul des revenus mobilisant les évaluations laissées par les acheteurs et les prix affichés par les vendeurs. Ainsi, il est nécessaire de proposer une façon d'évaluer les revenus des carders en s'inspirant des méthodes utilisées par les recherches sur la réussite criminelle.

Ainsi, ce projet aura comme objectif général de comprendre la réussite criminelle différentielle des carders actifs sur le darknet. Afin de répondre à la première limite, nous analyserons les carders sans distinction de lieux de convergence. Ce choix se justifie par le fait que les carders n'ont jamais été étudiés sur les types de lieux de convergence de deuxième génération et qu'uniquement étudier les forums représente une limite échantillonnale. Pour cela, un sondage en ligne hébergé sur le réseau Tor sera utilisé pour questionner directement les carders. Cette technique de collecte présente des avantages car les participants sont libres de répondre où et quand bon leur semble en affichant aussi plus de sincérité dans leurs réponses (Mann & Stewart, 2000; Schonlau et al., 2002).

Nous déclinons notre objectif principal en trois objectifs spécifiques. Le premier s'attardera à mesurer les revenus criminels des carders. Il répondra à la seconde limite méthodologique inhérente à la méthode de calcul. Ici, l'intérêt d'utiliser un sondage sera double car nous nous inspirons des recherches sur la réussite criminelle. Pour rappel, une technique d'opérationnalisation repose sur l'utilisation de sondages interrogeant directement les criminels sur leurs revenus illégitimes (Tremblay & Morselli, 2000; Morselli & Tremblay, 2004a; Morselli & Tremblay, 2004b; Thompson & Uggem, 2012; Rowan, McGoin & Nguyen, 2018). Dans le cadre de ce mémoire, les carders seront interrogés sur leurs revenus et les profits engendrés par leurs activités illégitimes. Il sera aussi question de distinguer les vendeurs de produits du carding et les acheteurs qui les monétisent (Hutchings & Holt, 2014; Hardeveld, Webber & O'Hara, 2016).

Notre second objectif spécifique sera de décrire les caractéristiques personnelles et sociales des carders. Pour ce faire nous transposerons les différentes variables mises de l'avant dans les travaux portant sur la réussite financière à notre objet d'étude. Au-delà d'appliquer le modèle théorique de la réussite criminelle à cette forme de cybercriminalité, cette approche permettra aussi de soulever de nombreux points d'ombres dans la connaissance au sujet des carders. Premièrement, la littérature ayant porté sur le carding fournit peu d'éléments quant au degré de spécialisation des délinquants. Bien que nous savons que les rôles ne sont pas mutuellement exclusifs dans ces communautés (Haslebacher, Onaolopo & Stringhini, 2016), nous interrogerons leur degré de spécialisation en nous référant à ce qui a été fait par les travaux portant la réussite criminelle. Deuxièmement, au sujet des compétences et habiletés particulières, il sera d'intérêt de sonder, par exemple, les habiletés informatiques en demandant

aux participants s'ils ont déjà utilisé des logiciels malveillants pour dérober des informations financières. Troisièmement, la mise en place de tactiques nous renseignera sur la force des mesures sécuritaires mises en place par le participant. En nous inspirant des éléments mis de l'avant par Hardeveld, Webber et O'Hara (2017), nous questionnerons les carders sur leur fréquence d'utilisation de technologies d'anonymats. Finalement, nous questionnerons les acheteurs sur leurs expériences de victimisation endogène mis en avant par Herley et Florêncio (2010). Le tableau 4 présente un récapitulatif des sections du sondage présentant l'ensemble des variables qui seront questionnées pour répondre aux deux premiers objectifs spécifiques.

Il est clair qu'une partie des prédictors ayant un impact sur la réussite criminelle qui ont été mis de l'avant lors de la revue de la littérature sont absents. Ces absences se justifient par plusieurs explications. Tout d'abord, certains prédictors ne sont pas pertinents au phénomène de carding. Ceci est particulièrement le cas pour les déplacements et la mobilité qui s'inscrivent relativement mal dans l'étude d'une délinquance en ligne. Aussi, étant donné qu'un sondage sera utilisé, d'autres prédictors ont dû être mis de côté pour ne pas avoir des temps de passation trop longs. Par exemple, nous n'avons pas inclus des mesures relatives aux liens redondants dans un réseau criminel ou encore à une mesure du contrôle de soi. En effet, questionner ce type de prédictors nécessite beaucoup d'items qui rallongeraient le temps de passation et nuiraient à la qualité des données collectées et aux taux de réponse.

Tableau 4. Sections du sondage et variables à interroger

Sections	Sous-sections	Variables
Filtrage	-	Consentement éclairé ; Type de profil
Les activités des carders	Réussite criminelle	Revenus ; Profits
	Expérience	Spécialisation ; Compétences et habiletés particulières ; Mise en place de tactiques ; Victimisation endogène
	Sociabilité	Clients ; Vendeurs ; Collaborateurs
Sociodémographiques	-	Âge ; Genre ; Éducation ; Revenus légitimes ; ...

Notre troisième et dernier objectif spécifique s'attellera à identifier les caractéristiques personnelles et sociales qui expliquent les revenus des carders. La littérature sur la réussite financière des délinquants prévoit que certains prédicteurs peuvent avoir une influence tantôt positive, tantôt négative sur les revenus illégitimes. À titre d'exemple, nous avons vu que la spécialisation, le nombre de condamnations passées ou la mise en place de tactiques lors de la commission d'un crime ont un impact positif sur les revenus illégitimes (Tremblay & Morselli, 2000; Robitaille, 2004; Ouellet & Tremblay, 2014). Ainsi, au cours de cet objectif nous confronterons les résultats émis dans la littérature sur la réussite financière des délinquants en analysant l'impact des différentes caractéristiques personnelles et sociales des carders mises en avant lors de l'objectif spécifique précédent sur leurs revenus criminels. Ceci nous permettra d'identifier la contribution de chaque prédicteur. Nous utiliserons les revenus et les profits comme variables dépendantes.

CHAPITRE 2 - DONNEES

L'objectif général de ce projet de recherche est de comprendre la réussite différentielle des carders actifs sur le darknet. Un sondage a été utilisé pour collecter les données nécessaires au traitement des objectifs spécifiques. Ce chapitre se divise en trois sections qui séquent le processus d'obtention et d'échantillonnage des données. La première section développe l'élaboration générale du sondage et la seconde décrit la phase de collecte des données au travers des stratégies de promotion utilisées. Au vu de la qualité et de la quantité des données collectées, il était aussi important de composer avec la présence de réponses aberrantes et de données manquantes. La quatrième section explique les stratégies mobilisées pour pallier ces problématiques. Finalement, une dernière section se penche sur les limites inhérentes aux différentes étapes menées pour constituer les deux échantillons à l'étude.

2.1. LA CONSTITUTION DU SONDAGE

Un sondage en ligne a été conçu s'adressant directement aux carders qui avaient, au cours des 12 derniers mois, participé à des activités marchandes pouvant générer des revenus et impliquant des données financières ou bancaires. Les participants devaient être âgés d'au moins 18 ans pour qu'ils soient en mesure de fournir leurs consentements libres et éclairés. Le sondage s'articulait autour de 6 sections avec des questions portant successivement sur leurs (I) *Activités marchandes*, leurs (II) *Compétences et habiletés particulières*, leurs (III) *Expériences de victimisation endogène*, leurs (IV) *Utilisations des technologies d'anonymats*, leurs (V) *Contacts* et leurs (VI) *Caractéristiques sociodémographiques*. L'accès aux différentes sections dépendait du type de profil que le participant déclarait. Trois configurations étaient possibles : *vendeur de données financières* (30 questions), *acheteur de données financières* (35 questions) et *profil mixte* (vendeur et acheteur) (53 questions). Dans la configuration comptant le plus de questions, il était attendu que le sondage ne prenne pas plus de 15 minutes à être complété. Les participants étaient laissés libres de ne pas répondre à certaines questions en déclarant "*I would rather not say*". Le sondage est présenté en annexe I.

La section portant sur les (I) *Activités marchandes* se composait de 8 questions et était disponible en deux versions différentes selon que le participant ait déclaré être un vendeur ou un acheteur. Cette section interrogeait les revenus et les profits générés par les activités de carding, le nombre de produits achetés ou vendus, l'année de début des activités, les types de produits du carding achetés ou vendus, les types de lieux de convergences fréquentés, les rôles

occupés sur les lieux de convergence et les moyens de paiements utilisés pour faire des transactions. Certaines questions requéraient des réponses ouvertes alors que d'autres proposaient des choix de réponses.

La seconde section portant sur les (II) *Compétences et habiletés particulières* comptait 4 questions pour les vendeurs et 3 questions pour les acheteurs. Elles demandaient aux carders s'ils avaient déjà été recrutés ou parrainés en vertu de leur expérience et de leurs compétences, mais aussi d'évaluer, sur une échelle de 0 à 10, leurs propres compétences en tant que vendeur ou acheteur. Dans le cas particulier des vendeurs, une question supplémentaire demandait s'ils avaient déjà utilisé un logiciel malveillant pour dérober des informations financières ou bancaires. Mise à part la question demandant d'évaluer leurs propres compétences, l'ensemble des questions étaient fermées et proposaient de répondre par "Oui" ou par "Non".

La troisième section était exclusivement réservée aux acheteurs et s'intéressait aux (III) *Expériences de victimisation endogène*. En effet, dans le cadre de transactions mettant en jeu des produits du carding, ce sont les acheteurs qui peuvent être lésés par les vendeurs, par exemple, en ne recevant jamais le produit qu'ils ont payé. Cette section se composait de questions demandant aux carders pour quelle proportion de leurs achats ont-ils été arnaqués. Sur une échelle de 6 choix, ils pouvaient préciser avoir été arnaqué pour "100% du temps" ou ne "Jamais" l'avoir été. Au nombre de 6, ces questions se déclinaient pour interroger la victimisation endogène en générale (sans tenir compte du lieu de convergence) ainsi que 5 types de lieux de convergence (sites web, carding shops, forums de discussions, chat en ligne et cryptomarchés).

La quatrième section utilisait le même design de réponses que la section précédente et questionnait les carders sur leurs (IV) *Utilisations des technologies d'anonymats*. Une seule et même version de cette section était disponible et accessible à tous les participants, qu'ils soient vendeurs ou acheteurs. Les 6 questions interrogées successivement la proportion d'utilisation de machine virtuelle, de système d'exploitation garantissant l'anonymat, de réseaux virtuels privés (VPN), de moyens de communication encryptés, de réseaux superposés (darknets) et de services de blanchiment d'argent.

La cinquième section se composait de 3 questions ouvertes interrogeant les carders sur (V) leurs *Contacts* en tant que vendeur ou en tant qu'acheteur. Il était demandé combien de clients/vendeurs avaient-ils eus au cours des 12 derniers mois et combien de leurs collaborateurs étaient conscients ou ignorés participer à des activités de carding. Deux versions de cette section étaient accessibles dépendamment du profil du répondant.

La dernière et sixième section réunissait des questions portant sur les (VI) *Caractéristiques sociodémographiques* des carders. Cette section était accessible à tous les profils de répondants. Elle était composée de 9 questions portant sur l'âge, le genre, le fait d'avoir été ou non déjà condamné, le niveau d'études, les revenus provenant d'activités légitimes et d'autres activités illégitimes que le carding ainsi que le temps passé par semaine à faire des activités de carding et le temps passé par semaine à faire d'autres activités criminelles.

Afin de garantir l'anonymat des participants, ce sondage a été hébergé sur un serveur externe. Ceci a permis l'opérationnalité de deux mesures essentielles pour garantir l'anonymat des participants : 1) leur permettre d'utiliser une connexion anonyme et 2) de ne pas activer JavaScript sur leur navigateur. Outre le fait de garantir l'anonymat aux participants, ces mesures permettaient aussi de plus facilement gagner leur confiance. Étant donné que l'Université ne pouvait offrir qu'un site web statique, et que cela ne pouvait pas assurer la mise en place des deux mesures, un serveur privé a été utilisé pour permettre d'héberger un site web dynamique.

Les participants n'étaient pas rémunérés et leur participation était soumise à l'acceptation libre et éclairée du formulaire de consentement présent dès le début du sondage (voir annexe II). En date du 5 novembre 2018, le projet a été approuvé par le comité de la recherche en arts et sciences de l'Université de Montréal et le sondage a officiellement été mis en ligne sur Tor³ (#CERAS-2018-19-164-D) (voir annexe III).

2.2. LES STRATEGIES DE PROMOTION

La collecte de données officielle s'est étendue entre le 6 décembre 2018 et le 4 avril 2019. Au cours de ces 4 mois, plusieurs stratégies ont été utilisées pour promouvoir le sondage auprès des carders. Dans un premier temps, un courriel a été envoyé au site journalistique spécialisé

³ Le sondage était accessible via l'adresse suivante : <http://fopvitnzpm5jl4or.onion/>.

dans la cybercriminalité, DeepDotWeb⁴, pour leur demander de relayer le projet. Ainsi, le 12 décembre 2018, ce site a publié un article le décrivant et invitant ses lecteurs à y participer. Plus qu'une simple promotion anecdotique, cet article a permis de commencer à générer de la confiance autour du sondage en rejoignant leur lectorat. De plus, mentionner cet article dans les invitations a permis, d'une part, d'avoir un plus grand crédit auprès des carders mais aussi, d'écourter les messages de promotion souvent trop lourds en indiquant aux intéressés que l'explication du projet était détaillée dans l'article. Par la suite, l'étape de l'envoi des messages d'invitations par le biais des lieux de convergences a pu commencer. Ainsi, jusqu'à fin janvier 2019, 4 types de lieux de convergences ont été identifiés et des invitations ont été envoyées aux carders qui les fréquentaient : les chats en ligne, les forums, les carding shops et les cryptomarchés.

Les chats en ligne tels qu'ICQ ou Telegram sont les lieux de convergence qui ont été le plus sollicités pour contacter les carders. En effet, un grand nombre de carders sont présents sur ces plateformes. En s'organisant en groupes de discussions pouvant être plus ou moins privés les carders peuvent faire des offres ou des demandes à des milliers de leurs homologues. L'interface de ces chats offre aussi la possibilité de communiquer de manière privée avec un autre utilisateur. Grâce à cette fonctionnalité, il a été possible d'entrer avec environ 2,000 carders. Pour identifier rapidement les carders et faciliter la transmission du message d'invitation, près de 80 groupes de discussions ont été rejoints. Ceci nous a permis d'accéder aux historiques de conversations de ces groupes. Malgré le fait que les messages de ces historiques soient cryptés, l'identifiant appartenant à chaque participant reste visible. Il a ainsi été possible, à l'aide d'un parser, d'extraire ces identifiants des historiques de conversations pour établir une liste de carders potentiels à contacter. La mise à jour régulière des historiques a permis d'incrémenter cette liste avec de nouveaux identifiants. À partir de cette liste, des milliers de messages d'invitations ont été envoyés à autant de carders. Cette stratégie constituait le cœur de la campagne de promotion.

En parallèle des invitations lancées sur les chats en ligne, et étant donné qu'il fallait limiter l'envoi des messages d'invitations pour éviter d'être bloqué par les plateformes soutenant les salles de clavardage, d'autres carders ont été contactés sur des forums de discussion sur Tor et

⁴ Ce site a été fermé par les autorités le 7 mai 2019.

sur le *clearweb*. Cette stratégie s'articulait autour de deux axes. Premièrement, l'envoi d'invitations par messages privés via le système de messagerie offert par le forum. Ceci nécessitait une identification préalable de carders en lisant les différents messages postés sur les forums. Deuxièmement, l'identification des administrateurs des forums suivie d'une prise de contact plus informelle que le message d'invitation permit de présenter le projet et de demander leurs autorisations pour créer un fil de discussion afin de promouvoir le sondage. Aussi bien pour la prise de contact direct avec les carders que lors des discussions plus informelles avec les administrateurs, cette stratégie s'est avérée peu payante dans la mesure où très peu de réponses ont été retournées par les carders et que peu d'administrateurs ont accédé à notre requête.

Dans une même optique, l'envoi de messages d'invitations privées a aussi été entrepris auprès de carders évoluant sur des cryptomarchés et des carding shops. Contrairement aux forums de discussion, où il est possible de distinguer les vendeurs des acheteurs au travers des fils de discussion, les cryptomarchés et les carding shops sont des lieux de convergence mettant les vendeurs en avant. Dans le cadre des cryptomarchés, le système de messagerie privée a été utilisé pour envoyer les messages d'invitations à plusieurs vendeurs. Étant donné que les cryptomarchés organisent les offres en diverses catégories, il a été plus facile d'identifier les vendeurs proposant des produits du carding. Dans le cas des carding shops, deux canaux de communication ont été utilisés pour rentrer en contact avec le ou les gérants de carding shops. Alors que certains carding shops fournissent un contact courriel pour correspondre, d'autres proposaient une fonctionnalité *Support* pour contacter directement le ou les gérants via le site hébergeant le carding shop. Dans les deux cas, un e-mail ou un message présentant le projet a été envoyé. Comme pour les forums de discussions, cette stratégie a été peu fructueuse dans la mesure où très peu de réponses ont été reçues.

Malgré la mise en place de ces différentes stratégies sur une multitude de lieux de convergences, peu de visites ont été enregistrées sur le serveur hébergeant le sondage. Ce constat est consistant avec la littérature sur le sujet qui stipule que les taux de participation aux sondages en ligne sont relativement faibles (Décorte, 2010). Dans notre cas, ce phénomène se retranscrit bien dans la série chronologique du nombre de visites sur le site du sondage par jour présentée dans la figure 1. En effet, avant fin janvier 2019, le nombre de visites reste relativement stable et faible, oscillant entre 10 et 20 par jour. Ainsi, la décision a été prise de promouvoir le sondage sur d'autres plateformes. À partir du 30 janvier 2019, nous avons pris contact avec les équipes

promouvoir encore davantage le projet. À terme, cette stratégie a permis de poster un message de promotion sur 4 subreads dont 2 ayant vérifié l'identité du chercheur. De même qu'avec la stratégie de promotion visant reddit, cette stratégie s'est avérée efficace dans la mesure où elle a permis, pendant plus de deux semaines, de soutenir un rythme oscillant entre 50 et 80 visites par jour. De plus, le fait que, comme le sondage, Dread soit hébergé sur Tor incite plus facilement les intéressés à parcourir le site du sondage car ils n'avaient pas à changer de navigateur pour y accéder.

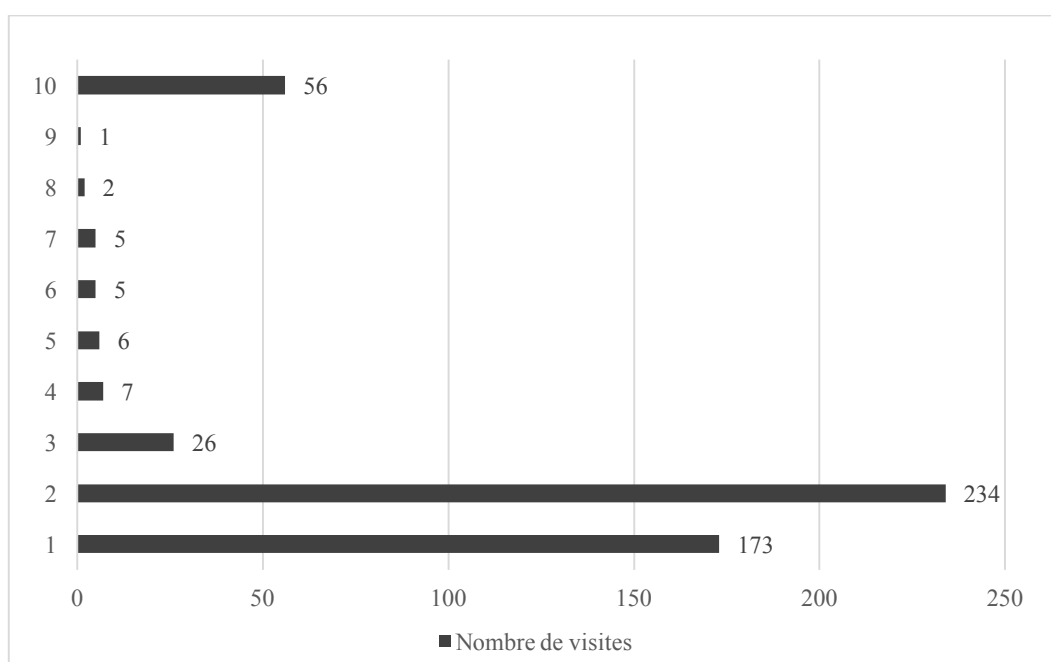
Pour conclure, une rétrospective générale des stratégies de promotion utilisées et la série chronologique du nombre de visites par jour permettent de constater des impacts différentiels selon la stratégie mobilisée. En effet, cette série présente de fortes différences en termes de nombre de visites selon les périodes. À ce propos, la période creuse entre le 1^{er} et le 6 mars 2019 où aucune visite n'a été enregistrée s'explique par le fait que des problèmes techniques ont été rencontrés au niveau de l'hébergement du sondage. La stratégie s'étant avérée être la plus payante consistait à contacter les modérateurs des différents subreddits ou subreads pour leur demander s'il était possible de poster un message. Néanmoins, cette stratégie ne peut s'inscrire dans le temps dans la mesure où il existe un nombre limité de subs qu'il est pertinent de contacter pour promouvoir le sondage. Les autres stratégies de promotion menées directement sur les différents types de lieux de convergence se sont avérées moins rentables en termes de visites. De plus, ces dernières étaient aussi plus dispendieuses en termes de temps en ce sens qu'il faille créer un compte sur chacun des lieux de convergence pour communiquer avec sa communauté. Ce désavantage est particulièrement probant dans le cas des carding shops qui nécessitent la vérification de l'inscription pour simplement obtenir une adresse email à contacter. Cependant, cette démarche a pour avantage d'offrir au chercheur de glaner des connaissances plus généralistes sur le fonctionnement des communautés et du carding, et ce même si des expériences de victimisation peuvent être vécues.

2.3. L'ECHANTILLON

En date du 4 avril 2019, la collecte s'est achevée et 2,961 visites sur la page d'accueil du sondage ont été comptabilisées. Les données collectées pendant ces visites étaient hébergées sur le serveur et avaient chacune un identifiant unique et anonyme attribué à chaque connexion sur la page d'accueil. Ainsi, un utilisateur qui rafraîchirait cette page d'accueil serait comptabilisé

comme une nouvelle visite. Parmi ces 2,961 visites sur la page d'accueil, 515 (17%) d'entre elles ont conduit à parcourir la seconde page qui hébergeait le formulaire de consentement libre et éclairé dont l'approbation était essentielle pour participer au sondage. Le sondage s'étalonnant sur un nombre de 10 pages (en comptant le formulaire de consentement en page n°1), un participant s'étant rendu à la page n°10 a donc aussi parcouru certaines des pages précédentes dépendamment de son profil. La figure 2 présente la distribution du nombre de visites par page parcourues. À titre d'exemple, 26 participants ont arrêté de compléter le sondage en page n°3.

Figure 2. Distribution du nombre de visites par pages parcourues



Une large majorité des participants ne se sont pas rendus plus loin que la page n°2 (n = 407 ; 79%). Pour rappel, la page n°1 hébergeait le formulaire de consentement libre et éclairé d'attestation et la page n°2 les questions relatives à l'âge minimal et aux types de profils des carders (vendeur et/ou acheteur). À la lumière des discussions informelles entretenues avec les carders au cours de la promotion du sondage, il est fort probable que ces désistements s'expliquent par le fait qu'une grande partie des carders soient relativement réfractaires à communiquer des informations relatives à leurs activités. Néanmoins, la figure 2 montre que les participants ayant passé la page n°2 semblent enclins à maintenir leur participation jusqu'à la fin du sondage. Il est tout de même important de garder à l'esprit que certains des participants s'étant rendus jusqu'à la fin peuvent tout simplement avoir parcouru les pages sans pour autant répondre aux questions.

Il était important d'observer le contenu des réponses de notre échantillon de 56 participants ayant parcouru l'ensemble des pages du sondage. Cet exercice a laissé ressortir une certaine forme d'inconsistance dans les réponses chez certains participants. En effet, au vu du caractère sensible de la population d'intérêt, il n'était pas étonnant d'observer que les données collectées contenaient des réponses aberrantes ainsi que des réponses manquantes. Au vu de la petite taille de l'échantillon, des stratégies ont été développées pour pallier ces problèmes qui auraient nui à la qualité des résultats. Ainsi, les stratégies utilisées pour identifier les réponses aberrantes et imputer les réponses manquantes sont développées dans la sous-section suivante.

2.3.1. IDENTIFICATION DES REponses ABERRANTES

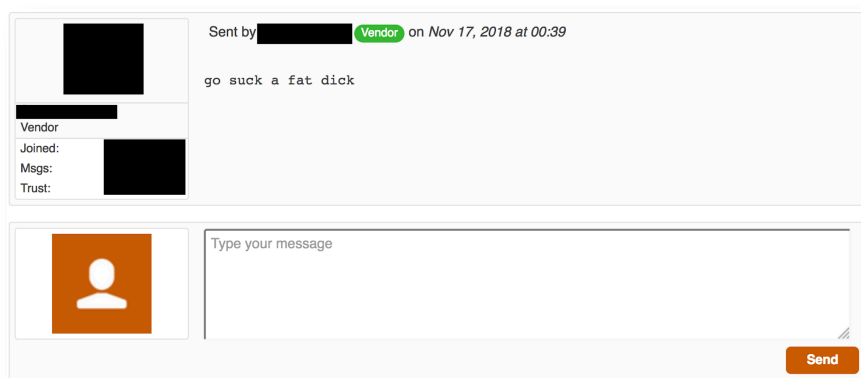
Dans la littérature, l'identification de réponses aberrantes peut s'inscrire dans un cadre relativement large. Appelé *outliers*, les réponses aberrantes peuvent revêtir un aspect d'anomalie qui se réfère à "toute observation (ou sous-set d'observations) qui apparaît être inconsistante avec le reste des observations" (Barnett & Lewis, 1994). Dépendamment du système dans lequel elles s'inscrivent, ces anomalies peuvent provenir de problèmes techniques, de phénomènes naturels, de comportements volontaires ou involontaires. Dans le cas de ce projet, ces anomalies s'exprimaient par la présence de réponses aberrantes. Il était important d'identifier ce type d'observations qui sont inutilisables et/ou invalides et qui doivent être supprimées pour offrir une meilleure consistance aux résultats (Huang, Liu, & Bowling, 2015). Dans le cadre des sondages en ligne, la littérature soutient que ces observations peuvent provenir de trois sources : (1) une mauvaise compréhension, (2) un manque d'attention ou d'intérêt et (3) une fausse déclaration (Johnson, 2005).

Le premier facteur pouvant mener à des réponses aberrantes émane d'une mauvaise compréhension des questions (Johnson, 2005). L'un des moyens pour éviter d'avoir des questions pouvant être mal comprises est de faire une phase de prétest. Ceci permet d'identifier les questions du sondage pouvant mener à des interprétations fluctuantes pour effectuer des modifications si nécessaire (Krosnick, 1999). Dans le cadre de ce sondage, cette phase s'est déroulée sur une période de 5 jours (du 15 au 20 novembre 2019) avant le lancement officiel du sondage. Au cours de celle-ci 193 invitations ont été envoyées à des carders sur tous les types de lieux de convergence (cryptomarchés, carding shops, chats en ligne et forums). Un

retour relativement détaillé et positif a été obtenu de la part de 2 carders. Ces derniers précisait que le sondage était clair et pertinent. De plus, cette phase de prétest a permis d'appréhender les difficultés inhérentes à entrer en contact avec des cyberdélinquants. En effet, hormis ces 2 carders, l'ensemble des autres carders invitées ont refusé de participer. Certains des refus étaient d'ailleurs accompagnés d'insultes ou de menaces (voir figure 3). Néanmoins, les retours positifs des 2 carders interrogés ont permis de soutenir que cette source de réponses aberrantes a été tout du moins contrôlée a posteriori.

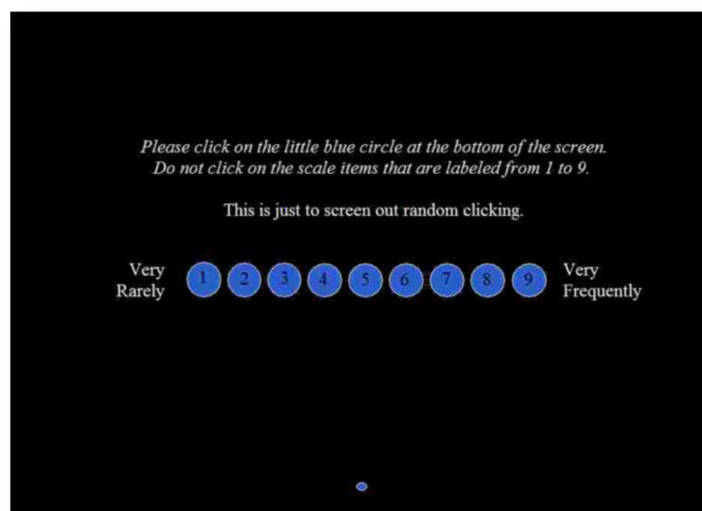
Le second facteur pouvant mener à des réponses aberrantes est le manque d'attention ou d'intérêt (Johnson, 2005). Bien que ce facteur soit difficilement appréhendable, il était possible de mettre en avant deux points qui laissaient présager un manque d'attention ou d'intérêt de la part de certains des répondants. Premièrement, il a été observé qu'une majorité des sondages n'ont pas été entièrement complétés. Ceci laisse envisager que certains répondants l'ont délaissé par manque d'attention ou d'intérêt. Cette hypothèse pouvait d'ailleurs être soutenue par le fait que les cyberdélinquants sont récalcitrants à donner leurs informations car cela pourrait mettre à mal leur sécurité. Deuxièmement, lors des discussions informelles entretenues avec les carders, il a été possible d'obtenir des retours de leur part quant au design général du sondage. Contrairement à ceux interrogés au cours de la phase de prétest certains d'entre eux ont émis des critiques vis-à-vis de la longueur du sondage, de la complexité de la formulation de certaines questions ou encore du caractère sensible des informations demandées qui auraient pu mener à un manque d'attention ou d'intérêt.

Figure 3. Exemple d'insulte reçue sur un cryptomarché lors de la phase de test



La littérature sur les sondages en ligne renseigne des techniques permettant de contrôler le niveau d'attention d'un répondant. Parmi elles, les *Instructional Manipulation Checks* (IMC) prendront la forme de questions qui vont être incorporées au cours du sondage et qui permettent de contrôler le niveau de désengagement des répondants (Anduiza & Galais, 2017). Elles permettent de mettre en exergue certains phénomènes telle que la suffisance qui se réfère au fait d'être peu concentré et de dépenser peu ressources cognitives lors de la formulation d'une réponse (Krosnick, 1999; Huang et al., 2012). À titre d'exemple, le fait qu'un répondant réponde sans avoir lu les questions est considéré comme une forme de suffisance. La figure 4 illustre bien un IMC où le système de choix réponses sert de tâche interférente pour contrôler si le participant a bel et bien lu la question (Oppenheimer, Meyvis & Davidenko, 2009). Bien qu'aucun IMC n'ait été implémenté dans le sondage, il demeure qu'une métrique était disponible pour évaluer le niveau d'attention du répondant. En effet, le fichier contenant les réponses des sondés renseignait aussi l'heure à laquelle un participant s'était connecté sur chaque page du sondage. Ainsi, il était possible de déterminer combien de temps le participant a passé à compléter le sondage. Bien qu'il soit difficile de déterminer des standards en termes de temps de réponse, les temps des réponses paraissant trop courts pour avoir mené à une complétion crédible du sondage ont été examinés (Curran, 2016). Ils ont permis d'identifier les répondants qui pourraient présenter un manque d'attention ou d'intérêt.

Figure 4. Exemple d'un IMC - the Blue Dot task (Oppenheimer, Meyvis & Davidenko, 2009)



Enfin, étant donné le caractère sensible des informations demandées à une population de cyberdélinquants tout aussi sensible au fait que l'on puisse s'intéresser à leurs activités illégales, il était fort probable que l'échantillon initial contienne de fausses déclarations. Cette hypothèse peut être soutenue par le fait que, lors de la promotion du sondage, des menaces mentionnant que de fausses informations pourraient y être entrées ont été reçues. Pour identifier ce type de réponses aberrantes, des questions proposant volontairement des choix de réponses étendus ont été placées dans le sondage. Ceci permettait d'identifier les répondants fournissant des réponses irréalistes. Ainsi, pour la question portant sur l'année du début des activités de carders, il était possible de choisir une année de début des activités allant de 1960 à 2018. Cette stratégie permettait d'identifier et d'éliminer les répondants malhonnêtes (Beach, 1989; Meade & Craig, 2012). De plus, en utilisant l'approche recommandée par Johnson (2005), il a été possible d'identifier la présence de patterns de réponses répétitifs à des questions mesurant des variables différentes pour discriminer et éliminer d'autres répondants ayant répondu malhonnêtement.

En conclusion, pour contrôler les trois sources de réponses aberrantes, une stratégie a été mise en place a posteriori du sondage et d'autres ont été opérationnalisées après la collecte des données. Effectuée a posteriori du lancement officiel, la phase de prétest a permis de contrôler la bonne compréhension des questions. Néanmoins, il est important de noter qu'elle se basait sur un échantillon relativement petit de deux testeurs et que certains carders interrogés au cours de la promotion du sondage ont émis des critiques quant à la complexité des questions. D'autres indices laissaient présager que certains participants manifestaient un manque d'attention ou d'intérêt. En effet, un certain nombre de sondages n'ont pas été complétés et, comme précisé plus tôt, des participants se sont plaints de la complexité des questions. De plus, aucun IMC n'a été mis en place lors du design du sondage pour contrôler l'attention. Néanmoins, en bénéficiant des temps de réponse des participants, il a été possible de contrôler le manque d'attention ou d'intérêt. Pour finir, pour contrôler le cas des fausses déclarations, choix de réponses irréalistes ont volontairement été ajoutés afin d'identifier les participants malhonnêtes qui se verront porter une attention particulière pour noter s'il y a présence de patterns de réponses répétitifs ou de réponses incohérentes.

2.3.1.1. Contrôle des réponses aberrantes

L'échantillon initial se composait de 56 sondages ayant été visités jusqu'à la fin. Pour identifier les réponses aberrantes, notre première stratégie utilisait la question disposant de choix de

réponses volontairement étendus. Elle demandait aux carders en quelle année avaient-ils débuté leurs activités et proposait de sélectionner une réponse entre 1960 et 2018. En prenant en considération que la première loi applicable au carding a été adoptée en 2003 en Californie (Perretti, 2009), nous avons utilisé une approche conservatrice en identifiant les répondants ayant déclaré avoir commencé leurs activités de carding avant l'année 2000. Un seul d'entre eux a été identifié et avait déclaré avoir commencé le carding en 1977.

Notre seconde stratégie visait à identifier les patterns répétitifs. Les patterns répétitifs sont le fait qu'un répondant ait entré des caractères ou des séquences de caractères similaires et/ou suspectes à des questions adjacentes dans le sondage. À titre d'exemple, le fait qu'un participant ait répondu "999999" à une question et "888888" à la suivante est considéré comme un pattern répétitif. Cette stratégie nous a permis d'identifier 5 participants présentant des patterns répétitifs dans leurs réponses. Le participant identifié lors de l'étape précédente en faisait partie.

Pour finir, notre troisième et dernière stratégie visait à identifier les réponses incohérentes. Une réponse sera considérée incohérente lorsqu'elle ne peut pas être réellement envisageable physiquement ou qu'elle entre en contradiction avec une autre. Pour identifier les réponses incohérentes, nous avons vérifié : si les participants n'avaient pas déclaré des profits plus haut que leurs revenus, si les participants n'avaient pas un âge trop jeune ou inconsistant avec la date de début de leurs activités et si le nombre d'heures par semaine déclaré n'excède pas le nombre d'heures que contient une semaine. Suite à cette vérification un seul répondant a été identifié. Il avait déclaré participer à des activités criminelles près de 190 heures par semaine. À noter que ce participant a aussi été identifié lors de la stratégie précédente. À l'issue de cette étape, 5 participants ont été identifiés comme ayant au moins l'un des trois critères que nous avons mis en place et ont été éliminés.

2.3.1.2. Contrôle de l'attention et de l'intérêt

Pour chaque page visitée, le serveur hébergeant le sondage renseignait à quel moment le participant accédait à la page en question. Ainsi, entre soustrayant le moment auquel le participant accède une page du sondage au moment où il accède à la suivante, il était possible de déterminer le temps qu'il aura mis pour compléter la page. Le tableau 5 présente les indices de tendance centrale et de dispersion pour chacun des pages du sondage.

Au niveau des temps de passation sur l'ensemble du sondage, les résultats restent relativement consistants avec ce qui était attendu. En effet, le sondage devait prendre entre 10 et 15 minutes à être complété et la moyenne et la médiane du temps total de passation s'élèvent respectivement à 12 minutes 43 secondes et 9 minutes 23 secondes. Il est aussi intéressant de noter qu'il existe une dispersion importante du temps total de passation (É.-t. = 11:13 ; Min = 01:38 ; Max = 49:45). Ces indices nous laissent penser qu'il est fort probable que les participants ayant fourni des réponses aberrantes n'aient pas passé beaucoup de temps à faire le sondage. À l'inverse, il est aussi intéressant de noter qu'un participant a passé près de 50 minutes à le compléter.

L'analyse de temps de réponse montre que certaines pages ont nécessité plus de temps que d'autres pour être complétées. En effet, les pages n°3, n°4 et n°11 présentent les médianes les plus élevées (respectivement Mdn = 02:16 ; Mdn = 01:29 ; Mdn = 01:44). Bien que ce sont ces pages qui contenaient le plus de questions, les maximums nous laissent penser que certains répondants peuvent avoir pris une pause au cours du sondage. Cette hypothèse entre d'ailleurs en résonance avec le fait que la passation n'était pas supervisée par le chercheur et que nous avons reçu différentes critiques quant à la complexité des questions lors de la promotion.

Tableau 5. Indices de tendance centrale et de dispersion pour le temps de passation par page

Page	Moyenne	Médiane	Écart-type	Min	Max
0	00:31	00:10	01:32	00:03	11:29
1	00:21	00:12	00:28	00:04	02:32
2	03:01	02:16	03:51	00:10	20:41
3	03:18	01:29	06:13	00:15	35:25
4	00:53	00:30	01:02	00:08	04:23
5	00:39	00:24	00:42	00:06	03:03
6	01:22	00:56	01:02	00:09	04:35
7	01:22	00:47	01:20	00:10	05:35
8	01:25	00:37	01:46	00:03	07:46
9	00:41	00:31	00:59	00:04	05:08
10	00:16	01:44	04:23	00:10	26:58
Total	12:43	09:23	11:13	01:38	49:45

Au vu de l'importante dispersion des temps de réponse pour chaque page, les médianes ont été utilisées pour contrôler l'attention et l'intérêt des participants. Ainsi, les réponses de chaque participant dont le temps de réponse total est en dessous de la médiane ont été analysées. Cette étape a été réitérée pour chacune des pages qu'il avait complétées. Un total de 26 participants ont mis moins de 9 minutes 23 secondes à parcourir l'ensemble du sondage. Parmi les participants ayant eu les plus petits temps de passation, 4 des 5 participants identifiés lors de l'identification des réponses aberrantes ont été retrouvés. Ces participants affichaient des temps de réponse parmi les plus bas alors que le cinquième avait passé plus de 44 minutes à le faire. Les réponses des autres participants étant en dessous de la médiane ont été examinées. La totalité d'entre eux a précisé être soit des vendeurs, soit des acheteurs. Ce constat permet d'expliquer pourquoi leurs temps de passation se retrouvent en dessous de la médiane. En effet, les participants ayant précisé n'occuper qu'un seul rôle avaient à remplir moins de questions que ceux occupant les deux rôles. L'examen de ces participants a mené à l'identification de deux participants supplémentaires présentant des temps de réponse suspects qui ne peuvent vraisemblablement pas mener à une passation sérieuse du sondage.

À la lumière des critères permettant d'identifier les réponses aberrantes, nous avons été en mesure de mettre de côté 5 participants. Parmi eux, 4 d'entre eux présentaient des temps de passation en dessous de la médiane ($Mdn = 09:23$) et le dernier présentait un temps de passation de plus de 40 minutes. L'examen des autres temps de réponse nous a permis de constater que 2 participants ne pouvaient vraisemblablement pas avoir complété le sondage correctement. En conséquence, un total de 7 participants a été éliminé du jeu de données. À l'issue des stratégies mises en place pour composer avec les réponses aberrantes, l'échantillon se compose de 49 sondages ayant été visités jusqu'à la fin et présentant des réponses cohérentes.

La section suivante s'attarde à décrire les moyens mis en place pour composer avec les données manquantes présentes dans le jeu de données. Pour cela, deux échantillons distincts ont été tirés de l'échantillon initial : un pour les vendeurs ($N = 24$) et un pour les acheteurs ($N = 36$).

2.3.2. LES DONNEES MANQUANTES

La présence de données manquantes dans un jeu de données est un problème récurrent lorsque ce dernier provient d'un sondage. Il n'est pas étonnant de constater l'absence de certaines

réponses en particulier lorsque des informations sensibles sont demandées. Dans notre cas plus particulièrement, les carders ne souhaitent pas divulguer certaines de leurs informations pour des raisons évidentes de sécurité. Étant donné la taille relativement modeste de notre échantillon, il est important d'utiliser une méthode permettant de tirer le meilleur parti de nos données en composant avec ces valeurs manquantes. Parmi les plus communément utilisées, la méthode *listwise* consiste à éliminer les observations incomplètes (Allison, 2002; Tsiriktsis, 2005). Bien qu'elle puisse être utilisée pour mener n'importe quel type d'analyses statistiques et qu'elle soit facile à opérationnaliser, cette approche conservatrice réduit la puissance statistique de l'échantillon et mène à une identification moins précise des relations significatives (Tsiriktsis, 2005; Wayman, 2005). Dans le cas de données provenant d'un sondage, cette approche contraint aussi le chercheur à sacrifier un grand nombre d'informations qui ont pu nécessiter d'importants investissements humains et financiers (Kaufman, 1988). Une autre méthode régulièrement utilisée est la substitution par la moyenne. Elle consiste à remplacer toutes les valeurs manquantes par la moyenne de la variable. Bien qu'elle présente aussi des facilités d'opérationnalisation et qu'elle permet d'utiliser les observations incomplètes, cette méthode aura pour effet de nuire à la puissance statistique en réduisant la variance de la variable en plus de mener à une identification moins précise des relations significatives qu'elle pourrait entretenir avec d'autres variables (Wayman, 2003).

Au vu de notre échantillon, il est donc important de sélectionner une méthode performante pour composer avec nos données manquantes. Dans cette optique, nous utiliserons une imputation multiple. Cette méthode prédit les valeurs des données manquantes en fonction des valeurs des autres variables et permet de conserver la consistance des caractéristiques présentées par le jeu de données (Wayman, 2005; Allison, 2012). En effet, l'imputation multiple va prendre en compte le fait que la donnée qu'elle va remplacer est une valeur manquante à l'origine tout en préservant les caractéristiques originelles du jeu de données (Lall, 2016). Ainsi, cette méthode va chercher à imputer une valeur à une observation en prenant en considération l'ensemble des données complètes qui possède une valeur pour la variable contenant la valeur à imputer. À la lumière de l'analyse de toutes les observations et des patterns détectés, l'imputation multiple va ainsi affecter une valeur en fonction de ce qu'elle a observé parmi les observations les plus similaires à celle qui nécessite une imputation. En ajoutant une composante aléatoire lors de l'estimation des valeurs à remplacer, l'imputation multiple permet de pallier un des problèmes

que présente la substitution par la moyenne et ainsi d'éviter de produire des sous-estimations de la variance.

Évidemment, pour chaque imputation effectuée, cette composante aléatoire mènera à l'estimation de valeurs légèrement différentes. Pour pallier cette inconsistance, l'imputation multiple effectuera plusieurs fois cet exercice de prédiction pour obtenir différents jeux de données (Gelman & Hill, 2007). Il est recommandé d'effectuer au moins 5 imputations pour obtenir des estimés fiables (Allison, 2002). Les moyennes des données imputées pour chaque itération seront utilisées pour constituer un jeu de données agrégées qui sera analysé (Gelman & Hill, 2007).

2.3.2.1. L'imputation multiple

Pour chacun des deux jeux de données, une imputation multiple a été réalisée grâce au logiciel SPSS. La base de données des acheteurs concentre uniquement les participants ayant déclaré avoir acheté des produits du carding au cours des 12 derniers mois (à compter de la date de passation). Pour rappel, la base de données des vendeurs contenait 24 observations et la base de données des acheteurs en contenait 36. Cette section présente l'opérationnalisation des imputations multiples réalisées sur chacun des deux jeux de données.

Dans un premier temps, il était nécessaire d'analyser si des patterns étaient présents dans la distribution des valeurs manquantes. L'ensemble des variables des deux jeux de données a été soumis à des analyses descriptives des valeurs manquantes. Les tableaux 6 et 7 présentent respectivement les distributions des valeurs manquantes pour les vendeurs et les acheteurs.

Tableau 6. Distribution des valeurs manquantes pour la base de données des vendeurs

Vendeurs	Complètes	Manquantes	N
Variables	4 (9%)	39 (91%)	43 (100%)
Participants	9 (38%)	15 (63%)	24 (100%)
Valeurs	938 (91%)	94 (9%)	1,032 (100%)

Dans chacune des deux bases de données, une faible proportion des variables à l'étude n'affichait aucune valeur manquante (respectivement $n = 4$; 9% pour les vendeurs et $n = 5$; 10% pour les acheteurs). Il était aussi possible de constater que dans les deux échantillons, seul

9 des participants ont complété entièrement le sondage ; bien que le nombre de participants soit supérieur dans l'échantillon des acheteurs (N = 36). Dans l'ensemble, il est possible de constater une forme de consistance dans la distribution des valeurs manquantes dans les deux échantillons. En effet, plus de 90% des valeurs ont été entrées par les participants (respectivement n = 938 ; 91% pour les vendeurs et n = 1,590 ; (92%) pour les acheteurs). Ces constats permettent de dire qu'il y a une bonne consistance des informations disponibles initialement dans les deux bases de données qui encourage la démarche d'utiliser des imputations multiples.

Tableau 7. Distribution des valeurs manquantes pour la base de données des acheteurs

Acheteurs	Complètes	Manquantes	N
Variables	5 (10%)	43 (90%)	48 (100%)
Participants	9 (25%)	27 (75%)	36 (100%)
Valeurs	1,590 (92%)	138 (8%)	1,728 (100%)

Il était d'importance de contrôler l'existence de patterns dans la distribution des valeurs manquantes afin de déterminer le modèle d'imputation. Pour cela, le test de *Missing Completely At Random* (MCAR) de Little (1988) a été utilisé. Ce test va examiner si la probabilité d'avoir une valeur manquante dans une variable X est liée aux valeurs déjà présentes dans la variable X ou dans n'importe quelle autre variable du jeu de données. Dans le cas de nos deux échantillons, ce test s'est avéré non-significatif (respectivement $\chi^2 = 526.32$; $p > 0.05$ pour les vendeurs et $\chi^2 = 206.91$; $p > 0.05$ pour les acheteurs). Ceci suggère que les données respectent le postulat de MCAR et qu'elles ne présentent ni de patterns répétitifs, ni de monotonie. Ainsi, une méthode de Monte-Carlo par chaînes de Markov utilisant un modèle de régression linéaire servira de méthode d'imputation pour les deux échantillons.

Pour chacun des jeux de données, les variables présentant des valeurs manquantes ont été soumises à 5 imputations menant la constitution de 6 jeux de données : 5 jeux de données présentant les données imputées légèrement différemment à chaque imputation et 1 jeu de données agrégeant par la moyenne les valeurs imputées précédemment. Pour les vendeurs et les acheteurs, ce sont ces derniers jeux de données qui seront utilisés lors des analyses.

2.4. LIMITES

Les différentes étapes décrites précédemment qui nous ont permis de constituer les deux échantillons finaux présentent certaines limites. Tout d'abord, il est important de mentionner que les stratégies de promotion utilisées peuvent mener à des limites échantillonnales. En effet, dans un souci d'anonymat et de gain de temps, l'ensemble des pseudonymes des carders contactés n'a pas été conservé. Il devient donc difficile de savoir exactement combien de carders ont été contactés en tout et pour tout lors de la phase de promotion. De plus, le nombre d'invitations envoyées sur chacun des lieux de convergence s'est avéré être quantitativement très différent. Ceci s'exprime particulièrement au travers de la prise de contact auprès des gérants des carding shops. Alors qu'il est possible de joindre plusieurs dizaines voir centaines de carders sur un forum, un chat en ligne ou un cryptomarché, les carding shops n'offrent généralement qu'une adresse mail pour entrer en contact avec le gérant. Ainsi, il est fort probable que notre échantillonnage, au travers de nos stratégies de promotion, n'ait touché qu'une faible proportion de carders évoluant sur les carding shops comparativement à ceux évoluant sur d'autres types de lieux de convergence.

Deuxièmement, même si des stratégies pour composer avec les réponses aberrantes ont été développées en se basant sur la littérature, il n'est pas à exclure que certains carders aient volontairement fourni des réponses fausses qui, de par une forme de consistance et de plausibilité, n'aient pas été identifiées par les critères fixés par nos stratégies. Quand bien même, des observations ont dû être supprimées pour assurer aux analyses de traiter les données les plus véraçes, ce qui a réduit nos échantillons qui étaient déjà relativement petits. Cette troisième limite va nous contraindre à ne pas pouvoir entreprendre d'analyses multivariées dans la mesure où nos échantillons ne permettront pas de respecter le postulat du nombre d'observations par rapport au nombre de variables. Finalement cette problématique liée à notre petit nombre d'observations nous mène à la dernière limite relative à l'utilisation de jeux de données ayant subi des imputations de données manquantes. Bien que cette méthode soit relativement robuste et préserve la consistance statistique de l'échantillon (Wayman, 2005; Allison, 2012), il demeure qu'une partie des valeurs traitées lors des analyses ont été générées artificiellement par un algorithme.

CHAPITRE 3 - METHODOLOGIE

Pour comprendre la réussite différentielle des carders actifs sur le darknet, il est important de transposer les prédicteurs de la réussite criminelle identifiés lors de la revue de littérature au phénomène de carding. Cette démarche permet de générer un modèle empirique qui a servi de calque à la constitution du sondage. Ainsi, ce chapitre aborde successivement les trois objectifs spécifiques de cette recherche sous le prisme des variables interrogées. Les deux premières sections s'attellent à présenter respectivement les variables dépendantes et indépendantes ainsi que les stratégies d'analyses dont elles feront l'objet dans le prochain chapitre. La troisième section présente les hypothèses ainsi que les stratégies d'analyses qui permettront de répondre à notre troisième objectif spécifique qui cherche à identifier les caractéristiques personnelles et sociales qui expliquent les revenus des carders. Pour finir, la dernière section présente les limites méthodologiques identifiées.

3.1. MESURER LES REVENUS CRIMINELS DES CARDERS

La réussite criminelle des carders s'exprimant essentiellement au travers de l'argent qu'ils peuvent dégager de leurs activités, le premier objectif spécifique était de mesurer les revenus et les profits engendrés par les carders. Deux questions ont été utilisées pour mesurer les deux variables dépendantes de cette recherche. Dans un souci d'homogénéité des réponses fournies, les questions mesurant ces deux variables demandaient de préciser ces informations sur la période des 12 derniers mois. Ces deux questions étaient présentées dès le début du sondage dans la section (I) *Activités marchandes* du sondage.

Les revenus criminels : mesure les revenus criminels en dollars USD générés par les carders au cours des 12 derniers mois et était disponible en deux versions, selon que le participant ait déclaré être vendeur ou acheteur. Un bref paragraphe introductif au début de la section précisait que les revenus devaient être considérés comme le montant total des gains générés par les activités de vente ou d'achat de produits du carding. À titre d'exemple, voici la question destinée aux acheteurs: “*At how much would you estimate the income (in USD) you earned directly from the use of stolen financial information you bought through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?*”. Le participant disposait d'une boîte de texte pour y entrer sa réponse.

Les profits criminels : mesure les profits criminels en dollars USD générés par les carders au cours des 12 derniers mois et était aussi disponible en deux versions selon le profil du répondant. Comme pour la mesure des revenus criminels, des précisions quant à la conception des profits étaient fournies dans le paragraphe introductif de la section. Il y était indiqué que les profits devaient être considérés comme les gains nets (les revenus moins les investissements) obtenus par le participant au cours des 12 derniers mois. La question suivante mesurait les profits des vendeurs: *“At how much would you estimate the profits you earned directly from the sale of stolen financial information through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?”*. Comme pour les revenus, le participant devait entrer sa réponse dans une boîte de texte.

Pour répondre à ce premier objectif spécifique, des statistiques descriptives seront présentées pour chacune de ces variables présentes dans nos deux échantillons. Ainsi, les indices de tendance centrale et de variance seront examinés pour les revenus et les profits des vendeurs et des acheteurs. Au-delà de simplement mesurer les revenus criminels des carders, ces analyses conduiront à porter un regard inédit sur la distribution des revenus et des profits au sein de deux échantillons de carders. La prochaine section décrit l'opérationnalisation des différentes variables indépendantes de cette étude.

3.2. DECRIRE LES CARACTERISTIQUES PERSONNELLES ET SOCIALES DES CARDEURS

La littérature sur la réussite criminelle s'est largement penchée sur les prédicteurs de la réussite financière dans un contexte de criminalité plus traditionnelle que la cybercriminalité. Il était ainsi important de transposer ce modèle théorique et la conceptualisation de ces prédicteurs à notre phénomène tout en interrogeant des composantes étant propres aux activités des carders. Ainsi, la présente section décrit l'ensemble des variables dépendantes à l'étude. Comme pour la section précédente, l'opérationnalisation qui a mené à la mesure de chacune de ces 23 variables y est décrite.

Profils : le script criminel du carding a mis en évidence que les carders qui dérobent les informations financières sont peu enclins à les utiliser eux-mêmes et préfèrent alors les vendre à d'autres qui les monétiseront (Dupont, 2012). Cette étape du script met en exergue la présence

de deux types de carders, les vendeurs et les acheteurs, qu'il était important de distinguer (Hutchings & Holt, 2014; Hardeveld, Webber & O'Hara, 2016). La constitution de cette variable s'appuyait sur deux questions présentes avant même l'accès au sondage. Chacune d'elle demandait si le participant avait, au cours des 12 derniers mois, participé à des activités de ventes ou d'achats de produits du carding. Lorsque les deux réponses fournies étaient négatives, le participant n'accédait pas au sondage. À titre d'exemple, voici la question demandant au participant s'il a déjà été vendeur : *“In the past 12 months, have you sold stolen financial information through an online website, online autoshop, online forum, online chat room or online market at least once?”*.

Section (I) Activités marchandes :

Nombre de produits vendus/achetés. Les études portant sur le carding ont mis en exergue que ces délinquants disposent d'une panoplie de techniques pour dérober des informations financières. Certaines de ces techniques peuvent vraisemblablement mener à la compromission d'un grand nombre de données (Sullivan, 2010; Symantec, 2015; Green & Stavins, 2016; Chakraborty et al., 2016; Kashmiri, Nicol et Hsu, 2016; Manworren, Letwat et Daily, 2016; Ferrell, 2016). Ainsi, les carders ayant obtenu ces informations préfèrent les vendre plutôt que de les utiliser eux-mêmes (Dupont, 2012). Il était alors important de quantifier le nombre de produits vendus par les carders étant vendeurs mais aussi le nombre de produits achetés par les carders étant acheteurs. Ces deux variables étaient mesurées en demandant aux participants combien de produits avaient-ils approximativement vendus/achetés au cours des 12 mois. Les participants étaient libres d'entrer leur réponse numérique dans une boîte de texte.

Année de début des activités. La littérature sur la réussite criminelle a mis en lumière que l'expérience criminelle a un impact positif sur la génération de revenus illégitimes. Ce concept a particulièrement été étudié à l'aide de l'âge et du nombre de condamnations passées (Robitaille, 2004; Ouellet & Tremblay, 2014). Le carding étant un phénomène criminel relativement récent, il était d'importance de demander aux carders depuis combien de temps ils s'y adonnaient pour exprimer un pan de l'expérience en termes d'années d'activité. Ainsi, deux questions interrogeaient respectivement les vendeurs et les acheteurs sur ce sujet-là. À titre d'exemple, voici la question destinée aux vendeurs : *“In what year did you first start selling stolen financial information?”*.

Les types de produits : demande aux participants quel(s) type(s) de produits utilisent-ils lors de leurs activités de carding. Cette question comportait les mêmes choix de réponses dépendamment des deux versions disponibles selon le profil du participant. La littérature renseigne quatre principaux types de produits vendus sur les lieux de convergences et utilisés par les acheteurs : les *dumps*, les *fullz*, les *CVV* et les *identifiants de comptes en ligne* (Clarke & Newman, 2003; Thomas & Martin, 2006; Franklin et al., 2007; Peretti, 2009; Holt & Lampke, 2010; Hutchings & Holt, 2014; Du et al., 2018). Les participants pouvaient déclarer utiliser un ou plusieurs de ces types de produits en cochant les choix de réponses disponibles. Les réponses débouchaient à la constitution d'autant de variables dichotomiques que de types de produit.

Les types de lieux de convergences fréquentés : questionne les participants sur le(s) type(s) de lieux de convergence qu'ils fréquentaient dans le cadre de leurs activités de carding. Disponible aussi en deux versions selon le profil du répondant, cette question à choix de réponses multiples demandait au répondant de sélectionner les types de lieux de convergence identifiés dans la littérature, à savoir : les *sites web*, les *carding shops*, les *forums*, les *chats en ligne* et les *cryptomarchés* (Thomas & Martin, 2006; Franklin et al., 2007; Fallman, Wondracek et Platzer, 2010; Yip, Shadbolt et Webber, 2010; Motoyama et al., 2011; Décary-Héту & Leppänen, 2013; Yip et al., 2013; Benjamin et al., 2015; Bulakh & Gupta, 2015; Broséus et al., 2016; Décary-Héту & Giommoni, 2016; Haslebacher, Onalopo & Stringhini, 2016; Smirnova & Holt, 2017). Cette question débouchait sur la constitution de 5 variables dichotomiques pour chacun des lieux de convergence.

Les rôles occupés sur les lieux de convergence : interroge les participants sur le ou les rôles occupés sur les lieux de convergences fréquentés dans le cadre de leurs activités de carding. Elle était disponible en deux versions, pour les vendeurs et les acheteurs. Les études sur le carding et ses lieux de convergences ont fait ressortir plusieurs rôles : l'*administrateur*, le *modérateur*, le *vérificateur* et le *courtier financier* (Décary-Héту & Eudes, 2015; Holt et al., 2015; Dupont et al. 2016; Lusthaus, 2018). Tous ces rôles ont été questionnés et le choix de réponse "*Je n'ai jamais eu de rôle*" a été ajouté aux choix de réponses. La question qui suit mesurer cette variable pour les vendeurs : "*In the past 12 months, besides your seller activities, did you play an official role on an online website, online autoshop, online forum, online chat*

room or online market related to carding?”. Comme pour la variable précédente, cette question permet de constituer 5 variables dichotomiques pour chacune des possibilités.

Les moyens de paiements utilisés : demande aux participants de renseigner le ou les moyens de paiements qu'il a utilisés pour vendre ou acheter des produits du carding. L'ensemble des types de moyens de paiement en ligne y était questionné sous forme de choix de réponse multiple. Ainsi, les carders pouvaient déclarer utiliser des *cryptomonnaies pseudonymes* (ex. : Bitcoin, Litecoin), des *cryptomonnaies anonymes* (ex. : Monero, DASH, Zcash) et/ou des *services de transferts financiers légitimes* (ex. : PayPal, transferts bancaires, Western Union). Pour les acheteurs, cette variable était mesurée par la question suivante : *“In the past 12 months, when buying stolen financial information from an online website, online autoshop, online forum, online chat room or online market, did you use the following currencies or legitimate financial service?”*. De même que pour les trois précédentes, cette question amenait à la constitution de trois variables dichotomiques.

Section (II) Compétences et habiletés particulières :

L'utilisation de logiciels malveillants. Des travaux ont montré que certains vendeurs peuvent faire appel à des logiciels malveillants pour dérober des informations financières afin de les vendre sur les lieux de convergence (Holt & Lampke, 2010). Cette technique peut vraisemblablement être la plus efficace pour collecter un grand nombre de données financières qui peuvent équivaloir à de fortes sommes d'argent (Holz, Engelberth & Freiling, 2009). Ainsi, il a été demandé aux participants ayant déclaré être vendeurs si oui ou non ils avaient déjà utilisé un logiciel malveillant pour dérober des informations financières : *“In the past 12 months, did you ever use malware to steal financial information?”*. Cette variable dichotomique permettra de mesurer la présence de cette compétence particulière parmi les vendeurs.

Le fait d'avoir été recruté : mesure si le participant s'est déjà fait recruter dans un groupe d'au moins deux carders pour vendre des informations financières ou en monétiser suite à un achat. Beaucoup de recherches ont mis l'emphase sur le fait que les carders peuvent constituer une forme de criminalité organisée qui leur permet, par exemple, d'être plus résilients aux opérations policières (Sullivan, 2010; Décary-Hétu & Leppänen, 2013, Hazel, Kwon & Shakarian, 2018). Il est donc intéressant de constater l'impact d'un recrutement sur les revenus

criminels. C'est la question suivante qui mesurait cette variable pour les acheteurs : *“Were you ever recruited by a group of at least two people to help in the monetizing of stolen financial information?”*.

Le fait d'avoir été parrainé : le parrainage est l'un des dispositifs utilisés par les lieux de convergence pour contrôler la qualité des nouveaux participants et éviter les indésirables (Holt, 2007; Markham, 2011; Holt & Dupont, 2018; Lusthaus, 2018b). En mesurant si le participant s'est déjà fait parrainer ou non, il est possible de jeter un regard sur ses compétences. En effet, un parrainage pour devenir membre d'un lieu de convergence plus insulaire retranscrit le fait qu'un homologue aura déjà fait état de ses capacités. La question suivante mesurait cette variable dichotomique pour les vendeurs : *“To the best of your knowledge, on an online forum or an online chat room, did anyone ever publicly or privately vouch for your competence or ability to sell financial information?”*.

Mesure autoévaluée des compétences : cette question demandait au participant d'autoévaluer ses compétences à mener des activités de carding. Elle se déclinait en deux versions selon le profil déclaré. Le répondant pouvait alors s'évaluer sur une échelle de 0 à 10 qui mena à la constitution de cette variable continue. À titre d'exemple, voici la question destinée aux acheteurs : *“On a scale of 1 to 10 where 10 is the most competent and 1 is the least competent, how would you rate your competence at monetizing stolen financial information?”*.

Section (III) Expériences de victimisation endogène :

Fréquence des expériences de victimisation endogène : un pan de la recherche sur le carding soutient que les marchés de carding sont des marchés de tacos (Herley & Florêncio, 2010). Ceci implique la présence d'un phénomène de victimisation endogène entre les cardeurs. En effet, certains opportunistes vont en profiter pour vendre des produits de mauvaises qualités aux acheteurs. Aucune étude à ce jour ne s'est intéressée à mesurer la fréquence des expériences de victimisation subies par les acheteurs et leurs impacts sur la réussite financière de ces derniers. Ainsi, au cours du sondage, 6 questions interrogeaient exclusivement les acheteurs sur la fréquence de leurs expériences de victimisation. Chaque question proposait les mêmes choix de réponses, à savoir une échelle de 6 niveaux de fréquence, mais se transposait à chaque type de lieu de convergence pour offrir un regard plus précis sur la victimisation endogène

dépendamment du type de lieu de convergence. À titre d'exemple, voici la question portant sur les forums de discussion : *“In the past 12 months, how often were you scammed while buying stolen financial information on an online forum?”*.

Section (IV) Fréquence d'utilisations des technologies d'anonymat :

Fréquence d'utilisation des technologies d'anonymat : la mise en place de tactique a priori de la commission d'un crime peut être un prédicteur d'une meilleure réussite financière (Robitaille, 2004). Dans un contexte de cybercriminalité, cette mise en place de tactique peut s'exprimer par l'utilisation de technologies d'anonymat visant à réduire la traçabilité des activités illégales en ligne. Les 6 questions relatives à ce sujet constituaient une section à part entière du sondage disponible en une seule version et ce peu importe le rôle du participant. Six choix de réponses étaient possibles pour mesurer à quelle fréquence le participant utilisait la technologie questionnée (voir les questions 33 à 38 en annexe I). Elles y abordaient successivement l'utilisation : de *machines virtuelles*, de *systèmes d'exploitation préservant l'anonymat*, de *réseau virtuel privé (VPN)*, de *moyens de communication cryptés*, de *réseaux superposés* (ex. : *Tor*) et de *services de blanchiment d'argent en ligne* (ex. : *casinos en ligne*).

Section (V) Contacts :

Nombre de clients/vendeurs. Les lieux de convergence soutenant des marchés de carding abritent des communautés pouvant réunir de nombreux vendeurs et acheteurs. Ainsi, cette variable continue présente le nombre de clients/vendeurs avec lesquels le participant a eu affaire. Déclinée en deux versions selon le profil du participant, c'est la question suivante qui mesurait cette variable pour les vendeurs : *“In the past 12 months, how many customers did you have?”*.

Le nombre de collaborateurs non consentants. Cette variable continue mesure le nombre de collaborateurs qu'a eu le participant et qui ne sont pas conscients ou n'ont pas consenti à participer à des activités de carding. Elle s'intéressait principalement aux collaborateurs ayant procuré une aide de par leurs places dans une entreprise légitime. Elle se déclinait en deux versions pour chaque type de profil. À titre d'exemple, pour les acheteurs, elle était représentait par la question suivante : *“In the past 12 months, how many people facilitated your purchases of stolen financial information through their legitimate enterprises while not being aware of the illicit nature of your activities?”*.

Le nombre de collaborateurs consentants. Dans la continuité de la variable précédente, cette variable continue s'intéresse aux collaborateurs qui ont consciemment fourni une aide au participant lors de ses activités de carding. Pour les vendeurs, elle était mesurée grâce à la question suivante : “*In the past 12 months, how many people facilitated your purchases of stolen financial information through their legitimate enterprises while being aware of the illicit nature of your activities?*”.

Section (VI) Caractéristiques sociodémographiques :

La dernière section du sondage portait sur les caractéristiques sociodémographiques des carders. Les questions la composant étaient disponibles en une seule et même version pour tous les types de profils. La littérature ne renseignant que peu d'informations sociodémographiques à propos des carders, il était d'importance de questionner les participants sur ce type de variables pour obtenir un regard plus large sur ces délinquants et répondre à notre second objectif spécifique.

Âge : questionne les participants sur leur âge au moment de la passation du sondage. Plusieurs études s'accordent à dire que les cyberdélinquants sont en général des personnes relativement jeunes (Kshetri, 2006; Hutchings, 2014). Il sera alors attendu que les indices de tendance centrale de nos échantillons sur cette variable continue reflètent ce constat. Pour mesurer cette variable, la question suivante était posée : “*How old are you?*”.

Genre. Les communautés de carders seraient majoritairement composées d'hommes (Hutchings, 2014). La question interrogeant le genre du participant proposait 3 choix de réponses suivants : *hommes, femme, autre* et était la suivante : “*What is your gender?*”. Elle menait à la constitution d'une variable nominale.

Condamnation criminelle. La littérature sur la réussite criminelle soutenait que l'expérience pouvait s'exprimer au travers du nombre de condamnations reçues par le délinquant (Robitaille, 2004; Ouellet & Tremblay, 2014). Dans le cadre de ce projet, et dans un souci d'anonymat, il a été préféré de ne pas demander aux participants le nombre de condamnations dont ils avaient déjà fait l'objet. Plutôt, il leur était demandé de spécifier si oui ou non ils avaient déjà fait l'objet d'une condamnation.

Niveau d'éducation. Certaines études soutiennent que les cyberdélinquants sont des individus relativement éduqués (Kshetri, 2006). La démonstration de compétences techniques en informatique étant un vecteur de crédibilité (Lusthaus, 2012) mais nécessitant des apprentissages, il ne devrait pas être étonnant de trouver des individus ayant un bon niveau d'éducation au sein de nos échantillons. Pour mesurer cette variable une variable ordinale a été utilisée. Elle se basait sur la réponse à la question suivante : *“What is the highest level of education you have completed?”*. Elle proposait les 5 choix de réponses suivants : *No high school, High school, College diploma/Technical vocation, University degree* et *Graduate studies (Masters/Ph.D)*.

Revenus légitimes : Le fait d'avoir une activité légitime est un prédicteur d'une plus faible réussite criminelle au niveau financier (Robitaille, 2004; Thompson & Uggen, 2012; Rowan, McGloin & Nguyen, 2018). En mesurant les revenus légitimes, cette variable permettra à la fois de contrôler si le participant a une activité légitime générant des revenus mais aussi de comparer si les montants gagnés légitimement ont un impact sur les revenus gagnés lors d'activités de carding. C'est la question suivante qui mesure cette variable continue : *“In the past 12 months, how much did you earn in USD from your legitimate activities?”*.

Revenus illégitimes provenant d'autres activités criminelles : La spécialisation dans un type de délinquance est prédicteur d'une meilleure réussite criminelle (Tremblay & Morselli, 2000). Cette question demandait aux participants de préciser combien d'argent avaient-ils fait en commettant d'autres types de crimes que le carding et ce, au cours des 12 derniers mois. En comparant leurs réponses avec les revenus provenant du carding, il sera possible d'appréhender leurs degrés de spécialisation au niveau de leurs gains criminels. La question suivante était utilisée pour mesurer cette variable : *“In the past 12 months, how much did you earn in USD from other illegitimate activities?”*.

Heure(s) passée(s) par semaine à faire du carding : La fréquence des activités criminelles est corrélée positivement avec les revenus criminels (Tremblay & Morselli, 2000; Robitaille, 2004). Dans cette optique, il était important de questionner la fréquence horaire des activités des carders. Cette fréquence était demandée sur une semaine. Cette question était disponible en deux versions, l'une s'adressait aux vendeurs et l'autre aux acheteurs. À titre

d'exemple, voici la question destinée aux vendeurs : *“In the past 12 months, how many hours per week did you spend selling stolen financial information?”*.

Heure(s) passée(s) par semaine à faire d'autres activités criminelles. Comme pour la question mesurant les revenus illégitimes provenant d'autres activités criminelles, cette question cherchera à interroger le degré de spécialisation des répondants (Tremblay & Morselli, 2000). En mesurant le nombre d'heures par semaine à commettre d'autres types de crime que le carding, cette variable permettra de porter un regard horaire sur la spécialisation du participant. La question mesurant cette variable était la suivante : *“In the past 12 months, how many hours per week did you spend doing other criminal activities?”*.

Pour répondre au second objectif spécifique, l'ensemble de ces variables indépendantes seront analysées à l'aide de statistiques descriptives. Étant donné que la plupart d'entre elles sont à la fois disponibles pour les vendeurs et pour les acheteurs il sera intéressant de comparer les résultats entre ces deux types de profils au niveau échantillonnal. La section suivante explique la conceptualisation des prédicteurs construits à partir de ces différentes variables dont l'impact sur les revenus et les profits sera testé.

3.3. IDENTIFIER LES CARACTERISTIQUES PERSONNELLES ET SOCIALES QUI EXPLIQUENT LES REVENUS DES CARDEURS

Au cours de cette section, la confrontation entre le modèle théorique et le modèle testé empiriquement est présentée. L'opérationnalisation de la transposition au carding des différents prédicteurs ayant une influence sur la réussite criminelle y est présentée. En effet, lors du premier chapitre, un certain nombre de prédicteurs ayant une influence sur la réussite financière des délinquants a été mis en lumière. Ces prédicteurs ont été catégorisés en diverses dimensions et constituent le modèle théorique qui sera testé par nos données empiriques. Le tableau 8 récapitule l'ensemble des dimensions et prédicteurs identifiés ainsi que le sens du lien entre ces prédicteurs et la réussite criminelle. La dernière colonne précise si les prédicteurs ont été ou non mesurés au cours du sondage. De plus, certaines variables contrôles ont été aussi mesurées au cours du sondage pour conférer aux analyses plus de profondeur et d'en apprendre davantage sur les carders. Ces dernières sont présentées dans le tableau 9.

L'expérience :

Le modèle théorique développé identifie 5 prédicteurs qui ont une influence positive sur la réussite criminelle des délinquants. Premièrement, le nombre de condamnations passées est corrélé avec le fait d'avoir de plus grands revenus (Robitaille, 2004; Ouellet & Tremblay, 2014). Bien que seul le fait d'avoir été ou non *condamné criminellement* ait été demandé aux participants du sondage, il sera attendu, lors des analyses, que les participants présentant ces caractéristiques génèrent plus de *revenus* et de *profits* que ceux n'ayant jamais été condamnés.

Tableau 8. Dimensions, prédicteurs et modèle empirique

Dimension	Prédicteur et variation identifiés	Impact	Mesurée
Expérience	↑ Nombre de condamnations	↑	Oui
	↑ Compétences et habiletés	↑	Oui
	↑ Établissement de tactiques	↑	Oui
	↑ Spécialisation	↑	Oui
Activités criminelles/ marchandes	↑ Fréquence de consommation de	↑	Non
	↑ Déplacement(s)	↑	Non
	↑ Fréquence des activités	↑	Oui
	↑ Périodes d'inactivité criminelle	↓	Non
Sociabilité	↑ Présence de co-délinquants lors	↓	Oui
	↑ Nombres de pairs délinquants	↑	Non
	↑ Propension à collaborer	↑	Oui
	↑ Présence d'un mentor	↑	Non
	↑ Liens redondants	↑	Non
	↑ Place de leader	↑	Oui
Sociodémographiques	↑ Activité légitime	↓	Oui
	↑ Consommation d'alcool	↓	Non
	↓ Contrôle de soi	↑	Non
	↑ Stabilité de la vie affective	↓	Non

Deuxièmement, la littérature sur la réussite criminelle renseigne que le fait d'avoir des *compétences et habiletés particulières* accroît les revenus criminels (McCarthy et Hagan 2001; Morselli et Tremblay 2004; Morselli, Tremblay et McCarthy 2006; Ouellet & Tremblay, 2014; Ouellet, 2018). Dans le cadre du carding il a été vu que le fait de disposer de *compétences et*

habiletés particulières permet de participer plus efficacement aux activités marchandes en agissant comme un vecteur de crédibilité et de reconnaissance au sein des communautés (Lusthaus, 2012; Décary-Héту, Mousseau & Vidal, 2018). Ainsi, parmi l'ensemble des variables disponibles, 4 d'entre elles seront utilisées pour mesurer cette composante : *l'utilisation de logiciels malveillants* (uniquement pour les vendeurs), *le fait d'avoir été recruté*, *le fait d'avoir été parrainé* et *la mesure autoévaluée des compétences*. Il sera attendu que présenter ces caractéristiques ait un impact positif sur les *revenus* et les *profits*.

Troisièmement, *l'établissement de tactiques* est aussi un facteur prédisant une meilleure réussite criminelle (Robitaille, 2004). Dans le cadre de ce projet, ce prédicteur sera testé empiriquement au travers des 6 questions portant sur *la fréquence d'utilisation des technologies d'anonymat*. En effet, le script criminel du carding mentionne que lors de l'étape de *Préparation*, les carders mettent en place des stratégies pour protéger leurs identités (Hutchings & Holt, 2015; Hardeveld, Webber & O'Hara, 2017). Ainsi, il sera attendu que les participants les plus prévoyants, ayant une utilisation plus fréquente de technologies d'anonymat, présenteront de meilleurs *revenus* et *profits* que les autres.

Tableau 9. Dimensions et variables contrôles ajoutées

Dimension	Variables contrôles ajoutées
Expérience	Année de début des activités
Activités criminelles/ marchandes	Types de produits
	Types de lieux de convergence
	Moyens de paiements utilisés
	Fréquence des expériences de victimisation endogène
Sociodémographiques	Âge
	Genre
	Niveau d'éducation

Enfin, la *spécialisation* dans un type de criminalité a été identifiée comme un prédicteur ayant un impact positif sur la réussite (Tremblay & Morselli, 2000). Dans ce projet, ce prédicteur sera mesuré grâce à deux variables construites. Tout d'abord, *les heures par semaine à faire du carding* et *les heures par semaine à faire d'autres activités criminelles* serviront à calculer un ratio de *spécialisation* au niveau horaire. Une même démarche sera entreprise pour construire un ratio de *spécialisation* au niveau des gains en utilisant *les revenus du carding*, *les*

revenus illégitimes provenant d'autres activités criminelles et les revenus légitimes. Il sera attendu que plus ces ratios seront élevés, plus les *revenus* et les *profits* seront grands.

Au niveau de la dimension d'*expérience* une variable contrôle a été mesurée au cours du sondage. Il s'agit de *l'année de début des activités*. Cette dernière va permettre une mesure directe de *l'expérience* en renseignant depuis combien d'années le participant agi en tant que carder. Il sera attendu qu'un participant présentant plus d'années d'expérience affichera de meilleurs *revenus* et *profits*.

Les activités criminelles/marchandes

La dimension des *activités criminelles* comptait 5 prédicteurs de la réussite criminelle dont un a été mesuré par le sondage. Il s'agit de *la fréquence des activités* qui sera mesurée grâce à la variable des *heures passées à faire du carding*. Il sera bien entendu attendu que plus le participant déclarera avoir passé du temps à faire du carding, plus ses *revenus* et ses *profits* seront conséquents. À cette dimension ont été ajouté 3 variables contrôles demandant : *les types de produits, les types de lieux de convergence fréquentés et les moyens de paiements utilisés*. La littérature renseigne peu d'informations quant à l'impact de différences au niveau de ces variables sur les *revenus* et les *profits* glanés par les carders. Il sera donc intéressant de constater l'impact de ces variables sur les variables dépendantes.

Pour finir, dans le cas particulier des acheteurs, les 6 variables mesurant les *fréquences des expériences de victimisation endogène* sur les différents types de lieux de convergence sont aussi prises en compte dans le cadre de cette dimension. En présentant les marchés de carders comme des marchés pour tacos, Herley et Florêncio (2010) ont mis l'emphase sur le fait que les acheteurs puissent se faire eux-mêmes frauder lors de l'achat de produits du carding. Ceci nous permet de poser l'hypothèse soutenant que les acheteurs les plus victimisés gagnent moins étant donné que ce phénomène implique des pertes monétaires.

La sociabilité

En termes de *sociabilité*, le modèle théorique renseigne 6 prédicteurs influençant positivement la réussite des délinquants. Trois d'entre eux ont été mesurés au cours du sondage. Tout d'abord,

la présence de co-délinquants lors de la commission a un impact négatif sur les revenus criminels (Rowan, McGloin & Nguyen, 2018). Ce prédicteur sera testé à l'aide de la variable mesurant le *nombre de collaborateurs consentants*. Il sera attendu que plus le *nombre de collaborateurs consentants* sera élevé, moins les *revenus* et les *profits* seront importants.

Deuxièmement, il a été vu que la *propension à collaborer* a un impact positif sur la génération sur deux dimensions de la réussite criminelle : les revenus illégaux et l'accès à des opportunités criminelles (Tremblay & Morselli, 2000; Descormiers, Bouchard & Corrado, 2011). Ainsi, la variable renseignant si le participant *a déjà ou non été recruté* sera utilisée pour tester ce prédicteur. Bien qu'imparfaite, cette mesure permet tout de même de constater si le participant à une certaine *propension à collaborer*. Il sera intéressant de contraster l'impact de cette variable comparativement au *nombre de collaborateurs*. En effet, alors qu'il sera attendu que les participants ayant déjà été recrutés présentent de meilleurs *revenus*, un trop grand nombre de collaborateurs est censé réduire ces derniers.

Finalement, pour mesurer le fait d'avoir eu une *place de leader*, les variables questionnant *les rôles occupés sur les lieux de convergence* seront utilisées. En effet, Levitt et Venkatesh (2000) ont montré que le fait d'occuper une place de leader dans un contexte d'organisation criminelle permet d'avoir de plus hauts revenus criminels, et donc une meilleure réussite, que ceux qui n'occupent pas de place de leader. En faisant le lien avec le fait que les communautés de carding constituent une forme de criminalité organisée (Sullivan, 2010), les rôles d'administrateurs ou de modérateurs, peuvent jouer, de par leurs responsabilités, un rôle de leader au sein des communautés. Il sera alors attendu que les participants ayant déclaré occuper l'un de ces rôles présentent de plus forts *revenus*.

Caractéristiques sociodémographiques

Le travail de revue de littérature sur la réussite criminelle a mis en lumière 4 prédicteurs sociodémographiques qui ont un impact sur la réussite criminelle. Parmi eux, seul le fait d'avoir *une activité légitime* a été mesuré au cours du sondage. Les études montrent que présenter cette caractéristique prédit un revenu plus faible (Robitaille, 2004). Pour tester empiriquement ce prédicteur une variable dichotomique sera construite à l'aide de la variable mesurant *les revenus légitimes*. En effet, le fait de ne déclarer aucun revenu légitime témoigne du fait que le

répondant n'a pas d'activité légitime. Il sera attendu que les participants n'ayant déclaré aucun *revenu légitime* aient de moins bons *revenus* et *profits* provenant de leurs activités de carding.

Bien qu'il ait été vu dans la littérature sur le carding que les cyberdélinquants sont relativement jeunes (Kshetri, 2006; Hutchings, 2014), les travaux sur la réussite criminelle montrent que les délinquants plus âgés gagnent substantiellement plus d'argent (Robitaille, 2004; Ouellet & Tremblay, 2014). Dans le cadre de ce travail, c'est la variable mesurant l'*âge* du répondant sera utilisé pour tester empiriquement ce prédicteur. Il sera attendu que plus le participant sera âgé, plus ses *revenus* et *profits* provenant du carding seront élevés.

Les travaux menés auprès des carders stipulent que ces communautés sont principalement composées d'hommes (Hutchings, 2014). Les travaux sur la réussite criminelle s'attardent principalement à étudier en majorité des échantillons de délinquants masculins, cette caractéristique n'a pas été traitée en tant que prédicteur ou non de la réussite financière. Ce manque de connaissance ne permet pas de générer une hypothèse mais il sera intéressant de constater l'impact du *genre* sur les variables dépendantes.

Pour finir, Kshetri (2006) mentionne que les cyberdélinquants sont en général relativement éduqués comparativement aux autres types de délinquants. Néanmoins, aucun des travaux recensés dans la revue de littérature sur la réussite criminelle n'a testé cette variable sur la réussite criminelle. L'absence de cette variable dans le modèle théorique ne permet donc pas de générer une hypothèse. En traitant cette relation, il sera alors possible de constater si le *niveau d'éducation* influence la génération de *revenus* et de *profits* pour les carders.

3.4. LIMITES

Certaines limites méthodologiques ressortent du processus opérationnalisation des différentes variables en vue de répondre aux trois objectifs spécifiques de ce mémoire. Tout d'abord, le modèle empirique utilisé pour tester les différents prédicteurs est incomplet. En effet, les prédicteurs identifiés lors de la revue de la littérature sur la réussite criminelle ne sont pas tous questionnés. Deux points expliquent cette limite : premièrement, le fait de questionner l'ensemble des prédicteurs aurait mené à la constitution d'un sondage beaucoup trop long à être passé. Par exemple, implémenter une mesure du *contrôle de soi* requiert la présence de

nombreuses échelles permettant d'assurer une mesure fidèle et valide qui implique du temps lors de la passation. Décorte (2010) suggère une durée maximale de passation de 30 minutes et celle-ci ne pouvait pas respectée par une version étendue. À cela s'ajoute que certains des prédicteurs ne peuvent pas être transposés au carding. À titre d'exemple, mesurer le *temps passé dans la rue* ne s'inscrit pas vraiment dans un contexte de cybercriminalité.

Il était aussi important de questionner des caractéristiques propres aux activités des carders pour accroître la connaissance à leur sujet mais pour permettre d'ancrer ce phénomène criminel dans cette recherche qui s'intéresse à leur réussite financière. Ce choix soulève une autre limite qui veut que certaines variables n'ont pas d'ancrage théorique, car n'étant pas mentionnées dans le modèle théorique de la réussite criminelle, ou méthodologique (ex. : la *mesure autoévaluée des compétences*). Ceci nous contraint à ne pas pouvoir générer certaines hypothèses.

Pour finir, il est important de noter que le *design* du sondage est aussi imparfait. En effet, certaines questions n'ont pas été placées dans les sections les plus pertinentes. Par exemple, le fait de questionner *les heures passées par semaine à faire du carding* aurait été plus à sa place dans la section (II) *Activités marchandes* plutôt que dans la section (VI) *Caractéristiques sociodémographiques*. Ce point-ci soulève donc une limite relative à la traçabilité et à la continuité du processus d'opérationnalisation.

CHAPITRE 4 - ANALYSES ET RESULTATS

Dans ce chapitre sont présentés les résultats des analyses réalisées. Dans la plupart des cas, les variables étaient questionnées auprès des vendeurs et des acheteurs. Ainsi, une majorité des analyses a été effectuée sur les deux échantillons à l'étude. Tout d'abord, les deux premières sections présentent les analyses univariées menées pour répondre aux deux premiers objectifs spécifiques. Elles mesurent les revenus criminels des carders ainsi que leurs caractéristiques personnelles et sociales. La confrontation des résultats entre les deux échantillons permet de comparer les deux types de profils au niveau échantillonnal. Par la suite, la troisième section présente les analyses bivariées mettant en lumière les associations entre les variables dépendantes et les variables indépendantes.

4.1. MESURER LES REVENUS CRIMINELS DES CARDERS

Les deux variables dépendantes de cette étude sont les *revenus* et les *profits* des carders. Elles ont été analysées sur chacun des deux échantillons. Pour rappel, ces mesures sont annuelles; elles étaient questionnées sur une période de 12 mois. Le tableau 10 présente les indices de tendance centrale et de dispersion de ces deux variables.

Tableau 10. Indices de tendance centrale et de dispersion pour les revenus et les profits

	n	Mdn	M	É.t.	Min	Max
Vendeurs						
Revenus	24	11,000\$	45,592\$	74,434\$	100\$	300,000\$
Profits	24	11,000\$	25,334\$	36,531\$	100\$	120,000\$
Acheteurs						
Revenus	36	24,500\$	71,605\$	115,959\$	300\$	500,000\$
Profits	36	19,000\$	51,677\$	87,676\$	150\$	400,000\$

Tout d'abord, l'observation des minimums et maximums des quatre distributions montrent d'importantes différences de revenus au sein des deux échantillons. En effet, que ce soit pour les *revenus* ou les *profits*, les minimums témoignent que des répondants ont peu gagné au cours des 12 derniers mois. À titre d'exemple, le vendeur et l'acheteur ayant généré le moins de *profits* n'ont déclaré qu'une centaine de dollars (respectivement Min = 100\$ et Min = 150\$). A contrario, les maximums montrent que d'autres carders ont déclaré des *revenus* et des *profits* élevés. Ceci est particulièrement probant pour l'acheteur qui revendique 400,000\$ de *profits* au

cours des 12 derniers mois. Les acheteurs interrogés ont un *profit* moyen supérieur à celui des vendeurs (respectivement $M = 51,677\$$ et $M = 25,334\$$).

D'un point de vue plus général, une majorité des carders ont généré des *revenus* et des *profits* relativement modestes sur cette période comme en attestent les médianes. Par exemple, la moitié des vendeurs ont fait 11,000\$ ou moins de *profits* ou de *revenus*. Le constat fait plus haut qui concédait d'importantes différences de réussite au sein des échantillons est nettement appuyé par les écarts-types et les moyennes. En effet, dans toutes les distributions les écarts-types sont largement supérieurs aux moyennes. Ceci suggère de fortes dispersions des *revenus* et des *profits* entre les participants. En résumé, ces résultats permettent de conforter le fait qu'il y a d'importantes différences en termes de réussite criminelle au sein des deux échantillons mais aussi qu'une majorité des carders n'ont pas engendré des *profits* importants au cours des 12 derniers mois.

4.2. MESURER LES CARACTERISTIQUES PERSONNELLES ET SOCIALES DES CARDERS

Les différentes variables indépendantes de cette étude se répartissaient au sein de 6 parties qui décomposaient le sondage. Ainsi, les sous-sections suivantes présentent les analyses univariées réalisées pour chacune des variables questionnées au cours de ces parties. La prochaine sous-section présente ces analyses pour les *Activités marchandes* des carders. Elles visaient, par exemple, à mesurer *l'année de début des activités* ou encore les *types de produits* utilisés.

4.2.1. ACTIVITES MARCHANDES

Les résultats présentés dans le tableau 11 montrent que la moitié des vendeurs a déclaré avoir commencé leur activité de carding en 2016 ($Mdn = 2016$). Étant donné qu'un répondant peut au maximum avoir démarré au mois de décembre de l'année qu'il mentionne, et que le sondage a été lancé officiellement le 6 décembre 2018, ce résultat montre que la moitié des vendeurs de l'échantillon participent à de telles activités depuis au moins 2 ans. Néanmoins, ce constat n'est pas consistant avec la moyenne de l'échantillon qui se situe en 2015 ($M = 2015$). Cette inconsistance est d'autant plus soulignée par l'écart-type qui précise qu'il y a une différence

moyenne d'environ 2 ans et 5 mois entre deux vendeurs. Cette différence est considérée comme importante compte tenu de l'étendue des réponses (Min = 2010 et Max = 2018). Malgré ces variations, et de manière générale, les vendeurs de l'échantillon peuvent être considérés comme relativement expérimentés en termes de temps.

Tableau 11. Indice de tendance centrale et de dispersion pour l'année de début des activités et les nombres de produits

	n	Mdn	M	É.t.	Min	Max
Vendeurs						
Année de début	24	2016	2015	2	2010	2018
Nombre de produits vendus	24	1,250	2,019	2,572	2	2,010
Acheteurs						
Année de début	36	2014	2013	3.12	2006	2018
Nombre de produits achetés	36	325	3,267	10,068	3	60,000

Les acheteurs, quant à eux, ont en moyenne démarré leurs activités plus tôt de deux ans que les vendeurs interrogés (M = 2013). Ce constat se répète à la comparaison des médianes des deux échantillons (respectivement Mdn = 2016 pour les vendeurs et Mdn = 2014 pour les acheteurs). Bien qu'il y ait une forte dispersion des réponses parmi les acheteurs (É.t. = 3), ces derniers agissent depuis plus longtemps, en moyenne et en médiane, que leurs homologues vendeurs.

Le tableau 11 présente aussi les analyses descriptives des *nombres de produits achetés et vendus* par les participants. Il n'est pas étonnant de constater que les vendeurs ont, en médiane, vendu plus de produits que les acheteurs revendiquent en avoir acheté (respectivement Mdn = 1,250 et Mdn = 325). En effet, étant donné que la vente constitue le cœur de leur activité, les vendeurs multiplient les transactions pour pouvoir augmenter leurs revenus. Cependant, cette interprétation s'oppose au fait que les acheteurs ont acquis, en moyenne, plus de 3,000 produits (M = 3,267). L'écart-type de la distribution des acheteurs suggère une très forte variation du *nombre de produits achetés* selon les acheteurs. En effet, il y a en moyenne une différence de 10,068 entre deux acheteurs de l'échantillon. Ces résultats sont vraisemblablement influencés par le maximum élevé de la distribution (Max = 60,000).

La section des *Activités marchandes* questionnait aussi plusieurs variables dichotomiques par exemple, les *types de produits* ou les *moyens de paiement* utilisés. Les répondants avaient le

choix de sélectionner une ou plusieurs réponses. À titre d'exemple, un répondant peut déclarer utiliser tous les types de produits alors qu'un autre peut simplement n'en mentionner qu'un seul. Le tableau 12 présente les proportions des réponses pour chacune de ces variables dans les cas des deux échantillons.

Au niveau des types de produits, les *Fullz* se distinguent dans les deux échantillons comme étant le type de produit le plus prévalent. En effet, 75% des vendeurs (n = 18) ont déclaré en vendre et près de 70% des acheteurs (n = 25) en monétisent. L'utilisation des *CVV* et des *identifiants de comptes en ligne* est modérément populaire au sein des deux échantillons. À titre d'exemple, 54% des vendeurs (n = 13) proposent des *CVV* et la moitié des acheteurs (n = 18) achètent des *identifiants de comptes en ligne*. Finalement, les *Dumps* sont les types de produits les moins mentionnés dans les deux échantillons (respectivement 42% ; n = 10 pour les vendeurs et 25% ; n = 9 pour les acheteurs).

Contrairement aux *types de produits* dont les distributions restent similaires entre les vendeurs et les acheteurs, les distributions des *types de lieux de convergence* sont différentes. Une large majorité des vendeurs interrogés utilisent des *salles de clavardages* pour vendre leurs produits (n = 18 ; 75%). Ce type de lieux de convergence est plus populaire auprès des vendeurs que les *forums* (n = 13 ; 54%), les *sites web* (n = 10 ; 42%) ou les *cryptomarchés* (n = 10 ; 42%). Les *carding shops* sont le type de lieux de convergence le moins utilisés par les vendeurs (n = 7 ; 29%). Pour les acheteurs, les *cryptomarchés* se distinguent comme étant le type le plus utilisé par les répondants (n = 20 ; 56%). Ce constat se répète pour les *carding shops* qui sont le deuxième type plébiscité par les acheteurs (n = 17 ; 47%).

Comparativement à l'échantillon des vendeurs, les acheteurs ayant participé au sondage sont en moins grande proportion à avoir déclaré occuper des *rôles* sur les lieux de convergence. En effet, près de 70% d'entre ont déclaré n'occuper *aucun rôle* alors que 66% des vendeurs ont déclaré au moins un rôle occupé (Pas de rôle = 33% pour les vendeurs). Il est aussi intéressant de noter que le rôle le plus mentionné par les vendeurs est celui d'*administrateur* (n = 9 ; 38%). Ce constat peut être interprété comme un artefact de la grande proportion de vendeurs évoluant sur les *salles de clavardages*. En effet, ce type de lieux de convergence ne nécessite pas d'investissement particulier pour constituer un groupe de discussion et en être administrateur. En quelques cliques, il est possible de créer un groupe et d'y inviter rapidement plusieurs

dizaines de personnes. Il aurait été tout de même intéressant de questionner les rôles en fonction des lieux de convergence car il est, par exemple, plus précieux d'être *administrateur* sur un *cryptomarché* que sur une *salle de clavardage*. Pour finir, au niveau des *moyens de paiements* utilisés, les analyses montrent une très forte prévalence des *cryptomonnaies pseudonymes* (respectivement n = 24 ; 100% pour les vendeurs et n = 33 ; 92% pour les acheteurs).

Tableau 12. Proportions des types de produits, types de lieux de convergence, rôles occupés et moyens de paiement

	Vendeurs		Acheteurs	
	n	%	n	%
Types de produits	24	100%	36	100%
Dumps	10	42%	9	25%
Fullz	18	75%	25	69%
CVV	13	54%	17	47%
Identifiants de compte en ligne	13	54%	18	50%
Types de lieux de convergence	24	100%	36	100%
Site web	10	42%	12	33%
Carding shops	7	29%	17	47%
Forum	13	54%	10	28%
Salle de clavardage	18	75%	15	42%
Cryptomarchés	10	42%	20	56%
Rôles occupés	24	100%	36	100%
Administrateur	9	38%	4	11%
Modérateur	6	25%	5	14%
Vérificateur	4	17%	2	6%
Courtier financier	7	29%	4	11%
Pas de rôle	8	33%	25	69%
Moyens de paiements	24	100%	36	100%
Cryptomonnaies pseudonymes	24	100%	33	92%
Cryptomonnaies anonymes	4	17%	11	31%
Transferts financiers légitimes	9	38%	7	19%

4.2.2. HABILITES ET COMPETENCES PARTICULIERES

La section du sondage questionnant les *habiletés et compétences particulières* s'articulait autour de 3 à 4 variables selon le profil du répondant. Pour rappel, les vendeurs avaient une question supplémentaire portant sur l'*utilisation de logiciel malveillant*. Le tableau 13 présente les analyses univariées des variables interrogées lors de cette section dans les cas des deux échantillons.

Tableau 13. Statistiques descriptives des variables dichotomiques des habiletés et compétences particulières

	Vendeurs		Acheteurs	
	n	%	n	%
Utilisation de logiciels malveillants	12	50%	-	-
Recruté	16	67%	20	56%
Parrainé	23	96%	25	69%

Tableau 14. Statistiques descriptives des mesures autoévaluées des compétences

	n	%	Mdn	M	É.t.	Min	Max
Vendeurs							
Mesure autoévaluée des compétences	24	100%	7	7	2	4	10
Acheteurs							
Mesure autoévaluée des compétences	36	100%	6	6	2	2	10

Les résultats du tableau 13 montrent que la moitié des vendeurs interrogés ont déclaré avoir déjà utilisé de tels logiciels pour dérober des données (n = 12 ; 50%). Ce résultat suggère que cette compétence n'est pas conditionnelle à la vente de produits du carding. En effet, la littérature mentionne d'autres techniques, comme le *phishing* ou le *skimming*, qui permettent de dérober des informations financières (Peretti, 2008; Holt & Bossler, 2016). Que ce soit pour les vendeurs ou les acheteurs, les deux distributions montrent qu'une majorité d'entre eux ont déjà été *recrutés* pour leurs compétences à mener des activités de ventes ou d'achats (respectivement n = 16 ; 67% pour les vendeurs et n = 20 ; 56% pour les acheteurs). Le *parrainage* permet d'accéder à certains lieux de convergence plus prisés et participe à la construction d'une meilleure réputation. Les vendeurs sont quasiment la totalité à avoir déjà été *parrainé* (n = 23 ; 96%). Au niveau des *mesures autoévaluée des compétences*, les vendeurs ont, en moyenne, précisé être plus performants sur une échelle de 0 à 10 que les acheteurs (respectivement M =

7.26 et $M = 6.84$). Bien que la nature des activités des vendeurs et des acheteurs soit différente, les mesures utilisées dans le cadre de cette recherche font ressortir les vendeurs comme se considérant plus compétents.

4.2.3. EXPERIENCES DE VICTIMISATION ENDOGENE

Les *expériences de victimisation endogène* dans le cadre des activités des acheteurs se réfèrent au fait d'obtenir des produits du carding de mauvaise qualité voir aucun produit du tout après l'achat (Motoyama et al., 2010). Le tableau 14 présente les *fréquences des expériences de victimisation endogène* en fonction des *types lieux de convergence*. Les pourcentages cumulés sont aussi présentés afin d'apporter plus de profondeur aux analyses. En effet, étant donné la nature ordinale des mesures utilisées, il était possible de considérer que les répondants ayant déclaré une fréquence plus importante peuvent être inclus dans les catégories inférieures. À titre d'exemple, dans le cas des *sites web*, 1 acheteur a déclaré s'être fait victimiser sur ce type de lieux de convergence *100% du temps* et 4 *au moins 75% du temps* lors de leurs activités de carding. Ainsi, 5 acheteurs (14%) ont été victimisés sur ce type *au moins 75% du temps*.

De manière générale, sans distinction de type de lieux de convergence, une petite proportion des acheteurs ont déclaré *ne jamais s'être fait arnaquer* lors de l'achat d'un produit ($n = 6$; 17%). La problématique de la victimisation endogène est donc relativement présente au sein de l'échantillon. Cependant, cette fréquence est à nuancer dans la mesure où les pourcentages cumulés montrent que seuls 8 acheteurs ont déclaré s'être fait arnaquer pour *au moins 50% du temps* (22%). Ceci permet de noter la présence de ce phénomène mais aussi que sa fréquence générale reste relativement peu élevée au sein de l'échantillon.

En nous penchant plus précisément sur les types de lieux de convergence, les *cryptomarchés* semblent être le type de lieu de convergence où les acheteurs se sont fait le moins arnaquer. En effet, 21 acheteurs (58%) *n'ont jamais été victimisés* sur les cryptomarchés. Ce constat se retranscrit bien aussi au travers du fait que seuls 6 carders (17%) ont précisé s'être fait arnaquer *au moins 50% du temps* sur ce type de lieux de convergence. Un constat relativement similaire peut être fait pour les forums. La moitié des participants ont déclaré *ne jamais s'être fait arnaquer* sur les forums et seul 6 d'entre eux (17%) ont déclaré l'avoir été pour *au moins 50% du temps*. Pour finir, les *carding shops* ressortent comme étant le type de lieu de convergence

affichant le plus de victimisation endogène. C'est pour ce type que les participants ont déclaré avoir été le plus arnaqués (n = 13 ; 64%).

Tableau 15. Fréquences des expériences de victimisation endogène selon les types de lieux de convergence

Fréquences des victimisations	n	%	% cumulés
Général	36	100%	
100% du temps	1	3%	-
Au moins 75% du temps	5	14%	17%
Au moins 50% du temps	2	6%	22%
Au moins 25% du temps	8	22%	44%
Moins de 25% du temps	14	39%	83%
Jamais	6	17%	-
Site Web	36	100%	
100% du temps	1	3%	-
Au moins 75% du temps	4	11%	14%
Au moins 50% du temps	5	14%	28%
Au moins 25% du temps	2	6%	33%
Moins de 25% du temps	7	19%	53%
Jamais	17	47%	-
Carding shops	36	100%	
100% du temps	1	3%	-
Au moins 75% du temps	2	6%	8%
Au moins 50% du temps	7	19%	28%
Au moins 25% du temps	4	11%	39%
Moins de 25% du temps	9	25%	64%
Jamais	13	36%	-
Forum	36	100%	
100% du temps	4	11%	-
Au moins 75% du temps	1	3%	14%
Au moins 50% du temps	1	3%	17%
Au moins 25% du temps	5	14%	31%
Moins de 25% du temps	7	19%	50%
Jamais	18	50%	-
Salle de clavardage	36	100%	
100% du temps	4	11%	-
Au moins 75% du temps	5	14%	25%
Au moins 50% du temps	2	6%	26%
Au moins 25% du temps	5	14%	39%
Moins de 25% du temps	5	14%	53%
Jamais	15	42%	-
Cryptomarchés	36	100%	
100% du temps	4	11%	-
Au moins 75% du temps	0	0%	11%
Au moins 50% du temps	2	6%	17%
Au moins 25% du temps	4	11%	28%
Moins de 25% du temps	5	14%	42%
Jamais	21	58%	-

4.2.4. FREQUENCE D'UTILISATION DES TECHNOLOGIES D'ANONYMAT

Bien que la littérature ait souligné l'importance que revêt l'*utilisation de technologie d'anonymat* dans le cadre des activités des carders (Décary-Héту & Leppänen, 2013; Yip, Webber & Shadbolt, 2013; Hardeveld, Webber & O'Hara, 2016; Hardeveld, Webber & O'Hara, 2017), aucune étude, à notre connaissance, ne s'est penchée sur la fréquence d'utilisation des principales technologies d'anonymat dans le cadre du carding. Le tableau 15 présente les distributions des *fréquences d'utilisation des différentes technologies d'anonymat* pour les vendeurs et les acheteurs. La même démarche utilisée dans le cadre des résultats des expériences de victimisation endogène soutient le calcul des pourcentages cumulés.

Les *réseaux virtuels privés* ressortent comme étant la technologie d'anonymat la plus utilisée par les carders, qu'ils soient vendeurs ou acheteurs. En effet, dans les deux échantillons plus de la moitié des participants ont déclaré utiliser des *réseaux virtuels privés 100% du temps* et seulement 8% ont déclaré *ne jamais en utiliser*. Cela se retranscrit bien au travers des pourcentages cumulés qui montrent qu'une large majorité des carders a déclaré utiliser des *réseaux virtuels privés plus de 50% du temps* (respectivement 79% pour les vendeurs et 89% pour les acheteurs). Le second type de technologie d'anonymat le plus souvent utilisé par les carders interrogés est les *réseaux superposés* (Darknets). Bien que les proportions de participants ayant déclaré utiliser pour *100% du temps* les *réseaux superposés* soient en-deçà des réponses aux proportions analogues pour les autres technologies d'anonymat, l'observation des pourcentages cumulés permet d'entrevoir la prévalence de l'utilisation de ce type de technologie d'anonymat. En effet, dans les deux distributions, plus de 60% des carders utilisent pour *au moins 50% du temps* les *réseaux superposés* dans le cadre de leurs activités de carding.

Une même tendance est aussi observée pour les *services de blanchiment d'argent* qui comptent, dans les deux distributions, parmi les plus grandes proportions de participants ayant déclaré utiliser cette technologie d'anonymat pour *100% du temps* (respectivement n = 11 ; 46% pour les vendeurs et n = 11 ; 31%). Ce constat se retranscrit aussi au travers des pourcentages cumulés des deux échantillons qui montrent qu'environ 60% des répondants ont déclaré y faire appel pour *au moins 50% du temps*. Il est tout de même intéressant de noter qu'une part non négligeable des répondants a déclaré *ne jamais en utiliser* (particulièrement dans le cas des vendeurs n = 7 ; 29%).

Tableau 16. Fréquences d'utilisation des différentes technologies d'anonymat

	Vendeurs (n = 24)			Acheteurs (n = 36)		
	n	%	% cumulés	n	%	% cumulés
Machine virtuelle						
100% du temps	8	33%	-	11	31%	-
Au moins 75% du temps	4	17%	50%	2	6%	36%
Au moins 50% du temps	3	13%	63%	6	17%	53%
Au moins 25% du temps	2	8%	71%	4	11%	64%
Moins de 25% du temps	2	8%	79%	4	11%	75%
Jamais	5	21%	-	9	25%	-
Systèmes d'exploitation anonymes						
100% du temps	8	33%	-	13	36%	-
Au moins 75% du temps	2	8%	42%	1	3%	39%
Au moins 50% du temps	0	0%	42%	1	3%	42%
Au moins 25% du temps	2	8%	50%	2	6%	47%
Moins de 25% du temps	3	13%	63%	8	22%	69%
Jamais	9	38%	-	11	31%	-
Réseaux virtuels privés						
100% du temps	14	58%	-	20	56%	-
Au moins 75% du temps	3	13%	71%	6	17%	72%
Au moins 50% du temps	2	8%	79%	6	17%	89%
Au moins 25% du temps	1	4%	83%	0	0%	89%
Moins de 25% du temps	2	8%	92%	1	3%	92%
Jamais	2	8%	-	3	8%	-
Communications encryptées						
100% du temps	9	38%	-	9	25%	-
Au moins 75% du temps	3	13%	50%	6	17%	42%
Au moins 50% du temps	2	8%	58%	5	14%	56%
Au moins 25% du temps	2	8%	67%	0	0%	56%
Moins de 25% du temps	5	21%	87%	5	14%	69%
Jamais	3	13%	-	11	31%	-
Réseaux superposés (Darknets)						
100% du temps	7	29%	-	11	31%	31%
Au moins 75% du temps	2	8%	38%	6	17%	47%
Au moins 50% du temps	6	25%	63%	6	17%	64%
Au moins 25% du temps	1	4%	67%	3	8%	72%
Moins de 25% du temps	3	13%	79%	4	11%	83%
Jamais	5	21%	-	6	17%	-
Services de blanchiment d'argent						
100% du temps	11	46%	-	11	31%	-
Au moins 75% du temps	2	8%	54%	8	22%	53%
Au moins 50% du temps	2	8%	63%	2	6%	58%
Au moins 25% du temps	0	0%	63%	4	11%	69%
Moins de 25% du temps	2	8%	71%	4	11%	80%
Jamais	7	29%	-	7	19%	-

Enfin, les systèmes d'exploitation garantissant l'anonymat constituent la technologie d'anonymat la moins utilisée par les répondants. En effet, c'est le type pour lequel les plus grandes proportions de répondants ont déclaré ne jamais l'utiliser dans les deux échantillons (respectivement $n = 9$; 38% pour les vendeurs et $n = 11$; 31% pour les acheteurs). Ce constat se répète à l'observation des pourcentages cumulés. En effet, il s'agit du seul type n'affichant pas une majorité de répondants ayant déclaré l'utiliser *au moins 50% du temps* (42% pour les vendeurs et les acheteurs).

4.2.5. CONTACTS

La section *Contacts* du sondage regroupait trois mesures questionnant les carders sur la nature de leurs relations d'affaires. Ainsi, il était par exemple demandé aux vendeurs le nombre de clients avec qui ils avaient fait affaire au cours des 12 derniers mois et aux acheteurs à combien de vendeurs différents avaient-ils acheté sur la même période. Le tableau 16 présente les résultats des analyses univariées menées sur les variables de cette section.

Tableau 17. Indices de tendance centrale et de dispersion des mesures des contacts

	n	Mdn	M	É.t.	Min	Max
Vendeurs						
Nombre de clients	24	160	344	499	1	2,000
Collaborateurs non consentants	24	7	169	412	0	2,000
Collaborateurs consentants	24	15	59	109	0	500
Acheteurs						
Nombre de vendeurs	36	9	95	266	0	1,200
Collaborateurs non consentants	36	3	40	93	0	500
Collaborateurs consentants	36	6	34	88	0	500

Il n'est pas étonnant de constater que le *nombre de vendeurs* soit en médiane moins élevé que le *nombre de clients* (respectivement $Mdn = 9$ et $Mdn = 160$). Logiquement, les acheteurs préfèrent entretenir des relations avec un petit contingent de vendeurs avec qui ils pourront nouer une relation de confiance afin d'obtenir des produits de bonne qualité à des prix intéressants. À l'inverse, les vendeurs multiplient les clients pour pouvoir effectuer plus de ventes et ainsi gagner plus d'argent. Malgré cette tendance, il demeure que ces deux distributions présentent de fortes dispersions comme en témoignent les écarts-types largement supérieurs aux moyennes (respectivement $É.t. = 499$ pour les vendeurs et $É.t. = 263$ pour les

acheteurs). Ceci s'explique par la présence de valeurs extrêmes dans ces distributions. À titre d'exemple, l'un des participants a déclaré avoir eu affaire avec près de 1,200 vendeurs. Cette observation entre en contradiction avec le rationnel émis plus haut. En effet, si une majorité de carders achète auprès d'un petit contingent de vendeurs, cet acheteur a multiplié les vendeurs avec qui il a fait affaire.

Le *nombre de collaborateurs non consentants* présente le nombre de personnes qui ont facilité l'achat ou la vente de produits du carding de par leur emploi légitime sans être conscientes de participer à une entreprise criminelle. Il pouvait par exemple s'agir de personne recruter pour effectuer des transferts d'argent via leurs comptes sans savoir que l'argent provient d'une fraude. À l'inverse, le *nombre de collaborateurs consentants* demandait combien de personnes du même type étaient conscientes de participer à cette activité criminelle. Dans le cas du *nombre de collaborateurs non consentants* rapporté par les répondants, les résultats montrent une très importante dispersion des distributions (par exemple, É.t. = 412 pour les vendeurs). Un même constat peut être fait dans le cadre des *collaborateurs consentants* (par exemple, É.t. = 88 pour les acheteurs). Au vu des importantes étendues dans ces deux distributions, il semble que ce ne sont pas tous les carders qui font appel à ce type de collaborateurs dans le cadre de leurs activités de carding.

4.2.6. CARACTERISTIQUES SOCIODEMOGRAPHIQUES

Cette dernière sous-section présente les résultats des analyses univariées menées sur les variables s'intéressant aux caractéristiques sociodémographiques des carders. Le tableau 17 récapitule ces résultats.

Les distributions du *niveau d'éducation* chez les vendeurs et les acheteurs montrent que, dans l'ensemble, les carders sont relativement éduqués. En effet, dans chacun des deux échantillons, seuls 17% des répondants ont spécifié ne pas avoir obtenu de diplôme secondaire (respectivement $n = 4$ pour les vendeurs et $n = 6$ pour les acheteurs). Il est aussi intéressant de noter que la tendance générale veut que les vendeurs soient plus éduqués que les acheteurs au niveau des deux échantillons. Ceci se retranscrit bien au travers du fait que près de 40% des vendeurs ont mentionné avoir au moins un diplôme universitaire alors qu'ils sont environ 30% dans l'échantillon des acheteurs.

À ce propos, les résultats quant aux *âges* des répondants restent relativement consistants entre les deux distributions. En effet, les carders sont relativement jeunes avec des médianes et des moyennes se situant autour de 24 ans (Mdn = 24 ; M = 25 pour les vendeurs et les acheteurs). Il est aussi observé que les deux échantillons comptent une majorité d'*hommes* en leur sein (respectivement n = 21 ; 88% pour les vendeurs et n = 29 ; 81% pour les acheteurs).

Tableau 18. Analyses descriptives des caractéristiques sociodémographiques

	Vendeurs (n = 24)		Acheteurs (n = 36)				
	n	%	n	%			
Niveau d'éducation							
Pas de secondaire	4	17%	6	17%			
Secondaire	7	29%	16	44%			
Diplôme collégial	3	13%	3	8%			
Baccalauréat	5	21%	5	14%			
Études graduées (M.Sc/Ph.D)	5	21%	6	17%			
Homme	21	88%	29	81%			
Condamnation criminelle (Oui)	5	21%	7	19%			
Activité légitime (Oui)	18	75%	29	81%			
	n	%	Mdn	M	É.t.	Min	Max
Vendeurs							
Âge	24	-	24	25	7	18	46
Revenus légitimes	24	-	12,000\$	16,100\$	18,427\$	0\$	70,000\$
Revenus illégitimes (autres)	24	-	2,100\$	25,276\$	56,225\$	0\$	250,000\$
Heures carding (achat)	24	-	18	18	8	2	35
Heures non carding	24	-	10	12	13	0	50
Spécialisation horaire	24	-	0.67	0.65	0.26	0.06	1
Spécialisation revenus	24	-	0.70	0.63	0.38	0.02	1
Acheteurs							
Âge	36	-	24	25	5	18	45
Revenus légitimes	36	-	12,000\$	19,104\$	24,910\$	0\$	120,000\$
Revenus illégitimes (autres)	36	-	6,500\$	30,101\$	54,979\$	0\$	250,000\$
Heures carding (vente)	36	-	21	20	11	2	46
Heures non carding	36	-	10	11	1	0	40
Spécialisation horaire	36	-	0.69	0.68	0.24	0.05	1
Spécialisation revenus	36	-	0.69	0.67	0.30	0.11	1

Les résultats des analyses du fait d'avoir été *condamnés criminellement* ressortent comme consistants entre les deux échantillons. En effet, dans les deux cas près de 20% des répondants ont spécifié avoir déjà fait l'objet d'une condamnation criminelle. Ce chiffre peut être considéré comme relativement important mais demeurera difficile à interpréter dans la mesure où il n'est pas possible de savoir pour quels types et pour combien d'offenses il y a eu condamnation.

Les revenus légitimes ont été utilisés pour calculer la proportion de répondants occupant une *activité légitime*. Lorsqu'aucun revenu légitime n'était précisé par un carder, il était considéré qu'il n'occupait pas d'emploi au cours des 12 derniers mois. Dans le cas des deux distributions, une majorité des carders occupait une activité légitime qui leur permettait de générer des revenus au cours des 12 derniers mois. Ils représentaient 75% dans le cas des vendeurs (n = 18) et près de 80% dans le cas des acheteurs.

Les distributions des *revenus légitimes* entre les deux échantillons présentent certaines similitudes. En effet, les médianes sont identiques et montrent que la moitié des carders interrogés ont gagné 12,000\$ ou moins grâce à une activité légitime au cours des 12 derniers mois. De plus, l'observation des écarts-types suggère qu'il existe de fortes dispersions des revenus légitimes dans les deux distributions (respectivement É.t. = 18,427\$ pour les vendeurs et É.t. = 24,910\$ pour les acheteurs). Ceci peut d'ailleurs s'expliquer par les étendues importantes des deux distributions. À titre d'exemple, un participant a déclaré avoir gagné 120,000\$ en revenus légitimes au cours des 12 derniers mois alors qu'un autre n'a généré aucune entrée d'argent légitimement.

Une même tendance peut être observée pour les *revenus illégitimes provenant d'autres activités illégales* que le carding. En effet, bien que leurs médianes et moyennes soient quelque peu différentes, les deux distributions présentent surtout de très fortes dispersions (respectivement É.t. = 56,225\$ pour les vendeurs et É.t. = 54,979\$ pour les acheteurs). Comme précédemment, cette observation est appuyée par les étendues des deux distributions.

Les deux échantillons présentent des similitudes quant aux heures passées par semaine à faire des activités de carding. En effet, en moyenne et médiane les répondants ont mentionné y passer entre 17 et 20 heures. Alors que certains ont mentionné s'y consacrer à temps plein (respectivement Max = 35 pour les vendeurs et Max = 46 pour les acheteurs), d'autres n'y consacrent pas beaucoup de temps (Min = 2 pour les vendeurs et les acheteurs). Il est intéressant de comparer ces résultats à ceux obtenus pour le nombre d'heures passées à faire d'autres activités criminelles que le carding. De manière générale, il n'est pas étonnant de constater qu'en moyenne et médiane, les répondants passent moins de temps à effectuer d'autres types d'offenses. Le carding est donc, pour une majorité des répondants, le cœur de leurs activités criminelles au niveau horaire.

Dans les deux cas, il est aussi intéressant de noter que la moitié des répondants passent au moins une dizaine d'heures par semaine à commettre d'autres types d'offenses (Mdn = 10 pour les vendeurs et les acheteurs). Comme pour le carding, certains répondants participent à d'autres formes d'activités criminelles à temps plein (respectivement Max = 50 pour les vendeurs et Max = 40 pour les acheteurs), alors que d'autres semblent être uniquement spécialisés dans le carding (Min = 0).

La spécialisation horaire était calculée en effectuant un ratio entre le nombre d'heures passées à faire des activités de carding par semaine et la somme des heures passées à faire des activités criminelles (carding et autres). Dans les deux échantillons, les distributions de ces indices sont très similaires. Elles confortent le fait que certains carders sont spécialisés dans cette forme de criminalité (Max = 1) et que d'autres la pratiquent de manière anecdotique comparativement au temps qu'ils consacrent à leurs activités illicites (respectivement Min = 0.06 pour les vendeurs et Min = 0.05 pour les acheteurs). Les médianes démontrent qu'une majorité des carders fait du carding leur activité criminelle principale au niveau horaire (respectivement Mdn = 0.67 pour les vendeurs et Mdn = 0.69 pour les acheteurs). Des résultats très semblables émanent des analyses des distributions des indices de spécialisation en termes de revenus criminels. En effet, pour certains carders l'ensemble des revenus criminels proviennent du carding (Max = 1) alors que pour d'autres l'argent gagné grâce au carding représente une part marginale de leurs revenus criminels (respectivement Min = 0.02 pour les vendeurs et Min = 0.11 pour les acheteurs). Pour finir, comme pour la spécialisation horaire, une majorité des carders gagnent une majorité de leurs revenus criminels par le biais des activités de carding (respectivement Mdn = 0.70 pour les vendeurs et Mdn = 0.69 pour les acheteurs).

4.3. IDENTIFIER LES CARACTERISTIQUES PERSONNELLE ET SOCIALES QUI EXPLIQUENT LA REUSSITE DES CARDERS

Cette section présente les résultats des analyses bivariées effectuées. Étant donné la nature des variables dépendantes et indépendantes des corrélations ainsi que des tests de moyennes non paramétrique ont été effectués. En effet, dans les deux échantillons, aucune variable dépendante ne satisfaisait les postulats d'utilisation de ces deux tests (par exemple, le postulat de normalité des distributions). En effet, les résultats des tests de Shapiro-Wilk suggèrent de rejeter

l'hypothèse nulle qui stipule que les distributions sont normales. Ainsi, le choix a été fait de se tourner vers des tests non-paramétriques utilisant le coefficient Rhô de Spearman et le U de Mann-Whitney. Le tableau 18 présente les corrélations effectuées.

Les résultats présentés dans le tableau 18 mettent en lumière qu'une majorité des variables n'ont pas de relations significatives avec la génération de revenus ou de profits. À titre d'exemple, toutes les variables relatives à la victimisation endogène n'ont pas de lien significatif avec les revenus et les profits des acheteurs. Cependant, certaines variables ressortent comme ayant une relation statistiquement significative sur la réussite criminelle des carders. En effet, il existe un lien significatif fort entre *le nombre de produits* et la génération de revenus ou de profits (à titre d'exemple $Rh\hat{o} = 0.60$; $p < 0.01$ pour les revenus des vendeurs). Une même consistance dans les résultats est constatée pour l'association entre *le nombre de vendeurs* et les revenus et profits. Dans les deux échantillons, ces derniers entretiennent des liens proportionnellement forts et significatifs (à titre d'exemple $Rh\hat{o} = 0.50$; $p < 0.01$ pour les profits des vendeurs). Ainsi, plus *le nombre de produits* ou *les nombres de vendeurs ou d'acheteurs* auxquels le participant aura eu affaire seront élevés, plus les *revenus* et les *profits* seront importants.

Pareillement, les deux échantillons affichent des résultats semblables quant à la *mesure autoévaluée des compétences*. Dans les deux cas, le fait de se considérer comme plus compétent entraîne une augmentation des *revenus* et des *profits* (à titre d'exemple, dans le cas des vendeurs $Rh\hat{o} = 0.35$; $p < 0.05$ pour les revenus et $Rh\hat{o} = 0.38$; $p < 0.05$ pour les profits). Bien que les tailles d'effet de ces relations peuvent être considérées comme fortes dans le cas des acheteurs, elles seront qualifiées de moyennes dans le cas des vendeurs. Ainsi, plus un vendeur se considère comme compétent à mener des activités de carding, plus ses revenus et profits seront élevés.

Les *années de début des activités* des vendeurs sont négativement corrélés avec les revenus et les profits (respectivement $Rh\hat{o} = 0.35$; $p < 0.05$ pour les revenus et $Rh\hat{o} = 0.41$; $p < 0.05$ pour les profits). Cette relation peut être considérée comme moyenne. Elle signifie que plus un vendeur démarre tard son activité, moins ses revenus et profits seront élevés.

Tableau 19. Coefficient de corrélation Rhô de Spearman entre les variables indépendantes et les revenus et les profits des deux échantillons

	Vendeurs		Acheteurs	
	Revenus	Profits	Revenus	Profits
Activités marchandes				
Nombres de produits	.603**	.662**	.672**	.653**
Année de début	-.495**	-.409*	-.254	-.186
Mesure auto-évaluée	.349*	.377*	.578**	.599**
Victimisation endogène				
Générale	-	-	-.013	.003
Sites web	-	-	.177	.221
Carding shops	-	-	.006	.017
Forums	-	-	-.063	-.027
Salles de clavardage	-	-	-.110	-.065
Cryptomarchés	-	-	.011	-.043
Technologies d'anonymat				
Machine virtuelle	-.016	.032	.154	.148
Système d'explo. anony.	.315	.329	.323*	.359*
Réseaux virtuels privés	-.073	.006	.063	.106
Com. encrypté	-.214	-.105	.000	.040
Réseaux superposés	-.214	-.166	-.015	.023
Services de blanch.	.050	.119	.411**	.401**
Contacts				
Nombre vendeurs/acheteurs	.467*	.503**	.315*	.400*
Coll. inconscients	.268	.247	.263	.190
Coll. conscients	.045	.078	.255	.171
Sociodémographiques				
Âge	.266	.140	.235	.181
Niv. d'éducation	.111	-.013	.243	.254
Revenus légit.	-.176	-.163	.033	.039
Autres revenus illégit.	-.031	.007	.465**	.496**
H. par semaine (carding)	.177	.107	.324*	.292*
H. par semaine (autres)	-.151	-.175	.286*	.241
Spécialisation horaire	.318	.307	-0.113	-0.100
Spécialisation revenus	.516**	.475**	.168	.137

Note : * = p<0.05

** = p<0.01

*** = p<0.001

La fréquence d'utilisation d'un système d'exploitation garantissant l'anonymat (Système d'explo. anony.) est la seule variable parmi les technologies d'anonymat qui entretient une relation significative avec les revenus et les profits. En effet, cette variable est positivement

corrélée avec les variables dépendantes dans le cas des acheteurs (respectivement $R\hat{\theta} = 0.32$; $p < 0.05$ pour les revenus et $R\hat{\theta} = 0.36$; $p < 0.05$ pour les profits). La force de cette relation est moyenne. De ce fait, plus un acheteur utilise fréquemment ce type de technologie d'anonymat, plus ses revenus et profits seront élevés.

Une même tendance est observée pour les acheteurs s'agissant de la *fréquence d'utilisation de services de blanchiment d'argent* (Services de blanch.). Cette variable entretient aussi une relation significative avec les *revenus* et les *profits*. Cette corrélation positive a une taille d'effet moyenne (respectivement $R\hat{\theta} = 0.41$; $p < 0.01$ pour les revenus et $R\hat{\theta} = 0.40$; $p < 0.01$ pour les profits). Plus ce type de services seront utilisés fréquemment par les acheteurs, plus les revenus et les profits de ces derniers seront élevés.

Il en va de même pour les *revenus illégitimes provenant d'autres activités criminelles* (Autres revenus illégit.) dont les associations avec les revenus et les profits du carding sont statistiquement significatives. Ces relations positives peuvent être considérée comme fortes (respectivement $R\hat{\theta} = 0.47$; $p < 0.01$ pour les revenus et $R\hat{\theta} = 0.50$; $p < 0.01$ pour les profits). Ainsi, plus un acheteur générera de revenus d'autres activités criminelles, plus ses revenus et profits provenant du carding seront importants.

Les *heures par semaine passées à faire des activités d'achats de produits du carding* (H. par semaine (carding)) et les *heures par semaine passées à faire d'autres activités criminelles* (H. par semaine (autres)) entretiennent des liens significatifs avec les variables dépendantes (par exemple, pour les *heures passées à faire des achats* $R\hat{\theta} = 0.32$; $p < 0.05$ pour les revenus). Ce constat n'est d'ailleurs valable que dans le cas des *revenus* pour les *heures passées à faire d'autres activités criminelles*. Les tailles d'effet de ces relations peuvent être qualifiées de moyennes. Il est ainsi attendu qu'un acheteur passant plus de temps à faire des activités, plus ses *revenus* et ses *profits* seront élevés. Dans le cas des *heures passées à faire d'autres activités*, une même interprétation est valable mais uniquement dans le cas des revenus du carding.

Pour finir, l'indice de *spécialisation des revenus* entretient une relation statistiquement significative avec les *profits* et les *revenus* des vendeurs (respectivement $R\hat{\theta} = 0.52$; $p < 0.01$ et $R\hat{\theta} = 0.48$; $p < 0.01$). Plus les revenus criminels en général des vendeurs provient de leur activité en tant que carder, plus leurs revenus et leurs profits provenant exclusivement du

carding seront élevés. La taille d'effet de cette relation peut être considérée comme forte. Ce résultat n'est pas étonnant dans la mesure où nous avons constaté que les carders sont majoritairement spécialisés dans le carding.

Une part importante des variables sont de nature dichotomique. Pour identifier lesquelles d'entre elles expliquent les revenus des carders des analyses bivariées ont été réalisées. Étant donné le non respect des postulats d'utilisation des tests de moyennes paramétriques, des analyses faisant appel au U de Mann-Whitney ont été réalisées. Les tableaux 19 et 20 présentent les résultats des variables ayant un lien statistiquement significatif avec les variables dépendantes.

Tableau 20. Tests de U de Mann-Whitney pour les variables *Dumps*, *Forum* et *Logiciels malveillants* pour les vendeurs

Vendeurs	Medianes (rang moyen)		Z	n
	N'utilise pas	Utilise		
	Revenus			
Dumps	5,750\$ (9.28)	37,000\$ (16.45)	-2.314*	24
Forum	4,000\$ (9,05)	45,709\$ (15,42)	-2.203*	24
Logiciels mal.	4,000\$ (8.46)	37,000\$ (16.54)	-2.802**	24
	Profits			
Dumps	3,900\$ (9.75)	23,000\$ (16.35)	-2.256*	24
Forum	3,000\$ (9.00)	25,380\$ (15.46)	-2.232*	24
Logiciels mal.	3,400\$ (8.38)	25,500\$ (16.63)	-2.860**	24

Note : * = p<0.05 ** = p<0.01 *** = p<0.001

Dans l'échantillon des vendeurs, 3 variables parmi l'ensemble des variables dichotomiques ont des liens significatifs avec les revenus et les profits. Tout d'abord, il existe une différence statistiquement significative au niveau des revenus et des profits entre les vendeurs qui proposent des *Dumps* et ceux qui n'en proposent pas (respectivement $Z = -2.31$; $p < 0.05$ et $Z = -2.26$; $p < 0.05$). En effet, les vendeurs proposant des *Dumps* génèrent en médiane des revenus et des profits supérieurs à ceux qui n'en vendent pas (par exemple, $Mdn = 5,750\$$ contre $Mdn = 37,000\$$ dans le cas des revenus).

De manière semblable, l'utilisation de forums ressort comme entretenant des relations significatives avec les *revenus* et les *profits* (respectivement $Z = -2.20$; $p < 0.05$ pour les revenus et $Z = -2.23$; $p < 0.05$ pour les profits). Les vendeurs proposant leurs produits sur les forums gagnent en médiane plus que les vendeurs n'utilisant pas ce type de lieu de convergence (par exemple, Mdn = 3,000\$ contre Mdn = 25,380\$ pour les profits). Finalement, une même tendance est observable pour les vendeurs qui ont utilisé des logiciels malveillants pour dérober des données financières. L'utilisation de logiciels malveillants entretient une relation statistiquement significative avec les revenus et les profits (respectivement $Z = -2.01$; $p < 0.01$ et $Z = -2.86$; $p < 0.01$). Les vendeurs qui ont fait appel à ce procédé ont en médiane des revenus et des profits supérieurs à ceux n'ayant pas fait appel à des logiciels malveillants (par exemple, Mdn = 4,000\$ contre Mdn = 37,000\$ dans le cas des revenus).

Tableau 21. Tests de U de Mann-Whitney pour les variables *Courtier financier* et *Aucun rôle* pour les acheteurs

Acheteurs	Medianes (rang moyen)		Z	n
	N'occupe pas le rôle	Occupe le rôle		
Revenus				
Courtier financier	12,500\$ (17.11)	91,000\$ (29.63)	-2.241*	36
Aucun rôle	82,000\$ (27.77)	10,000\$ (14.42)	-3.504***	36
Profits				
Courtier financier	11,000\$ (16.88)	80,500\$ (31.50)	-2.618**	36
Aucun rôle	51,683\$ (26.95)	8,000\$ (14.78)	-3.195**	36

Note : * = $p < 0.05$ ** = $p < 0.01$ *** = $p < 0.001$

De même que dans l'échantillon des vendeurs, uniquement des variables relatives aux rôles des participants entretiennent des relations statistiquement significatives avec les variables dépendantes. En effet, les revenus et des profits sont reliés statistiquement avec le fait d'être ou non courtier sur les lieux de convergence (respectivement $Z = -2.24$; $p < 0.05$ et $Z = -2.62$; $p < 0.01$). Les acheteurs agissant aussi comme courtier financier gagnent en médiane plus de revenus et de profits que ceux qui n'ont pas ce rôle (par exemple, Mdn = 12,500\$ contre Mdn = 91,000\$ pour les revenus). Ce résultat est d'ailleurs consistant avec le suivant qui met en avant une différence statistiquement significative pour les revenus et les profits entre les acheteurs

n'ayant pas de rôle sur les lieux de convergence et ceux ayant précisé en avoir un (respectivement $Z = -3.50$; $p < 0.001$ et $Z = -3.20$; $p < 0.01$). Les acheteurs ayant mentionné ne pas occuper de rôle gagnent en médiane moins de revenus et de profits que ceux occupant au moins un des rôles proposés (par exemple, $Mdn = 82,000\$$ contre $Mdn = 10,000\$$ dans le cas des revenus).

CHAPITRE 5 - DISCUSSION

Dans le cadre de l'étude du carding, peu de recherches se sont intéressés à la réussite criminelle des cyberdélinquants qui y participaient. Bien que certains se soient penchés sur l'accès aux opportunités criminelles au travers de l'étude des réseaux criminels (Décary-Hétu & Leppänen, 2013), l'unique étude ayant fourni une évaluation des revenus de ces délinquants revêtait certaines limites méthodologiques, en particulier au niveau des types de lieux de convergence d'où provenaient les échantillons (Holt, Smirnova & Chua, 2016). Ainsi, ce mémoire avait pour objectif général de comprendre la réussite criminelle différentielle des carders évoluant sur le darknet. Pour y répondre, ce projet a utilisé un sondage en ligne pour questionner directement les carders dans leur environnement virtuel. Cette démarche s'appuyait sur les méthodes utilisées par les recherches sur la réussite criminelle (Tremblay & Morselli, 2000; Morselli & Tremblay, 2004a; Morselli & Tremblay, 2004b; Thompson & Uggen, 2012; Ouellet, 2018; Rowan, McGoin & Nguyen, 2018).

Dans le cas plus particulier du carding, les travaux ayant présenté des évaluations des revenus criminels montraient que ces derniers peuvent espérer des revenus élevés mais qu'il existe d'importantes différences en termes de gains (Holt, Smirnova & Chua, 2016). Nos résultats font ressortir une réalité en accord avec cette idée et montrent que les carders sont une majorité à ne pas gagner des revenus conséquents mais qu'un petit contingent a une réussite criminelle élevée. Notre démarche d'utiliser deux échantillons, pour s'intéresser à la fois aux vendeurs et aux acheteurs, nous permet de souligner que les acheteurs gagnent plus que les vendeurs. Cette différence s'inscrit dans l'idée que les vendeurs sont peu enclins à utiliser les produits eux-mêmes (Dupont, 2012). En effet, la monétisation des données, même lorsqu'il y a une faible probabilité d'avoir un produit fonctionnel, permet aux acheteurs de générer plus d'argent que les vendeurs qui offrent leurs produits en deçà de leurs valeurs réelles (Herley & Florêncio, 2010; Holt, Smirnova & Chua, 2016).

5.1. L'EXPERIENCE

L'expérience peut s'exprimer au travers de divers concepts. Alors que certaines études ont utilisé des mesures démographiques comme l'âge ou le nombre de condamnations passées, d'autres se sont penchées sur l'établissement de tactiques, la spécialisation ou les compétences et habiletés particulières (Tremblay & Morselli, 2000; McCarthy et Hagan 2001; Morselli et Tremblay 2004; Robitaille, 2004; Morselli, Tremblay et McCarthy 2006; Ouellet & Tremblay, 2014;

Ouellet, 2018). Ces caractéristiques sont positivement corrélées avec la génération de revenus illégitimes et témoignent de l'importance que revêt l'expérience du délinquant pour sa réussite criminelle. Notre étude montre que ce dernier constat est aussi valable dans le cadre du carding. En effet, les carders interrogés ressortent comme étant expérimentés. Ceci est d'ailleurs plus particulièrement le cas pour les acheteurs qui affichent plus d'années d'activités.

Ce résultat s'explique par le fait que la monétisation des données soit l'étape la plus flexible et complexe du script criminel du carding. Elle peut ainsi être conduite en ligne ou en magasin selon le produit acheté (Sullivan, 2010; DeFilippi & Michael, 2016). Aussi, l'abondance de tutoriaux disponibles reflète qu'il existe une multitude de manières de conduire cette étape (Hardeveld, O'Hara & Webber, 2016). Ainsi, les acheteurs doivent bénéficier de plus de pratique pour mener à bien l'étape de monétisation. Dans le cas des vendeurs, les résultats ont montré que plus un vendeur commence tard ses activités, moins ses revenus seront élevés. Ce résultat soulève l'importance de l'expérience dans la réussite criminelle des carders. En effet, comme soulevé dans d'autres études, les vendeurs doivent prendre le temps de se construire une réputation qui assurera la pérennité de leurs activités (Holt, 2013a; Hutchings & Holt, 2015; Cherqi et al., 2018).

Cette réputation est d'ailleurs soutenue par des mécanismes de confiance comme le parrainage qui permet de contrôler la qualité des participants sur les lieux de convergence et permet l'accès à des sections réservées (Holt, 2007; Markham, 2011; Holt & Dupont, 2018; Lusthaus, 2018b). En questionnant le parrainage et le recrutement comme mesure des compétences et habiletés particulière, les résultats de notre étude ne nous permettent pas de considérer ces variables de prédicteurs de la réussite des carders. Malgré cela, il ressort que ces caractéristiques demeurent importantes au sein des activités des carders. En effet, il a été vu qu'une majorité des carders ont déclaré avoir déjà été recrutées pour leurs compétences. Étant donné que le carding repose sur la collaboration entre divers acteurs, il n'est pas étonnant de constater qu'une majorité d'entre eux présente cette caractéristique (Leukfeldt, 2014; Caines et al., 2018). De plus, s'agissant du parrainage, cette observation devient plus probante dans le cas des vendeurs qui ont, pour plus de 95% déclaré avoir déjà été parrainé. Cette observation peut faire écho au rationnel suivant : les vendeurs interviennent plus tôt au cours du script criminel du carding. En accord avec la littérature, nos résultats montrent qu'il est important pour eux de capitaliser sur les mécanismes de confiance comme le parrainage pour bénéficier d'une bonne réputation afin de pérenniser

leurs activités (Holt, 2013a; Hutchings & Holt, 2015; Cherqi et al., 2018). Ainsi, le parrainage et le recrutement ressortent comme des phénomènes inhérents aux activités des carders de manière générale. Leurs fortes fréquences montrent qu'une grande majorité des carders, qu'ils affichent ou non une réussite criminelle, ont déjà utilisé ces mécanismes dans le cadre de leurs activités.

Cependant, le parrainage et le recrutement ne sont pas les seules manières d'opérationnaliser les concepts de compétences et d'habiletés particulières. Il a été vu que sur les communautés en ligne, la démonstration de compétences techniques offre des avantages certains au sein des communautés (Lusthaus, 2012) et qu'il est nécessaire d'avoir certaines compétences pour participer aux activités marchandes (Décary-Héту, Mousseau & Vidal, 2018). Nos résultats permettent de soutenir que l'utilisation de logiciels malveillants comme mesure de la démonstration technique ainsi que le fait de se considérer soi-même comme compétent sont des prédicteurs de la réussite criminelle des carders. Ainsi, ces résultats sont consistants avec la littérature (McCarthy et Hagan 2001; Morselli et Tremblay 2004; Morselli, Tremblay et McCarthy 2006; Ouellet & Tremblay, 2014; Ouellet, 2018)

S'agissant de la mise en place de tactiques, la littérature soutenait que les délinquants qui mettaient en place des tactiques a priori de la commission du crime affichaient une meilleure réussite criminelle (Robitaille, 2004). En transposant ce concept aux activités des carders, notre étude a été en mesure de fournir des mesures de ce concept au travers de la fréquence d'utilisation de technologies d'anonymat. En effet, il a été vu que les carders sont une majorité à utiliser des technologies d'anonymat dans le cadre de leurs activités. Plus particulièrement, il a été souligné la popularité des réseaux virtuels privés qui, semble-t-il, occupent une place privilégiée parmi les technologies utilisées. Ces résultats sont concordants avec le fait que les proxies ressortent comme étant l'un des outils les plus plébiscités (Hardeveld, Webber & O'Hara, 2017). En second lieu, nous avons vu que les réseaux superposés étaient aussi relativement utilisés par les carders. Ceci peut s'expliquer par le fait que certains lieux de convergence sont hébergés sur l'internet traditionnel. Bien que les réseaux superposés intègrent directement des mécanismes d'anonymisation (Christin, 2013; van Buskirk et al., 2016), la forte prévalence de l'utilisation de réseaux virtuels privés suggère que les carders sont déjà anonymes même lorsqu'ils naviguent sur l'internet traditionnel, ne faisant pas de l'utilisation des réseaux superposés une nécessité. Nos analyses ont montré que le fait qu'utiliser plus fréquemment des

systèmes d'exploitation garantissant l'anonymat et des services de blanchiment d'argent sont corrélés avec des revenus et des profits plus importants, même s'ils ne sont pas très populaires. Ainsi, le fait de mettre en place des tactiques est aussi un prédicteur de la réussite criminelle dans le cas des carders.

Malgré cette relation, deux interprétations peuvent ressortir du fait que les systèmes d'exploitation garantissant l'anonymat soient la technologie d'anonymat la moins fréquemment utilisée. Premièrement, l'utilisation d'un système d'exploitation garantissant l'anonymat plutôt que ceux utilisés communément peut être contraignante pour ces utilisateurs car il ne permet vraisemblablement pas de soutenir toutes les applications. Deuxièmement, au vu des précédents résultats présentés, la popularité des autres types de technologie d'anonymat peut venir faire de l'ombre à ce type-ci. En mobilisant d'autres technologies, les carders peuvent déjà s'assurer un anonymat effectif sans avoir la nécessité d'utiliser un système d'exploitation.

Les réseaux virtuels privés demeurent très largement utilisés. Il s'agit vraisemblablement de la technologie agissant comme la clef de voûte de l'anonymat dans la mesure où elle permet de couvrir l'information la plus sensible lors de l'identification de comportements illégaux en ligne, à savoir l'adresse IP (Décary-Héту & Leppänen, 2013; Hardeveld, Webber & O'Hara, 2017). Il est aussi intéressant de noter qu'une part non négligeable des répondants ont déclaré ne jamais utiliser de services de blanchiment d'argent. Ce résultat laisse en suspens plusieurs questions : quelles alternatives peuvent être utilisées ? Au vu de la popularité des cryptomonnaies, est-ce que ces répondants ne prêtent pas grande attention à l'anonymat de leurs transactions en conservant leurs richesses sur les réseaux des cryptomonnaies ?

Finalement, la littérature sur la réussite criminelle nous a appris que le fait qu'être spécialisé dans un type de criminalité garantit une meilleure réussite criminelle (Tremblay & Morselli, 2000). Notre étude abordait ce concept sous l'angle de deux mesures : la spécialisation horaire et la spécialisation en termes de revenus. Nos résultats ont fait ressortir qu'ils existent différents degrés de spécialisation et qu'une majorité des carders sont spécialisés dans le carding au niveau horaire et au niveau de leurs revenus illégitimes. Dans le particulier des vendeurs, l'indice de spécialisation des revenus s'est avéré être positivement corrélé à la génération de revenus et de profits.

5.2. ACTIVITES CRIMINELLES

Dans le cadre de ce projet de recherche, la dimension des activités criminelles des carders était testée par cinq prédicteurs. Une majorité d'entre eux provenait d'une transposition au carding des caractéristiques identifiées lors de la revue de la littérature portant sur la réussite criminelle conventionnelle.

Une fréquence élevée des activités criminelles est souvent associée à une meilleure réussite criminelle (Tremblay & Morselli, 2000; Robitaille, 2004). Étant donné que le script criminel a mis en avant le fait que le carding nécessite des apprentissages, il est envisageable que cette nécessité puisse engager le carder à passer beaucoup de temps à apprendre des connaissances pour mener à bien son activité criminelle (Yip, Webber & Shadbolt, 2013; Hardeveld, Webber & O'Hara, 2016; Hardeveld, Webber & O'Hara, 2017). Nos résultats ont tout d'abord souligné que les carders passent une part importante de leurs temps à s'adonner à des activités de ventes ou d'achats. Par la suite, nous avons vu que le fait de participer plus de temps par semaine à des activités de carding garantissait aux acheteurs une meilleure réussite criminelle. Ceci entre en concordance avec les précédents travaux qui ont porté sur la réussite criminelle (Tremblay & Morselli, 2000; Robitaille, 2004).

Cette section des activités criminelles se penchait aussi sur les types de produits utilisés par les carders. Nos résultats ont fait ressortir que les *Fullz* constituaient le type de produits le plus populaire. Cette prévalence s'explique par le fait que les *Fullz* contiennent le plus d'informations sur les victimes et qu'ils sont utilisés pour faire du carding en ligne qui revêt une plus grande facilité de monétisation (Peretti, 2009; Holt & Lampke, 2010). Bien que moins populaires que les *Fullz*, les CVV et les comptes en ligne, apparaissaient relativement peu utilisés par les carders des échantillons. Un même rationnel que celui fait pour les *Fullz* peut s'appliquer dans la mesure où ils permettent de monétiser l'information via des techniques en ligne mais contiennent moins d'informations personnelles (Clarke & Newman, 2003; Peretti, 2009; Hutchings & Holt, 2014). Pour finir, les *Dumps* sont apparus comme le type de produit le moins populaire. Ce constat reflète le fait que ce type de produit nécessite de posséder le matériel nécessaire pour parachever la contrefaçon de cartes (Mativat & Tremblay, 1997; Bulakh & Gupta, 2015). De plus, la monétisation se fait dans les magasins et présente plus de risques qu'une activité en ligne. Il n'est donc pas étonnant d'observer que ce type de produits soit

largement moins prévalent pour les acheteurs. Ces résultats s'opposent à ceux émis par les précédentes recherches qui mentionnaient que les *Dumps* étaient les produits les plus populaires sur les marchés (Thomas & Martin, 2006; Franklin et al., 2007; Du et al., 2018). Cependant, les résultats des analyses bivariées ont montré que les vendeurs proposant des *Dumps* gagnaient plus que les vendeurs n'en proposant pas. Ceci suggère que, bien que cela comporte plus de risques, faire du carding en magasin est une voie de monétisation garantissant de meilleurs revenus et profits et donc une meilleure réussite criminelle.

Les activités marchandes des carders reposent sur divers types de lieux de convergence (Leukfeldt, 2014; Caines et al., 2018). Nos résultats ont montré que les lieux de convergence les plus populaires parmi les vendeurs de produits du carding sont les salles de clavardages. Ces dernières sont plus utilisées que les forums et les cryptomarchés. Ceci témoigne du fait que les salles de clavardage constituent le type de lieux de convergence où il est le plus facile de promouvoir ses offres. Leurs organisations s'articulent principalement autour de grands groupes de discussions, réunissant des dizaines voir des centaines de personnes, dans lesquels n'importe quel vendeur peut proposer ses produits et peut ainsi atteindre des clients potentiels (Franklin et al., 2007; Décary-Héту & Dupont, 2012; Bernard et al., 2018). En effet, les mécanismes de confiance présents sur ces derniers nécessitent plus d'implications pour bâtir une réputation et assurer des ventes. Dans le cadre des forums, l'asynchronicité des discussions fait en sorte que les offres des vendeurs, une fois postées, peuvent être consultées et vérifiées par l'équipe administratrice du lieu de convergence (Holt & Lampke, 2010; Décary- Héту & Leppänen, 2013; Yip, Webber & Shadbolt, 2013; Holt et al., 2015). Pour le cas des cryptomarchés et des sites web, les systèmes de notation et d'évaluations peuvent aussi constituer un frein dans l'utilisation de ce type de lieux de convergence dans la mesure où il est important pour les vendeurs d'avoir d'effectuer a priori un certain nombre de ventes ayant satisfait leurs clients pour bénéficier d'une crédibilité leur permettant d'attirer de nouveaux acheteurs (Christin, 2013). A contrario, les autoshops sont apparus comme étant les moins populaires au sein de l'échantillon des vendeurs. Ce résultat est consistant avec la littérature qui soutient que la tenue d'un carding shop n'est pas chose aisée dans la mesure où le vendeur doit programmer l'automatisation des transactions et bénéficier d'une bonne réputation pour attirer les clients (Europol, 2017).

Cependant, lorsqu'il s'agit de constater l'impact de l'utilisation de tel ou tel types de lieux de convergence sur la réussite criminelle, seul le fait d'utiliser des forums de discussions est ressorti comme entretenant une relation statistiquement significative avec la génération de revenus et de profits. En effet, les vendeurs qui utilisent les forums pour proposer leurs produits gagnent en médiane plus que ceux qui n'utilisent pas ce type de lieux de convergence. Ce constat peut retranscrire le fait que les forums est l'un de premiers types de lieux de convergence à avoir vu le jour et qu'il demeure empreint de mécanismes de confiance qui garantissent sa pérennité en tant que lieu de marchandage (Yip, Shadbolt et Webber, 2010; Décary-Héту & Leppänen, 2013; Yip et al., 2013; Décary-Héту & Eudes, 2015; Lusthaus, 2018).

Pour les acheteurs, ce sont les cryptomarchés qui ressortent comme étant les plus utilisés au sein de leur échantillon. Cette observation retranscrit le fait que les cryptomarchés constituent le type de lieu de convergence le plus convivial à utiliser et que les systèmes mis en place pour soutenir la confiance entre vendeurs et acheteurs ainsi que l'anonymat fourni permettent d'assurer un niveau de service sophistiqué comparativement aux autres types (Custer, Pool & Cornelisse, 2018; Décary-Héту, Mousseau & Vidal, 2018). Ce résultat est d'ailleurs suppléé par le fait que les carding shops occupent la seconde position. Bien que ces derniers n'offrent pas l'ensemble des mesures sécuritaires soutenues par les cryptomarchés, il demeure qu'un carding shop bénéficiant d'une bonne réputation et fournissant des produits de bonne qualité peut attirer et fidéliser beaucoup de clients. Il est à noter qu'un des types de lieux de convergence questionnés, les *sites web* peuvent souffrir d'un mauvais design dans la mesure où l'ensemble des autres types de lieux de convergence proposés sont aussi des sites web en tant que tels. Ainsi, les réponses ayant fait état de ce choix demeurent difficilement interprétables.

Mikhaylov et Frank (2016) ont stipulés que les cryptomonnaies n'étaient pas très populaires parmi les carders. Nos résultats relatifs aux moyens de paiement ont montré que les cryptomonnaies sont très plébiscitées par les carders. Ce résultat souligne que, de par leur facilité d'utilisation, leurs vertus sécuritaires et leurs popularités dans les écosystèmes de cybercriminels, les cryptomonnaies pseudonymes largement préférées par les répondants. Il s'oppose ainsi à ceux Mikhaylov et Frank (2016) et se positionne sur un manque de consensus à ce sujet (Portnoff et al., 2017).

Enfin, une section entière du sondage était consacrée à interroger les acheteurs sur la fréquence des expériences de victimisation endogène qu'ils ont vécues. Pour rappel, ces fréquences étaient demandées sur les différents types de lieux de convergence fréquentés par les carders. Aucune relation statistiquement significative n'a été constatée entre le fait d'avoir une fréquence de victimisation plus élevée et la génération de revenus ou de profits. Néanmoins, nos résultats permettent de souligner certains points intéressants à ce sujet. Tout d'abord, de manière générale, la victimisation endogène semble être relativement courante au sein des communautés de carding. En effet, une petite proportion des répondants ont déclaré ne jamais s'être fait arnaquer. Bien que les résultats soutiennent l'existence de *rippers* (Motoyama et al., 2010), les résultats vont à l'encontre de l'idée que les marchés de carding seraient des marchés pour tacos (Herley & Florêncio, 2010).

En s'intéressant plus spécifiquement à la fréquence de victimisation dépendamment du type de lieux de convergence, nos résultats ont montré que les cryptomarchés sont là où les acheteurs ont déclaré s'être fait le moins arnaquer. En se fiant à la littérature, l'interprétation de ce résultat repose sur le fait que les cryptomarchés utilisent des mécanismes qui offrent des garanties quant au niveau de service (Christin, 2013; Custer, Pool & Cornelisse, 2018; Décary-Héту, Mousseau & Vidal, 2018). Un constat relativement similaire a été fait dans le cadre des forums de discussions. Ceci peut aussi être expliqué par la foule de mécanismes permettant de soutenir la confiance qui prennent place sur les forums (Thomas & Martin, 2006; Franklin et al., 2007; Herley & Florêncio, 2010; Holt, 2013a; Aldridge & Décary-Héту, 2014; Holt et al., 2015; Hutchings & Holt, 2015; Cherqi et al., 2018).

À l'inverse, les *carding shops* constituent le type de lieux de convergence où les acheteurs ont déclaré avoir été le plus fréquemment arnaqués. Les *carding shops* dépendent exclusivement d'un vendeur et ne sont pas soumis au contrôle d'une communauté ou d'une équipe administratrice comme pour les forums ou les cryptomarchés. Ainsi, il est plus probable d'y trouver des individus opportunistes qui vont profiter de cette main mise sur la plateforme de vente pour arnaquer des acheteurs.

Une limite au niveau du design des questions est à mentionner dans le cadre de la victimisation endogène. Les interprétations demeurent relativement limitées dans la mesure où le fait qu'un répondant ait déclaré ne jamais avoir été arnaqué sur tel type de lieux de convergence peut tout

simplement retranscrire le fait qu'il n'utilisait pas ce type-ci. Il aurait été préférable, lors du design du sondage de conditionner l'accès aux questions de cette section en fonction des réponses données lorsque les acheteurs étaient questionnés sur les types de lieux de convergence sur lesquels ils faisaient leurs activités.

5.3. SOCIABILITE

La propension à collaborer permet aux délinquants de bénéficier d'une meilleure réussite criminelle (Tremblay & Morselli, 2000; Descormiers, Bouchard & Corrado, 2011). La littérature sur le carding a montré que cette caractéristique est associée à un plus grand nombre de transactions qui peut vraisemblablement assurer plus de gains illégitimes (Motoyama et al., 2011). Cependant, nos résultats ne peuvent soutenir ce point étant donné que la variable mesurant ce concept n'est pas ressortie comme étant significatif. Il a tout de même été souligné qu'au niveau échantillonnal, une majorité des carders présente cette caractéristique. Il ressort donc que les carders ont une relative propension à collaborer.

Néanmoins, cette dimension de sociabilité était aussi examinée au travers du fait d'occuper une place de leader. Cette position, dans une organisation criminelle, permet d'avoir une meilleure réussite criminelle (Levitt & Venkatesh, 2000). Dans le cadre du carding, le fait d'occuper une place de leader est très nettement observable au travers des rôles occupés sur les lieux de convergence qui permettent de soutenir la confiance et la réputation des participants (Franklin et al., 2007; Yip, Shadbolt et Webber, 2010; Holt, 2013; Holt et al., 2015; Dupont et al. 2016). Nos résultats ont montré que les acheteurs sont une majorité à ne pas avoir déclaré de rôle comparativement aux vendeurs. Les vendeurs apparaissent plus tôt que les acheteurs dans le script criminel du carding et doivent s'appuyer sur les mécanismes de confiance pour se construire réputation qui assurera la pérennité de leurs activités (Holt, 2013a; Hutchings & Holt, 2015; Cherqi et al., 2018). En ayant bâti une réputation autour de leurs activités marchandes, il est fort probable que cette dernière puisse se déverser sur l'occupation de rôles à responsabilités sur les lieux de convergence.

Cette interprétation est soutenue par les résultats des analyses bivariées effectuées sur l'échantillon des acheteurs. En effet, s'agissant du rôle de *courtier financier*, les acheteurs qui occupent ce rôle gagnent en médiane plus que ceux qui ne l'occupent pas. À l'inverse, une

relation statistiquement significative a été constatée entre le fait de *ne pas avoir de rôle* et la génération de revenus et de profits. Les acheteurs qui déclarent n'occuper aucun rôle gagnent moins en médiane que ceux qui déclarent au moins un rôle sur les lieux de convergence. Ces résultats concordent directement avec le fait qu'occuper une place de leader qui, dans le cas du carding, peut se transposer à l'occupation d'un rôle sur les lieux de convergence, garantit une meilleure réussite criminelle aux délinquants (Levitt et Venkatesh; 2000). Plus particulièrement, le fait qu'être courtier financier offrent une meilleure réussite retranscrit bien que ce type d'acteur peut aussi se voir octroyer des commissions importantes en assurant l'intermédiaire entre deux parties lors d'une transaction (Thomas & Martin, 2006).

5.4. SOCIODEMOGRAPHIQUES

Quatre prédicteurs de nature sociodémographiques étaient questionnés au cours de cette recherche. Le fait d'occuper une *activité légitime* a été vu comme un frein à la réussite criminelle (Robitaille, 2004). Les résultats des analyses bivariées réalisées n'ont pas pu confirmer ou infirmer cette relation dans la mesure où aucun des tests ne s'est avéré significatif. Les résultats des statistiques descriptives ont montré qu'une large majorité des répondants occupaient une activité légitime et ce, qu'ils soient vendeurs ou acheteurs. L'analyse des activités conventionnelles des répondants était appuyée par l'analyse des *revenus illégitimes* gagnés par les carders au cours des 12 derniers mois. Bien qu'ici aussi, aucune relation statistiquement significative n'est ressortie entre cette variable et les variables dépendantes, les statistiques descriptives permettent de constater une forte dispersion et les grandes étendues des deux échantillons. Ce constat suggère que l'ensemble des répondants proviennent de statuts socio-économiques différents et en en couvrant un spectre relativement large au niveau salarial.

Les statistiques descriptives effectuées au niveau des âges des répondants ont montré une consistance entre les deux échantillons. En effet, les carders ayant participé à ce projet sont relativement jeunes avec une moyenne et une médiane autour de 24 ans. De plus, l'analyse du genre des répondants montre que ces derniers sont pour une majorité composée d'hommes. Bien que cela soit légèrement plus prononcé dans l'échantillon des vendeurs, ces résultats restent dans l'ensemble consistants avec ce qui avait été précédemment observé (Kshetri, 2006; Hutchings, 2014).

Néanmoins, une limite doit être mentionnée lorsque l'âge des répondants est analysé. Il s'agit du fait que, compte tenu des considérations éthiques, le sondage se soit adressé uniquement à des carders ayant plus de 18 ans. Il est fort possible que ces derniers soient encore plus jeunes. En effet, les discussions informelles entretenues lors de la promotion du sondage ainsi que les historiques des réponses sur le serveur hébergeant le sondage ont permis de constater que certains des carders qui ont été contacté étaient âgés de moins de 18 ans.

À propos du niveau d'éducation, les résultats des analyses univariées ont montré que les carders ayant répondu au sondage sont relativement éduqués. Ces résultats corroborent ceux évoqués dans la littérature. En effet, les cyberdélinquants sont en majorité jeunes et relativement éduqués (Kshetri, 2006; Hutchings, 2014). De plus, il est important de prendre en compte le fait que la médiane de l'âge des répondants (respectivement Mdn = 23.50 pour les vendeurs et Mdn = 24.00 pour les acheteurs) qui suggère qu'une majorité des individus sont peut-être trop jeunes pour avoir complété leurs cursus.

5.5. LIMITES

De par sa méthodologie, de nombreuses limites découlent de ce projet de recherche et doivent être mentionnées pour apprécier la juste portée de ces résultats. Plusieurs sous-limites sont reliées à la nature même des échantillons utilisés. Dans un premier temps, le fait de disposer de deux échantillons relativement petits a contraint les analyses, d'une part, à utiliser des tests bivariés non paramétriques. Une plus grande prudence est donc requise lors de la prise en compte des résultats émanant de ces analyses. De plus, ce même problème échantillonnal n'a pas permis d'entreprendre des analyses multivariées afin de comparer l'impact différentiel de chaque covariée par rapport aux autres. Ainsi, la portée générale des résultats présentés dans ce mémoire reste relativement modeste et ces derniers doivent être pris avec parcimonie.

Ces limites découlent principalement du terrain auquel ce projet de recherche s'est intéressé. Interroger des délinquants demeure vraisemblablement un défi difficile mais nécessaire pour nourrir les études empiriques. Nombreuses sont les études à avoir sondé les délinquants présents dans les institutions pénitentiaires, particulièrement dans le cadre de la réussite criminelle (Wilson & Abrahamse, 1992; Tremblay & Morselli, 2000; Morselli & Tremblay, 2004b; Morselli, Tremblay & McCarthy, 2006; Charest & Tremblay, 2009; Bouchard & Ouellet, 2011;

Ouellet & Tremblay, 2014; Ouellet, 2018). Bien qu'il puisse être envisager que cette démarche entraîne des élans de vantardise de la part des répondants (Wilson & Abrahamse, 1992), il a été montré que les mesures autorapportées des revenus des délinquants étaient consistants avec la réalité (Nguyen & Loughran, 2017). Néanmoins, la proximité physique dont peut bénéficier le chercheur lors de cette démarche ne peut s'appliquer en ligne auprès de cyberdélinquants.

L'identification des réponses aberrantes effectuée lors du chapitre 2 montre que certains des répondants ont tout bonnement boycotté le sondage en y inscrivant des réponses n'ayant aucune cohérence ou aucun sens. Quand bien même l'identification de ce genre de réponse est facilitée par le manque de consistance des réponses, il peut être envisagé que d'autres aient pris plus de soin à entrer des réponses plus cohérentes mais tout aussi fausses. Malheureusement, au vu du manque de connaissances sur le sujet d'intérêt de ce projet de recherche, il n'était pas possible d'identifier ce type de réponses pour les exclure des échantillons. Cette hypothèse soutenant la présence de réponses fausses mais cohérentes met encore en perspective la portée des résultats présentés précédemment.

Une dernière limite se réfère à la manière dont le sondage a été conçu. Bien que certaines questions auraient pu être déplacées dans des sections plus cohérentes ressort comme un problème marginal lorsqu'est remise en doute la pertinence de certaines d'entre elles. Premièrement, l'articulation plus attentionnée de certaines questions aurait pu permettre une meilleure précision des réponses reçues. Ceci est particulièrement le cas pour les mesures des fréquences de victimisation endogène. La section du sondage qui abritait ces questions était située a posteriori des questions portant sur les lieux de convergence. Comme les questions sur la victimisation interrogeaient les participants sur tous les types de lieux de convergence, il aurait été opportun de réduire seulement les possibilités de réponses aux lieux de convergence mentionnés précédemment. Cela aurait permis d'éviter les doutes quant à l'interprétation des carders ayant précisé ne jamais s'être fait arnaquer sur tel ou tel type de lieux de convergence. S'agissait-il réellement du fait de ne jamais avoir été victimisé ou le participant n'avait-il tout simplement jamais utilisé ce type de lieux de convergence ?

Deuxièmement, les formulations d'autres questions auraient pu être affinées. Ceci est particulièrement le cas pour la mention de sites web parmi les lieux de convergence. Dans la mesure où tous les types de lieux de convergence sont des sites web, il apparaît peu pertinent

d'offrir ce choix de réponse aux répondants. De plus, les questions de la section portant sur les *Contacts* des participants questionnaient les participants sur le nombre de collaborateurs conscients ou non conscients de participer à des activités de carding. Cette mesure souffre d'un manque d'empreinte théorique dans la mesure où aucun écrit provenant de la littérature sur la réussite criminelle ou le carding ne mentionne l'importance de distinguer le fait qu'un collaborateur soit conscient ou non de participer à une activité illégitime. Il aurait été intéressant de reformuler ces questions ou de préciser à l'aide d'une illustration pour leur offrir une place pertinente dans le sondage.

Finalement, le sondage est passé à côté de certains prédicteurs utilisés dans la littérature sur la réussite criminelle qui auraient pu être mesurées. À titre d'exemple, il a été vu que le fait d'avoir un mentor, la fréquence de consommation de drogue, d'alcool, la stabilité affective ou les périodes d'inactivité criminelle ont un impact sur la réussite criminelle (Robitaille, 2004; Morselli, Tremblay & McCarthy, 2006; Thompson & Uggen, 2012; Ouellet & Tremblay, 2014; Rowan, McGloin & Nguyen, 2018). Cependant, ces différents prédicteurs n'ont pas été mesuré dans le cadre du sondage et n'ont donc pas pu être testés dans le cadre des activités des carders.

CONCLUSION

La présente étude peut se targuer d'avoir fourni un regard inédit sur les activités des carders ainsi que sur les caractéristiques inhérentes à leurs activités criminelles qui sont importantes pour comprendre la réussite criminelle de ces cyberdélinquants. La littérature confrontant le cadre théorique de la réussite criminelle et ce phénomène cybercriminel récent étant très limitée, ce travail avait pour objectif d'améliorer les connaissances sur ce sujet en proposant de comprendre la réussite criminelle des carders actifs sur le darknet.

Pour ce faire, un sondage a été conçu et mis en ligne sur Tor afin de questionner directement les carders sur leurs caractéristiques et les caractéristiques de leurs activités criminelles. Cette approche inédite se reposait sur les méthodes de collecte de données utilisées par les travaux ayant porté sur la réussite criminelle des formes de délinquances, disons, plus traditionnelles. Elle s'est étalonnée sur une période de 4 mois et a permis de collecter 56 sondages complets. Au vu de la sensibilité des questions posées et du caractère de la population visée, des stratégies ont été opérationnalisées pour composer avec les réponses aberrantes et les réponses manquantes que comptaient les échantillons. Cette démarche permettait d'assurer à nos analyses de ne pas être pollué par de fausses observations et d'assurer la pérennité de nos résultats. Pour répondre à notre premier objectif spécifique des mesures des revenus et des profits, faisant état de la réussite criminelle des carders, ont été présentées. Le second objectif spécifique chercher quant à lui à décrire les caractéristiques personnelles et sociales des carders. Pour cela, les dimensions et concepts précédemment testés par la littérature sur la réussite criminelle ont été transposées au phénomène de carding. Il a ainsi été possible de répondre à notre troisième objectif spécifique qui visait à identifier lesquelles de ces caractéristiques expliquaient la réussite criminelle des carders.

Les deux premiers objectifs ont été menés au travers des résultats des analyses descriptives qui ont permis de dresser un portrait des activités des carders. Il a été vu qu'il existait d'importantes différences en termes de réussite criminelle au sein des carders et que les acheteurs réussissaient en moyenne mieux que les vendeurs. En effet, alors que certains ont rapporté ne gagner qu'une centaine de dollars au cours des 12 derniers mois, d'autres ont mentionné que leurs revenus et leurs profits pouvaient s'élever à plusieurs centaines de milliers. Ainsi, la réussite criminelle des carders ne se distribue pas équitablement et nos résultats confirment ceux précédemment évoqués par Holt, Smirnova et Chua (2016) qui soutenaient que l'étendue des revenus espérés par les carders peut aller de petits montants à de très forts gains.

L'examen des résultats des analyses univariées a aussi permis de confronter, d'affirmer ou d'apporter de nouveaux éléments aux connaissances générales déjà présentes sur le carding. En effet, notre étude a permis de mettre en lumière le fait que le carding nécessite une certaine expérience pour être mené à bien. Dans la mesure où cette expérience vient vraisemblablement soutenir la confiance que s'accorde les cybercriminels, nos résultats confortent le fait que la confiance est une pierre angulaire des activités des cybercriminels (Holt & Lampke, 2010; Holt, 2013a; Décary-Héту & Laferrière, 2015; Holt et al., 2015; Holt, Smirnova & Hutchings, 2016). Le phénomène de victimisation endogène mis en avant par Herley et Florêncio (2010) est d'ailleurs un bon exemple d'un manque de confiance entre les participants. Bien que ces auteurs aient spécifié que les marchés soient des marchés de tacos nos résultats ont apportés plusieurs éléments de précision. Tout d'abord, nous avons constaté que, de manière générale, ce phénomène de victimisation endogène est modérément fréquent au sein des communautés de carders. Ceci s'explique par le fait que certains lieux de convergence sont plus sécuritaires pour les acheteurs alors que d'autres semblent abriter plus de participants opportunistes désireux d'arnaquer les autres. Ce clivage est particulièrement ressorti entre les cryptomarchés qui constituent le type de lieu de convergence sur lequel la victimisation endogène est la moins présente et les carding shops qui sont le type où les acheteurs se font le plus arnaquer.

Dans un second temps, l'application du modèle empirique conçu à partir de la transposition des concepts et dimensions du modèle théorique de la réussite criminelle a permis de souligner l'importance de certaines caractéristiques dans la réussite criminelle des carders. En particulier, nous avons vu que l'expérience et les compétences sont des éléments tout autant essentiels à la réussite criminelle des carders ou de délinquants plus traditionnels (Tremblay & Morselli, 2000; McCarthy et Hagan 2001; Morselli et Tremblay 2004; Robitaille, 2004; Morselli, Tremblay et McCarthy 2006; Ouellet & Tremblay, 2014; Ouellet, 2018).

Pour continuer l'avancée des connaissances sur la réussite criminelle des carders, les futurs travaux qui s'attelleraient à utiliser des sondages pour interroger ces cyberdélinquants devront œuvrer à questionner des prédicteurs qui n'ont pas pu être mis en avant dans cette recherche. En effet, le contrôle de soi ou encore l'accès à des opportunités, qui influencent la réussite criminelle, n'ont pas été inclus dans notre sondage pour des raisons de temps de passation. Les futurs sondages en ligne devraient aussi pouvoir bénéficier de plus de moyens pour pouvoir obtenir plus de données dans un moindre temps. Notre démarche a mis en avant qu'il était

possible de collecter une cinquantaine de sondages complets au cours d'une période de 4 mois. En mettant plus de moyens sur un projet de recherche similaire, des résultats plus conséquents pourraient être obtenus. Ceci amènera le projet de recherche à bénéficier d'un plus grand échantillon pouvant mener à effectuer des analyses multivariées qui permettront une compréhension plus juste de la réussite criminelle des carders. Ces limites de notre recherche ne permettent pas la généralisation des résultats obtenus dans la mesure où aucune analyse multivariée n'a pu être entreprise et que les échantillons utilisés demeurent relativement petits pour affirmer pouvoir généraliser nos résultats.

BIBLIOGRAPHIE

- Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013). «Honor Among Thieves: A Common'S Analysis Of Cybercrime Economies.» *eCrime Researchers Summit (eCRS), 2013*. pp. 1-11.
- Aharoni, E., & Kiehl, K. A. (2013). «Evading Justice: Quantifying Criminal Success in Incarcerated Psychopathic Offenders.» *Criminal Justice and Behavior, 40*(6): 629-645.
- Akerlof, G. A. (1970). «The Market for Lemons: Quality, Uncertainty and the Market Mechanism.» *Quarterly Journal of Economics, 84*(3): 488-500.
- Aldridge, J., & Décary-Héту, D. (2014). «Not an'Ebay for Drugs': the Cryptomarket'Silk Road'as a Paradigm Shifting Criminal Innovation.»
- Allison, P. D. (2002). *Quantitative Applications in the Social Sciences: Missing data*. Thousand Oaks, CA: SAGE Publications, Inc.
- Anduiza, E., & Galais, C. (2016). “Answering Without Reading: IMCs and Strong Satisficing in Online Surveys.” *International Journal of Public Opinion Research, 29*(3), 497-519.
- Australian Payments Network (2018), «Fraud Statistics July 2018 - June 2018.» Australian Payments Network. Repéré au: <https://www.auspaynet.com.au/resources/fraud-statistics/July-2018-June-2018>
- Bancroft, A., & Reid, P. S. (2015). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy, 35*, 42-49.
- Barnett, V. & Lewis, T. (1994). *Outliers in Statistical Data, 3rd edn*. John Wiley & Sons.
- Barratt, M. J., & Aldridge, J. (2016). «Everything you Always Wanted to Know About Drug Cryptomarkets*(* but were afraid to ask).» *International Journal of Drug Policy, 35*: 1-6.

- Baumer, E. P., & Gustafson, R. (2007). «Social Organization and Instrumental Crime: Assessing the Empirical Validity of Classic and Contemporary Anomie Theories.» *Criminology*, 45(3): 617-663.
- Beach, D. A. (1989). «Identifying the Random Responder.» *The Journal of psychology*, 123(1), 101-103.
- Beaver, K. M., Schwartz, J. A., Nedelec, J. L., Connolly, E. J., Boutwell, B. B., & Barnes, J. C. (2013). «Intelligence is Associated with Criminal Justice Processing: Arrest Through Incarceration.» *Intelligence*, 41(5): 277-288.
- Benjamin, V., Li, W., Holt, T., & Chen, H. (2015, May). «Exploring Threats and Vulnerabilities in Hacker Web: Forums, IRC and Carding Shops.» In *Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on* (pp. 85-90). IEEE.
- Bernard, J., Shao, S., Tunc, C., Kheddouci, H., & Hariri, S. (2018). «Quasi-cliques Analysis for IRC Channel Thread Detection.» In *International Conference on Complex Networks and their Applications* (pp. 578-589). Springer, Cham.
- Blokland, A., Van Hout, L., van der Leest, W., & Soudijn, M. (2019). «Not your Average Biker; Criminal Careers of Members of Dutch Outlaw Motorcycle Gangs.» *Trends in Organized Crime*, 22(1), 10-33.
- Boccio, C. M., Beaver, K. M., & Schwartz, J. A. (2018). «The Role of Verbal Intelligence in Becoming a Successful Criminal: Results from a Longitudinal Sample.» *Intelligence*, 66: 24-31.
- Bouchard, M., & Ouellet, F. (2011). «Is Small Beautiful? The Link Between Risks and Size in Illegal Drug Markets.» *Global Crime*, 12(1): 70-86.
- Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press.

- Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Héту, D. (2016). «Studying Illicit Drug Trafficking on Darknet Markets: Structure and Organisation from a Canadian Perspective.» *Forensic science international*, 264: 7-14.
- Bulakh, V., & Gupta, M. (2015). «Characterizing Credit Card Black Markets On The Web.» *Proceedings of the 24th International Conference on World Wide Web*. Florence, Italie.
- Bylieva, D., Lobatyuk, V., & Rubtsova, A. (2018). «Homo Virtualis: Existence in Internet Space.» In *SHS Web of Conferences 44*.
- Caines, A., Pastrana, S., Hutchings, A., & Buttery, P. (2018). «Aggressive Language in an Online Hacking Forum.» In *Proceedings of the 2nd Workshop on Abusive Language Online (ALW2)* (pp. 66-74).
- Calderoni, F., & Superchi, E. (2019). «The Nature of Organized Crime Leadership: Criminal Leaders in Meeting and Wiretap Networks.» *Crime, Law and Social Change*, 1-26.
- Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). «Online Shopping Intention In The Context Of Data Breach In Online Retail Stores: An Examination Of Older And Younger Adults.» *Decision Support Systems*. 83: 47-56.
- Charest, M., & Tremblay, P. (2009). «Immobilité Sociale et Trajectoires de Délinquance.» *Revue française de sociologie*, 50(4): 693-718.
- Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2018). «Analysis of Hacking Related Trade in the Darkweb.» In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 79-84). IEEE.
- Christin, N. (2013). «Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace.» In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). ACM.

- Clarke, R. V., & Newman, G. R. (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. Cullumpton, Royaume-Uni: Willan Publishing.
- Coleman, R. P., Rainwater, L., & McClelland, K. A. (1979). *Social standing in America: New dimensions of class*. Taylor & Francis.
- CompariTech (2017) «Analysis: How Data Breaches Affect Stock Market Share Prices.» Repéré au: <https://www.comparitech.com/blog/information-security/data-breach-share-price/>
- Cornish, D. B. (1994). «The Procedural Analysis Of Offending And Its Relevance For Situational Prevention.» *Crime prevention studies*, 3: 151-196.
- Curran, P. G. (2016). “Methods for the Detection of Carelessly Invalid Responses in Survey Data”. *Journal of Experimental Social Psychology*, 66, 4-19.
- Custer, B., Pool, R. & Cornelisse, R. (2018). «Banking Malware and the Laundering of its Profits.» *European Journal of Criminology*, 1-19.
- Décary-Héту, D., & Dupont, B. (2012). «The Social Network Of Hackers.» *Global Crime*, 13(3): 160-175.
- Décary-Héту, D., & Giommoni, L. (2017). «Do Police Crackdowns Disrupt Drug Cryptomarkets?» A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, 67(1): 55-75.
- Décary-Héту, D., & Laferrière, D. (2015). «Discrediting Vendors in Online Criminal Markets.» In *Disrupting criminal networks: Network analysis in crime prevention* (pp. 129-152). Lynne Rienner, Boulder, CO.
- Décary-Héту, D., & Leppänen, A. (2013). «Criminals And Signals: An Assessment Of Criminal Performance In The Carding Underworld.» *Security Journal*.
- Décary-Héту, D., Mousseau, V., & Vidal, S. (2018). «Six Years Later: Analyzing Online Black Markets Involved in Herbal Cannabis Drug Dealing in the United States.» *Contemporary Drug Problems*, 45(4), 366-381.

- DeFilippi, D., & Michael, K. (2016). «Credit Card Fraud: Behind the Scenes.» *Online Banking Security Measures and Data Protection*. 263-282
- Department of Justice (2018) «Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than \$530 Million in Losses from Cybercrimes, 2018.» Repéré au: <https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible>
- Descormiers, K., Bouchard, M., & Ray, C. (2011). «Strain, Social Capital, and Access to Lucrative Crime Opportunities.» *International Journal of Child, Youth & Family Studies*, 2(1/2): 83.
- Devine, J., Egger-Sider, F., & Rojas, A. (2015). «The Evolving Impact of the Invisible Web: Exploring Economic and Political Ramifications.» *Journal of Web Librarianship*. 9(4): 145-161
- Dong, F., Yuan, S., Ou, H., & Liu, L. (2018, November). New Cyber Threat Discovery from Darknet Marketplaces. In *2018 IEEE Conference on Big Data and Analytics (ICBDA)* (pp. 62-67). IEEE.
- Du, P. Y., Zhang, N., Ebrahimi, M., Samtani, S., Lazarine, B., Arnold, N., & Chen, H. (2018). «Identifying, Collecting, and Presenting Hacker Community Data: Forums, IRC, Carding Shops, and DNMs.» In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 70-75). IEEE.
- Dupont, B. (2012). «Nouvelles Technologies Et Crime Désorganisé: Incursion Au Cœur D'Un Réseau De Pirates Informatiques.» *Sécurité et stratégie*. 11(4): 25-37.
- Dupont, B., Côté, A. M., Savine, C., & Décary-Hétu, D. (2016). «The Ecology of Trust Among Hackers.» *Global Crime*, 17(2): 129-151.
- Europol (2015), «*The Internet Organised Crime Threat Assessment, iOCTA*.» The Hague: Europol Police Office.

- Europol (2017), «The Internet Organised Crime Threat Assessment, iOCTA.» The Hague: Europol Police Office.
- Fader, J. J. (2016). «Criminal Family Networks: Criminal Capital and Cost Avoidance Among Urban Drug Sellers.» *Deviant Behavior*, 37(11): 1325-1340.
- Fallmann, H., Wondracek, G., & Platzer, C. (2010, July). «Covertly Probing Underground Economy Marketplaces.» *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. pp. 101-110. Bonn, Allemagne.
- Ferrell, O. C. (2016). «Broadening Marketing'S Contribution To Data Privacy.» *Journal of the Academy of Marketing Science*. 1-4.
- Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). «An Inquiry Into The Nature And Causes Of The Wealth Of Internet Miscreants.» *ACM conference on Computer and communications security*. pp. 375-388.
- Gambetta, D. (2009) *Codes of the Underworld: How Criminals Communicate*. New Jersey: Princeton Press University.
- Gelman, A., & Hill, J. (2007). *Data analysis using regression and hierarchical/multilevel models*. New York, NY: Cambridge.
- Greene, C., & Stavins, J. (2016).). «Did the Target Data Breach Change Consumer Assessments of Payment Card Security?» Repéré au: <https://www.bostonfed.org/-/media/Documents/researchdatareport/pdf/rdr1601.pdf>
- Gundur, R. V. (2019). «Finding the Sweet Spot: Optimizing Criminal Careers within the Context of Illicit Enterprise.» *Deviant Behavior*, 1-20.
- van Hardeveld, G. J., Webber, C., & O'Hara, K. (2016). «Discovering Credit Card Fraud Methods In Online Tutorials.» *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention*. Hanovre, Allemagne.

- van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). «Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis) Used by Carders on Cryptomarkets.» *American Behavioral Scientist*, 61(11): 1244-1266.
- Haslebacher, A., Onaolapo, J., & Stringhini, G. (2017). «All your Cards are Belong to us: Understanding Online Carding Forums.» In *Electronic Crime Research (eCrime), 2017 APWG Symposium on* (pp. 41-51). IEEE.
- Herley, C., & Florêncio, D. (2010). «Nobody Sells Gold For The Price Of Silver: Dishonesty, Uncertainty And The Underground Economy.» *Economics of Information Security and Privacy*. pp. 33-53.
- Holt, T. J. (2007). «Subcultural Evolution? Examining The Influence Of On-and Off-line Experiences On Deviant Subcultures.» *Deviant Behavior*. 28(2): 171-198.
- Holt, T. J. (2013a). «Examining the Forces Shaping Cybercrime Markets Online.» *Social Science Computer Review*, 31(2), 165-177.
- Holt, T. J. (2013b). «Exploring the Social Organisation and Structure of Stolen Data Markets.» *Global Crime*, 14(2-3): 155-174.
- Holt, T. J., & Bossler, A. M. (2014). «An Assessment of the Current State of Cybercrime Scholarship.» *Deviant Behavior*, 35(1): 20-40.
- Holt, T. J., & Dupont, B. (2018). «Exploring the Factors Associated with Rejection from a Closed Cybercrime Community.» *International journal of offender therapy and comparative criminology*.
- Holt, T. J., & Lampke, E. (2010). «Exploring Stolen Data Markets Online: Products And Market Forces.» *Criminal Justice Studies*. 23(1): 33-50.
- Holt, T. J., & Smirnova, O. (2014). «Examining the structure, organization, and processes of the international market for stolen data.» No known publisher.

- Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). «Exploring And Estimating The Revenues And Profits Of Participants In Stolen Data Markets.» *Deviant Behavior*, 37(4): 353-367
- Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). «Examining the risk reduction strategies of actors in online criminal markets.» *Global Crime*, 16(2): 81-103.
- Holz, T., Engelberth, M., & Freiling, F. (2009). «Learning More About The Underground Economy: A Case-Study Of Keyloggers And Dropzones.» *Computer Security - European Symposium on Research in Computer Security 2009*. pp1-18.
- Huang, J. L., Curran, P. G., Keeney, J., Poposki, E. M., & DeShon, R. P. (2012). “Detecting and Detering Insufficient Effort Responding to Surveys.” *Journal of Business and Psychology*, 27(1), 99-114.
- Huang, J.L., Liu, M., & Bowling, N.A. (2015). “Insufficient Effort Responding: Examining an Insidious Confound in Survey Data.” *Journal of Applied Psychology*, 100, 828–845.
- Hutchings, A. (2014). « Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission.» *Crime, Law and Social Change*, 62(1): 1-20.
- Hutchings, A., & Holt, T. J. (2014). «A Crime Script Analysis Of The Online Stolen Data Market.» *British Journal of Criminology*. 55(3): 596-614.
- Ilyin Y (2014) «Cybercrime Inc.: How profitable is the business?» *Kaspersky Lab Daily*.
Repéré au: <https://blog.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/15034/>
- James, L. (2005). «Phishing Exposed: Uncover Secrets from the Dark Side.» *Rockland, MA: Syngress*. pp.395.
- Javelin Strategy & Research (2017) *en attente de la livraison du rapport*.
- Jeffery, C. R. (1965). «Criminal Behavior and Learning Theory.» *J. Crim. L. Criminology & Police Sci.*, 56: 294.

- Johnson, J. A. (2005). "Ascertaining the Validity of Individual Protocols from Web-based Personality Inventories." *Journal of research in personality*, 39(1), 103-129.
- Jordan, T., & Taylor, P. (1998). «A Sociology Of Hackers.» *The Sociological Review*. 46(4): 757-780.
- Kashmiri, S., Nicol, C. D., & Hsu, L. (2016). «Birds Of A Feather: Intra-Industry Spillover Of The Target Customer Data Breach And The Shielding Role Of IT, Marketing, And CSR.» *Journal of the Academy of Marketing Science*. pp1-21.
- Kaufman, C.J., 1988. The application of logical imputation to household measurement. *Journal of the Market Research Society* 30, 453–466.
- Kazemian, L., & Le Blanc, M. (2007). «Differential Cost Avoidance and Successful Criminal Careers: Random or Rational?.» *Crime & Delinquency*, 53(1): 38-63.
- Krebs B. (2017). «2nd Breach at Verticalscope Impacts Millions». Repéré au: <https://krebsonsecurity.com/2017/11/2nd-breach-at-verticalscope-impacts/>
- Krebs B. (2019). «A Year Later, Cybercrime Groups Still Rampant on Facebook». Repéré au: <https://krebsonsecurity.com/2019/04/a-year-later-cybercrime-groups-still-rampant-on-facebook/>
- Krosnick, J. A. (1999). "Survey Research." *Annual review of psychology*, 50(1), 537-567.
- Kshetri, N. (2006). «The Simple Economics of Cybercrimes.» *IEEE Security & Privacy*, 4(1): 33-39.
- Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.
- Kwon, K. H., & Shakarian, J. (2018). Black-Hat Hackers' Crisis Information Processing in the Darknet: a Case Study of Cyber Underground Market Shutdowns. In *Networks, Hacking, and Media—CITA MS@ 30: Now and Then and Tomorrow* (pp. 113-135). Emerald Publishing Limited.

- Lall, R. (2016). How multiple imputation makes a difference. *Political Analysis*, 24(4), 414-433.
- Lastdrager, E. E. (2014). «Achieving A Consensual Definition Of Phishing Based On A Systematic Review Of The Literature.» *Crime Science*. 3(1): pp1.
- Leukfeldt, E. R. (2014). «Cybercrime and Social Ties» *Trends in organized crime*, 17(4): 231-249.
- Leukfeldt, E. R. (2015). «Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions.» *The European Review of Organised Crime*, 2(2): 91-103.
- Leukfeldt, R., Kleemans, E., & Stol, W. (2017). «The Use of Online Crime Markets by Cybercriminal Networks: A View From Within.» *American Behavioral Scientist*, 61(11): 1387-1402.
- Levitt, S. D., & Venkatesh, S. A. (2000). «An Economic Analysis of a Drug-selling Gang's Finances.» *The Quarterly Journal of Economics*, 115(3): 755-789.
- Little, R. J. (1988). A test of missing completely at random for multivariate data with missing values. *Journal of the American statistical Association*, 83(404), 1198-1202.
- Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). «Social Network Analysis of a Criminal Hacker Community.» *Journal of Computer Information Systems*, 51(2): 31-41.
- Lussier, P., Bouchard, M., & Beauregard, E. (2011). «Patterns of Criminal Achievement in Sexual Offending: Unravelling the “Successful” Sex Offender.» *Journal of Criminal Justice*, 39(5): 433-444.
- Lussier, P., & Mathesius, J. (2012). «Criminal Achievement, Criminal Career Initiation, and Detection Avoidance: The Onset of Successful Sex Offending.» *Journal of Crime and Justice*, 35(3): 376-394.

- Lusthaus, J. (2012). «Trust in the World of Cybercrime.» *Global crime*, 13(2): 71-94.
- Lusthaus, J. (2018). «Honour Among (Cyber) thieves?» *European Journal of Sociology/Archives Européennes de Sociologie*, 59(2), 191-223.
- Mann, C., & Stewart, F. (2000). *Internet communication and qualitative research: A handbook for researching online*. Sage.
- Manworren, N., Letwat, J., & Daily, O. (2016). «Why You Should Care About The Target Data Breach.» *Business Horizons*. 59(3): 257-266.
- Markham, A. N. (2011), «Internet Research ». *Qualitative Research: Issues of Theory, Method, and Practice*. pp.111–27.
- Mativat, F., & Tremblay, P. (1997). «Counterfeiting Credit Cards: Displacement Effects, Suitable Offenders and Crime Wave Patterns.» *The British Journal of Criminology*, 37(2): 165-183.
- Matsueda, R. L., Gartner, R., Piliavin, I., & Polakowski, M. (1992). «The Prestige of Criminal and Conventional Occupations: A Subcultural Model of Criminal Activity.» *American sociological review*, 57(6): 752-770.
- McCarthy, B., & Hagan, J. (2001). «When Crime Pays: Capital, Competence, and Criminal Success.» *Social forces*, 79(3): 1035-1060.
- McQuade, S. C. (2006). *Understanding and managing cybercrime*. Boston, MA: Pearson/Allyn and Bacon.
- Meade, A. W., & Craig, S. B. (2012). “Identifying Careless Responses in Survey Data.” *Psychological methods*, 17(3), 437.
- Moore, T., & Clayton, R. (2007). «An Empirical Analysis Of The Current State Of Phishing Attack And Defence.» *The Workshop of Economics and Informations Security*. Pittsburg, États-Unis.

- Moore, T., Clayton, R., & Anderson, R. (2009). «The Economics Of Online Crime.» *The Journal of Economic Perspectives*, 23(3): 3-20.
- Morselli, C. (2003). «Career Opportunities and Network-based Privileges in the Cosa Nostra.» *Crime, Law and Social Change*, 39(4): 383-418.
- Morselli, C., & Royer, M. N. (2008). «Criminal Mobility and Criminal Achievement.» *Journal of Research in Crime and Delinquency*, 45(1), 4-21.
- Morselli, C., & Tremblay, P. (2004a). «Délinquance, Performance et Capital Social: Une Théorie Sociologique des Carrières Criminelles.» *Criminologie*, 37(2): 89-122.
- Morselli, C., & Tremblay, P. (2004b). «Criminal Achievement, Offender Networks and the Benefits of Low Self-Control.» *Criminology*, 42(3): 773-804.
- Morselli, C., Tremblay, P., & McCarthy, B. (2006). «Mentors and Criminal Achievement.» *Criminology*, 44(1): 17-43.
- Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). «An Analysis Of Underground Forums.» *Proceedings of the 2011 Internet Measurement Conference*. Berlin, Allemagne.
- Naylor, R. T. (2003). «Towards a General Theory of Profit-Driven Crimes.» *British Journal of Criminology*, 43(1): 81-101.
- Nguyen, H., & Loughran, T. A. (2017). «On the Reliability and Validity of Self-Reported Illegal Earnings: Implications for the Study of Criminal Achievement.» *Criminology*, 55(3): 575-602.
- Olson, P. (2013). « The Man Behind Silk Road-The Internet's Biggest Market For Illegal Drugs.» *The Guardian*. Repéré au:

<https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht>

- Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional Manipulation Checks: Detecting Satisficing to Increase Statistical power.” *Journal of experimental social psychology*, 45(4), 867-872.
- Ouellet, F. (2018). «Stop and Go: Explaining the Timing of Intermittency in Criminal Careers.» *Crime & Delinquency*, 65(5): 630-656.
- Ouellet, M., Bouchard, M., & Charette, Y. (2019). «One Gang Dies, Another Gains? The Network Dynamics of Criminal Group Persistence.» *Criminology*, 57(1), 5-33.
- Ouellet, F., & Tremblay, P. (2014). «Épisodes d’Inactivité et Revenus Criminels dans une Trajectoire de Délinquance.» *Canadian Journal of Criminology and Criminal Justice*, 56(5): 527-562.
- Patil, S. J., & Dange, A. S. (2016). «Credit Card Fraud Detection Using Hidden Markov Model.» *International Journal of Engineering Science and Computing*. 6(4).
- Peretti, K. K. (2009). «Data Breaches: What The Underground World Of Carding Reveals.» *Santa Clara Computer & High Tech Law Journal*. 25: pp375.
- Piquero, A. R., Farrington, D. P., & Blumstein, A. (2003). «The Criminal Career Paradigm.» *Crime and justice*, 30: 359-506.
- Portnoff, R. S., Afroz, S., Durrett, G., Kummerfeld, J. K., Berg-Kirkpatrick, T., McCoy, D., & Paxson, V. (2017). «Tools for Automated Analysis of Cybercriminal Markets.» In *Proceedings of the 26th International Conference on World Wide Web* (pp. 657-666). International World Wide Web Conferences Steering Committee.
- Robitaille, C. (2004). «À qui Profite le Crime? Les Facteurs Individuels de la Réussite Criminelle.» *Criminologie*, 37(2): 33-62.

- Rowan, Z. R., McGloin, J. M., & Nguyen, H. (2017). «Capitalizing on Criminal Accomplices: Considering the Relationship between Co-offending and Illegal Earnings.» *Justice Quarterly*, 35(2): 1-29.
- Sampson, R. J., & Laub, J. H. (1995). *Crime in the making: Pathways and turning points through life*. Harvard University Press.
- Schonlau, M., Ronald Jr, D., & Elliott, M. N. (2002). *Conducting research surveys via e-mail and the web*. Rand Corporation.
- Sherstobitoff, R. (2008). «Anatomy of a Data Breach.» *Information Security Journal: A Global Perspective*, 17(5-6): 247-252.
- Shover, N., & Thompson, C. Y. (1992). «Age, Differential Expectations, and Crime Desistance.» *Criminology*, 30(1): 89-104.
- Smirnova, O., & Holt, T. J. (2017). «Examining the Geographic Distribution of Victim Nations in Stolen Data Markets. *American Behavioral Scientist*, 61(11): 1403-1426.
- Soudijn, M. R., & Zegers, B. C. T. (2012). «Cybercrime and virtual offender convergence settings.» *Trends in organized crime*, 15(2-3), 111-129.
- Soska, K., & Christin, N. (2015). «Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.» In *24th {USENIX} Security Symposium ({USENIX} Security 15)*(pp. 33-48).
- Sullivan, R. J. (2010). «The Changing Nature of US Card Payment Fraud: Industry and Public Policy Options.» *Economic Review-Federal Reserve Bank of Kansas City*. 95(2): pp101.
- Symantec Corporation. (2015). «2015 Internet Security Threat Report, Vol. 20.» Repéré au: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RP_T-internet-security-threat-report-volume-20-2015.pdf

- Symantec (2017). «Internet Security Threat Report.» Repéré au: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>
- Thomas, R., & Martin, J. (2006). «The Underground Economy: Priceless.» ;login.: *the magazine of USENIX & SAGE*, 31(6): 7-16.
- Thompson, M., & Uggen, C. (2012). «Dealers, Thieves, and the Common Determinants of Drug and Nondrug Illegal Earnings.» *Criminology*, 50(4): 1057-1087.
- Tillyer, M. S., & Tillyer, R. (2015). «Maybe I Should Do This Alone: A Comparison of Solo and Co-Offending Robbery Outcomes.» *Justice Quarterly*, 32(6): 1064-1088.
- Tremblay, P., Bouchard, M., & Petit, S. (2009). «The Size and Influence of a Criminal Organization: A Criminal Achievement Perspective.» *Global Crime*, 10(1-2): 24-40.
- Tremblay, P., & Morselli, C. (2000). «Patterns in Criminal Achievement: Wilson and Abrahamse Revisited.» *Criminology*, 38(2): 633-657.
- Tremblay, P., Talon, B., & Hurley, D. (2001). «Body Switching And Related Adaptations In The Resale Of Stolen Vehicles. Script Elaborations And Aggregate Crime Learning Curves.» *British Journal of Criminology*, 41(4): 561-579.
- Tsikriktsis, N. (2005). A review of techniques for treating missing data in OM survey research. *Journal of operations management*, 24(1), 53-62.
- Uggen, C., & Thompson, M. (2003). «The Socioeconomic Determinants of Ill-gotten Gains: Within-person Changes in Drug Use and Illegal Earnings.» *American Journal of Sociology*, 109(1): 146-185.
- Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., & Burns, L. (2016). «Who sells what? Country Specific Differences in Substance Availability on the Agora Cryptomarket.» *International Journal of Drug Policy*, 35: 16-23.

- Vasiu, I., & Vasiu, L. (2015). «Riders On The Storm: An Analysis Of Credit Card Fraud Cases.» *Suffolk Journal of Trial & Appellate Advocacy*. 20: 184-217.
- Wall, D. (2005). «The Internet as a Conduit For Criminal Activity». In: Pattavina, A. (2005). *Information Technology and the Criminal Justice System*. Sage Publications.
- Wall, D. (2007). *Cybercrime: The Transformation Of Crime In The Information Age*. Cambridge, Royaume-Uni: Polity.
- Wayman, J. C. (2003). “Multiple Imputation for Missing data: What is it and how Can I use it.” In *Annual Meeting of the American Educational Research Association, Chicago, IL* (Vol. 2, p. 16).
- Wehinger, F. (2011, September). «The Dark Net: Self-regulation Dynamics of Illegal Online markets for Identities and Related Services.» In *Intelligence and Security Informatics Conference (EISIC), 2011 European* (pp. 209-213). IEEE.
- Wilson, J. Q., & Abrahamse, A. (1992). «Does Crime Pay?.» *Justice quarterly*, 9(3): 359-377.
- Yip, M., Shadbolt, N., & Webber, C. (2012). «Structural Analysis of Online Criminal Social Networks.» In *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on* (pp. 60-65). IEEE.
- Yip, M., Shadbolt, N., & Webber, C. (2013). «Why forums?: An Empirical Analysis Into The Facilitating Factors Of Carding Forums.» *Proceedings of the 5th Annual ACM Web Science Conference*. Paris, France.

ANNEXE I

SCREENING QUESTIONS

*In this survey, **stolen financial information** will refer to the different products used in the carding process: dumps, fullz, card verification value (CVV) and financial institution website credentials (ex.: BankofAmerica, PayPal).*

1. Are you at least 18 years old or older?

- Yes
- No

2. In the past 12 months, have you sold stolen financial information through an online website, online autoshop, online forum, online chat room or online market at least once?

- Yes
- No

3. In the past 12 months, have you bought stolen financial information through an online website, online autoshop, online forum, online chat room or online market at least once?

- Yes
- No

SECTION I (SELLERS)

ASSESSING INCOMES AND PROFITS FROM THE SALE OF STOLEN FINANCIAL INFORMATION

*To assess your success, it is first important that we learn about your carding activities that come from **selling** stolen financial information and the income and profits they generated. Your **income** is the total amount of money (in USD) you earned from your carding activities that come from **selling** stolen financial information. Your **profits** are the net gains (in USD) once you take out the costs of generating that income. Remember that your responses cannot be linked to you.*

4. At how much would you estimate the income you earned directly from the sale of stolen financial information through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?

\$ USD

5. At how much would you estimate the profits you earned directly from the sale of stolen financial information through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?

\$ USD

6. Approximately how many stolen financial information (dumps, fullz, card verification value (CVV) or financial institution website credentials) have you sold through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?

7. In what year did you first start selling stolen financial information?

8. In the past 12 months, what products did you sell?

- Dumps
- Fullz
- Card Verification Value (CVV)
- Financial institution website credentials (ex.: BankofAmerica, PayPal)
- I would rather not say

- Other:

9. In the past 12 months, on which platforms did you sell stolen financial information?

- Online website
- Online autoshop
- Online forum
- Online chat room
- Online market
- I would rather not say

- Other:

10. In the past 12 months, besides your seller activities, did you play an official role on an online website, online autoshop, online forum, online chat room or online market related to carding?

- Administrator (write, publish and enforce platform rules)
- Moderator (assistant to an Administrator)
- Reviewer (tester of carding product quality)
- Escrow (broker in a transaction of carding product)
- I never had a role
- I would rather not say
- Other:

11. In the past 12 months, when selling stolen financial information from an online website, online autoshop, online forum, online chat room or online market, did you receive payments in the following currencies or from a legitimate financial service?

- Open cryptocurrencies (ex. Bitcoin, BitcoinCash, Litecoin, Ethereum)
- Anonymous cryptocurrencies (ex. Monero, DASH, Zcash)
- Legitimate financial services (ex. PayPal, Bank transfers, Western Union)
- I would rather not say
- Other:

SECTION I (BUYERS)

ASSESSING INCOMES AND PROFITS FROM THE STOLEN FINANCIAL INFORMATION YOU BOUGHT ONLINE

*To assess your success, it is also important that we learn about your carding activities that come from **buying** stolen financial information and the income and profits they generated. Your **income** is the total amount of money (in USD) you earned from your carding activities that come from **buying** stolen financial information. Your **profits** are the net gains (in USD) once you take out the costs of generating that income. Remember that your responses cannot be linked to you.*

12. At how much would you estimate the income (in USD) you earned directly from the use of stolen financial information you bought through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?

\$ USD

13. At how much would you estimate the profits (in USD) you earned directly from the use of stolen financial information you bought through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?

\$ USD

14. Approximately how many stolen financial information (dumps, fullz, card verification value (CVV) or financial institution website credentials) have you bought through an online website, online autoshop, online forum, online chat room or online market in the past 12 months?

15. In which year did you first start buying stolen financial information?

16. In the past 12 months, what products did you use as part of your carding activities?

- Dumps
- Fullz
- Card Verification Value (CVV)
- Financial institution website credentials (ex.: BankofAmerica, PayPal)
- I would rather not say
- Other:

17. In the past 12 months, on which platforms did you buy stolen financial information?

- Online website
- Online autoshop
- Online forum
- Online chat room
- Online market
- I would rather not say
- Other:

18. In the past 12 months, apart from your buyer activities, did you have another role on an online website, online autoshop, online forum, online chat room or online market related to carding?

- Administrator (write, publish and enforce platform rules)
- Moderator (assistant to an Administrator)
- Reviewer (tester of carding product quality)
- Escrow (broker in a transaction of carding product)
- I never had a role
- I would rather not say

Other:

19. In the past 12 months, when buying stolen financial information from an online website, online autoshop, online forum, online chat room or online market, did you use the following currencies or legitimate financial service?

- Open cryptocurrencies (ex. Bitcoin, BitcoinCash, Litecoin, Ethereum)
- Anonymous cryptocurrencies (ex. Monero, DASH, Zcash)
- Legitimate financial services (ex. PayPal, Bank transfers, Western Union)
- I would rather not say

Other:

SECTION II (SELLERS)

CARDING EXPERIENCES : COMPETENCES AND SKILLS

*Competences and skills are important drivers of success. We would like to know more about yours as a carder who **sells** stolen financial information. Remember that your responses cannot be linked to you.*

20. In the past 12 months, did you ever use malware to steal financial information?

- Yes
- No
- I would rather not say

21. Were you ever recruited by a group of at least two people to help in the sale of financial information?

- Yes
- No
- I would rather not say

22. To the best of your knowledge, on an online forum or an online chat room, did anyone ever publicly or privately vouch for your competence or ability to sell financial information?

- Yes
- No
- I would rather not say

23. On a scale of 1 to 10 where 10 is the most competent and 1 is the least competent, how would you rate your competence at selling stolen financial information?

 [1 - 10]

SECTION II (BUYERS)

CARDING EXPERIENCES : COMPETENCES AND SKILLS

*Competences and skills are important drivers of success. We would like to know more about yours as a carder who **buys** stolen financial information. Remember that your responses cannot be linked to you.*

24. Were you ever recruited by a group of at least two people to help in the monetizing of stolen financial information?

- Yes
- No
- I would rather not say

25. To the best of your knowledge, on an online forum or an online chat room, did anyone ever publicly or privately vouch for your competence or ability to monetize stolen financial information?

- Yes
- No
- I would rather not say

26. On a scale of 1 to 10 where 10 is the most competent and 1 is the least competent, how would you rate your competence at monetizing stolen financial information?

 [1 - 10]

SECTION III (BUYERS)

CARDING EXPERIENCES : EXPERIENCES OF VICTIMISATION

*Some academics works have shown that carders' communities could be infested by rippers. Those unwanted participants try to scam others by, for example, selling bad quality products or by never sending the products the were paid for. In order to understand the factors which affect your success, it is important that we learn more about **your experiences of victimisation** to weigh how they impact your success. Remember that your responses cannot be linked to you.*

27. In the past 12 months, how often were you scammed while buying stolen financial information?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

28. In the past 12 months, how often were you scammed while buying stolen financial information on an online website?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

29. In the past 12 months, how often were you scammed while buying stolen financial information on an online autoshop?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

30. In the past 12 months, how often were you scammed while buying stolen financial information on an online forum?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

31. In the past 12 months, how often were you scammed while buying stolen financial information on an online chat room?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

32. In the past 12 months, how often were you scammed while buying stolen financial information on an online market?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

SECTION IV

CARDING EXPERIENCES : ANONYMIZATION TOOLS

*Academic studies have shown that a significant portion of carders may not be using on an ongoing basis **anonymization tools**. In this section, we need to ask you how often you use the following tools during your carding activities. Your responses will help us to understand the impact of such uses on your success.*

33. In the past 12 months, how often did you use virtual machine technics as part of your carding activities?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

34. In the past 12 months, how often did you use anonymity-focused operating system (ex. TAILS) as part of your carding activities?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

35. In the past 12 months, how often did you use virtual private networks or SOCKS as part of your carding activities?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

36. In the past 12 months, how often did you use communication encryption technologies (ex. PGP, GPG) as part of your carding activities?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

37. In the past 12 months, how often did you use a darknet (ex. Tor network, I2P, Freenet) as part of your carding activities?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

38. In the past 12 months, how often did you use money laundering services (ex. cryptocurrency anonymizer, tumblers, online casinos, money mules). as part of your carding activities?

- 100% of the time
- At least 75% of the time
- At least 50% of the time
- At least 25% of the time
- Less than 25% of the time
- Never
- I would rather not say

SECTION V (SELLERS)

CONTACT NETWORKS WHILE SELLING STOLEN FINANCIAL INFORMATION

*Some studies have shown that a large number of contacts can increase the benefits of carders (ex.: larger incomes, lower rate of detection). To better understand the relationship between social contacts and success, we need to ask you about **the individuals that you interacted with** when you **sold** stolen financial information.*

39. In the past 12 months, how many customers did you have?

40. In the past 12 months, how many people facilitated your sales of stolen financial information through their legitimate enterprises while not being aware of the illicit nature of your activities?

41. In the past 12 months, how many people facilitated your sales of stolen financial information through their legitimate enterprises while being aware of the illicit nature of your activities?

SECTION V (BUYERS)
CONTACT NETWORKS WHILE BUYING STOLEN FINANCIAL INFORMATION

*Some studies have shown that a large number of contacts can increase the benefits of carders (ex.: larger incomes, lower rate of detection). To better understand the relationship between social contacts and success, we need to ask you about **the individuals that you interacted with** when you **bought** stolen financial information.*

42. In the past 12 months, from how many sellers did you buy stolen financial information from?

43. In the past 12 months, how many people facilitated your purchases of stolen financial information through their legitimate enterprises while not being aware of the illicit nature of your activities?

44. In the past 12 months, how many people facilitated your purchases of stolen financial information through their legitimate enterprises while being aware of the illicit nature of your activities?

SECTION VI
DEMOGRAPHICS

This section asks a few questions about your background and will allow us to reliably assess the interaction between carding and success, while accounting for individual differences. Remember that your responses cannot be linked to you.

45. How old are you?

46. What is your gender?

Female

Male

Other

I would rather not say

47. Have you ever been convicted or found guilty of a criminal offence?

- Yes
- No
- I would rather not say

48. What is the highest level of education you have completed?

- No high school
- High school
- College diploma/Technical vocation
- University Degree
- Graduate studies (Masters/Ph.D.)
- I would rather not say

49. In the past 12 months, how much did you earn in USD from your legitimate activities?

\$ USD

50. In the past 12 months, how much did you earn in USD from other illegitimate activities?

\$ USD

51. In the past 12 months, how many hours per week did you spend buying and monetizing stolen financial information?

Hour(s) per week

52. In the past 12 months, how many hours per week did you spend selling stolen financial information?

Hour(s) per week

53. In the past 12 months, how many hours per week did you spend doing other criminal activities?

Hour(s) per week

ANNEXE II



INFORMED CONSENT FROM

« Carders and criminal success »

Who runs the project?

I, Mathieu Guillot. I am a master's degree student at the University of Montreal, School of Criminology. My research supervisor is David Décary-Héту, Assistant Professor, School of Criminology.

Tell me more about this project

The purpose of my research project is to improve our understanding of carders' criminal success. This concept will be mainly analysed through financial success. Our goal is to survey carders regarding their incomes, sociodemographics, criminal experiences and sociability.

If I participate, what do I have to do?

You will have to answer an online survey that should take about 15 minutes. The survey will make sure that you are connected to the TOR network and that your javascript is disabled before you answer the survey (though it will be possible for you to bypass these restrictions should you want to do so). None of your answers will be recorded unless you press the button at the end of the survey. We will never ask for any identifying information such as your name or your online vendor name.

Are there risks or benefits when participating in this research?

There is no risk to answer my questions. We will not collect any personally identifiable information and we will never share the data we collect with any other individual, organization or group. If you wish, you can simply decide not to answer any question that you want and leave the survey page whenever you want. Should you leave the survey page without submitting your answers by pressing the button at the bottom of the page, none of your answers will be collected. You will not be paid for your participation and you will not be making any personal benefit. Your participation could however help us better understand the real impact of carding activities.

What will you do with my answers?

I will analyze all the responses that all participants have given me to understand the impact of cryptomarkets on traditional illicit drug markets. Those analyses will be published in my master's thesis. You will be provided with a private URL so that you can access those papers for free.

Will my personal information be protected?

Yes! No information that could identify you in one way or another will be collected – not even your online vendor name. In addition, the information collected will be kept confidential. The survey data will be kept on an encrypted hard drive in a secure room at the University of Montreal. The records will be destroyed seven years after the end of my project.

Do I have to answer all the questions and go to the end?

No! You can choose not to answer one or more questions. You can at any time decide that you no longer want to participate in the survey and that you abandon the project. In this case, you can simply leave the survey page without pressing the button at the bottom of the page. None of your answers will be saved should you decide to leave the survey page.

Who can I contact if I have questions during the study?

For questions, you can contact me by telephone (+1 514-xxx-xxxx), by email (mathieu.guillot@umontreal.ca) and by secure text messaging using Wickr (xxxxx). After you submit your answers, you will be provided with a unique random participant ID. It will be essential that you keep this ID as it will be the only method for me to identify you.

This project was approved by the Research Ethics Committee of Arts and Sciences University of Montreal. For any concerns about your rights or responsibilities of researchers regarding your participation in this project, you can contact the committee by phone (+1-514-343-7338) or by e-mail (ceras@umontreal.ca). You can also visit the Web site: <http://recherche.umontreal.ca/participants>.

If you have complaints about your participation in this research, you can contact the Ombudsman (which is a "protector of citizens") of the University of Montreal by telephone (+1-514-343-2100) or by email (ombudsman@umontreal.ca). The Ombudsman accepts collect calls.

How can I give my consent to participate in the study?

By clicking the button at the bottom of this page. I recommend that you print or bookmark this page for future references.

Participant déclaration

- I understand that I can take my time to think before giving or not my consent.
- I can ask any question I want to the researcher and request that I receive adequate answers.
- I understand that by participating in this research project, I do not give up any or my rights nor do I release the researcher from his responsibilities.
- I have read the present informed consent form and I consent to participate in this research project. I agree with the participant declaration and I wish to answer the survey

I agree with the participant declaration and I wish to answer the survey

ANNEXE III



Comité d'éthique de la recherche en arts et en sciences

5 novembre 2018

Objet : Approbation éthique – « La réussite criminelle des participants à la fraude financière en ligne »

Monsieur,

Le Comité d'éthique de la recherche en arts et en sciences (CÉRAS) a étudié le projet de recherche susmentionné et a délivré le certificat d'éthique demandé suite à la satisfaction des exigences précédemment émises. Vous trouverez ci-joint une copie numérisée de votre certificat; copie également envoyée à votre directeur/directrice de recherche et à la technicienne en gestion de dossiers étudiants (TGDE) de votre département.

Notez qu'il y apparaît une mention relative à un suivi annuel et que le certificat comporte une date de fin de validité. En effet, afin de répondre aux exigences éthiques en vigueur au Canada et à l'Université de Montréal, nous devons exercer un suivi annuel auprès des chercheurs et étudiants-chercheurs.

De manière à rendre ce processus le plus simple possible et afin d'en tirer pour tous le plus grand profit, nous avons élaboré un court questionnaire qui vous permettra à la fois de satisfaire aux exigences du suivi et de nous faire part de vos commentaires et de vos besoins en matière d'éthique en cours de recherche. Ce questionnaire de suivi devra être rempli annuellement jusqu'à la fin du projet et pourra nous être retourné par courriel. La validité de l'approbation éthique est conditionnelle à ce suivi. Sur réception du dernier rapport de suivi en fin de projet, votre dossier sera clos.

Il est entendu que cela ne modifie en rien l'obligation pour le chercheur, tel qu'indiqué sur le certificat d'éthique, de signaler au CÉRAS tout incident grave dès qu'il survient ou de lui faire part de tout changement anticipé au protocole de recherche.

Nous vous prions d'agréer, Monsieur, l'expression de nos sentiments les meilleurs,

Marie-Pierre Bousquet, présidente
Comité d'éthique de la recherche en arts et en sciences (CÉRAS)
Université de Montréal

c. c. David Décary-Héту, professeur adjoint, FAS - École de criminologie
Cécile Sike Mouen, TGDE

p. j. Certificat #CERAS-2018-19-164-D

adresse postale
C.P. 6128, succ. Centre-ville
Montréal QC H3C 3J7

adresse civique
3333, Queen Mary
Local 220-2
Montréal QC H3V 1A2
www.ceras.umontreal.ca

Téléphone : 514-343-7338
ceras@umontreal.ca

Comité d'éthique de la recherche en arts et en sciences

CERTIFICAT D'APPROBATION ÉTHIQUE

Le Comité d'éthique de la recherche en arts et en sciences (CÉRAS), selon les procédures en vigueur, en vertu des documents qui lui ont été fournis, a examiné le projet de recherche suivant et conclu qu'il respecte les règles d'éthique énoncées dans la Politique sur la recherche avec des êtres humains de l'Université de Montréal.

Projet	
Titre du projet	La réussite criminelle des participants à la fraude financière en ligne
Étudiant requérant	Mathieu Guillot, étudiant à la maîtrise, FAS - École de criminologie
Sous la direction de	David Décary-Héту, professeur adjoint, FAS – École de criminologie, Université de Montréal
Financement	
Organisme	Non financé
Programme	
Titre de l'octroi si différent	
Numéro d'octroi	
Chercheur principal	
No de compte	

MODALITÉS D'APPLICATION

Tout changement anticipé au protocole de recherche doit être communiqué au CÉRAS qui en évaluera l'impact au chapitre de l'éthique.

Toute interruption prématurée du projet ou tout incident grave doit être immédiatement signalé au CÉRAS.

Selon les règles universitaires en vigueur, un suivi annuel est minimalement exigé pour maintenir la validité de la présente approbation éthique, et ce, jusqu'à la fin du projet. Le questionnaire de suivi est disponible sur la page web du CÉRAS.

Marie-Pierre Bousquet, présidente
Comité d'éthique de la recherche en arts
et en sciences
Université de Montréal

5 novembre 2018
Date de délivrance

1^{er} décembre 2021
Date de fin de validité

1^{er} décembre 2019
Date de suivi

adresse postale
C.P. 6128, succ. Centre-ville
Montréal QC H3C 3J7

adresse civique
3333, Queen Mary
Local 220-2
Montréal QC H3V 1A2
www.ceras.umontreal.ca

Téléphone : 514-343-7338
ceras@umontreal.ca