LES LIENS FAIBLES DU CRIME EN LIGNE :
ÉCOLOGIE DE LA MÉFIANCE AU SEIN DE DEUX COMMUNAUTÉS DE HACKERS MALVEILLANTS

Benoît Dupont
Université de Montréal - Centre international de criminologie comparée
Benoit.dupont@umontreal.ca

Résumé : Le dilemme de la confiance auquel sont confrontés les délinquants en ligne est souvent sous-estimé par ceux qui étudient les transformations que la révolution numérique a provoqué sur la criminalité. Pourtant, dans un contexte où une diversité d'expertises techniques et organisationnelles doivent converger afin de mener des projets lucratifs, les liens de confiance jouent un rôle déterminant permettant d'écarter les partenaires à la fiabilité douteuse et de stabiliser les collaborations afin d'améliorer la performance criminelle. À travers deux études de cas portant sur un réseau de hackers démantelé au Québec en 2008 et le principal forum de discussion de pirates informatiques observé pendant 27 mois de 2009 à 2011, cet article illustre les défis concrets auxquels les cybercriminels sont confrontés dans l'attribution et le maintien de la confiance à des pairs qui ont de nombreuses raisons de faire défection sans risques de sanctions. La nature fragile et éphémère des liens de confiance est notamment analysée, ainsi que le rôle joué par des normes culturelles transgressives qui empêchent les communautés de hackers de profiter pleinement des avantages des outils de gestion automatisée des réputations.

Version initiale du texte publié dans *Réseaux*, no. 197-198, pp. 109-136, 2016.

Le dilemme de la confiance auquel sont confrontés les délinquants en ligne est souvent sous-estimé par ceux qui étudient les transformations que la révolution numérique a provoqué sur la criminalité. Journalistes (Poulsen, 2011 ; Glenny, 2012 ; Krebs, 2014) et criminologues (Newman et Clarke, 2003 ; McGuire, 2007 ; Wall, 2007) décrivent avec force détails l'émergence d'une délinquance mondialisée capable d'exploiter pleinement le potentiel collaboratif d'internet pour structurer des réseaux internationaux de hackers aux talents complémentaires et aux performances dignes des startup de la Silicon Valley. S'il semble logique que les entrepreneurs illicites cherchent à mobiliser les innovations technologiques associées à la démocratisation de l'internet pour améliorer leur productivité et leur efficacité, à l'instar de leurs homologues de l'économie légale ces deux dernières décennies, le contexte organisationnel et juridique hostile dans lequel ils opèrent s'avère néanmoins source de nombreuses contraintes venant limiter leur capacité à profiter pleinement de ces bénéfices.

Quelques récents cas médiatisés de hackers de haut vol ayant été arrêtés au cours des dernières années par la police font par exemple état des nombreuses trahisons ayant précipité la chute de ces délinquants. Max Butler, qui fut l'un des pionniers dans l'univers de la fraude par carte bancaire et fusionna de manière hostile sept forums clandestins de revente de numéros de cartes volées et les 10 000 hackers qui les fréquentaient, fut livré à la police par l'un de ses complices, interpellé lors d'une opération de routine et cherchant ainsi à négocier une peine allégée (Poulsen, 2011). Le forum DarkMarket, qui était l'une des principales plateformes d'échange entre cyberdélinquants anglophones, fut démantelé durant la même période, ayant été infiltré par un agent du FBI qui parvint à en prendre le contrôle et à convaincre les autres participants de son statut de hacker légitime. Malgré la méfiance exprimée ouvertement par certains utilisateurs suspicieux, l'agent Mularski parvint à accumuler suffisamment de preuves pendant les deux années durant lesquelles il administra le forum pour conduire à l'arrestation d'une soixantaine de hackers (Poulsen, 2008 ; Glenny, 2012). Les cyberdélinquants russes ne sont pas à l'abri de la duplicité de leurs homologues, comme l'illustre la Guerre des deux principaux sites de produits pharmaceutiques contrefaits (GlavMed et Rx-Promotion), initiée par leurs propriétaires respectifs. Après une courte période de collaboration, ces deux entrepreneurs à l'origine de plus de 75% des envois massifs de pourriels (spam) expédiés quotidiennement par des dizaines de botnets se livrèrent à des attaques qui culminèrent dans la compromission réciproque et la divulgation publique de leurs bases de données internes (Krebs, 2014).

La confiance comme critère central dans la sélection et le recrutement de collaborateurs potentiels, ainsi que dans le maintien de relations productives avec ces derniers, constitue la question centrale abordée dans cet article. Prélude incontournable à la coopération et aux modes organisationnels qui régissent cette dernière, la confiance –ou son absence– mérite une plus grande attention de la part de ceux qui étudient la délinquance en ligne, notamment par une analyse empirique approfondie de ses manifestations concrètes. Il existe une importante littérature de nature théorique sur la confiance comme mécanisme de réduction de la complexité sociale destiné à limiter l'incertitude dans les processus de

prise de décision, et sur les nuances à établir entre la familiarité et la confiance, sur les divers mécanismes qui facilitent l'émergence d'une confiance personnelle ou au contraire systémique, ou enfin sur les processus par lesquels la méfiance l'emporte sur la confiance et paralyse les actions collectives (Luhmann, 2006 ; Gambetta, 2008). Toutefois, les études empiriques consacrées à l'expression des divers modes de confiance et à leurs retombées sur les pratiques délinquantes restent relativement rares (von Lampe et Johansen, 2004).

Nous tentons donc de comprendre dans cet article, à travers l'étude de deux groupes de pirates informatiques malveillants aux caractéristiques très différentes, comment la confiance peut s'établir, se maintenir ou au contraire se déliter entre délinquants conduits à collaborer dans le cadre de projets complexes liés à la création, la gestion et l'exploitation de botnets, qui constituent l'épine dorsale technique du cybercrime. La première section est consacrée à l'examen des caractéristiques organisationnelles de la cybercriminalité, qui se manifestent par la conception et la mise en oeuvre de projets complexes faisant appel à de multiples compétences techniques et sociales. Les mécanismes destinés à réguler les conduites des participants dans un environnement socio-technique où les moyens habituels du contrôle social informel sont absents sont d'un intérêt particulier. La seconde section est consacrée à l'étude d'un groupe de dix pirates informatiques arrêtés au Québec en 2008 pour avoir infecté plusieurs centaines de milliers d'ordinateurs et les avoir utilisés afin de lancer des attaques informatiques par déni de service. On examine plus spécialement la distribution des compétences au sein de ce réseau, le rôle que la confiance y joue afin de faciliter la collaboration de ces expertises diverses, et la dégradation rapide des liens de confiance les plus fragiles en expressions de méfiance et d'hostilité nuisant à la performance du réseau. Finalement, la troisième et dernière section permet un changement de perspective en portant le questionnement sur un échantillon beaucoup plus large d'un peu moins de 20 000 hackers ayant échangé pendant 27 mois plus de 285 000 évaluations destinées à quantifier leur réputation, une composante essentielle du processus d'allocation de la confiance. La structure des points de réputation distribués, ainsi que l'évolution temporelle et les motifs sous-jacents de ces évaluations sont analysés, montrant là encore la fragilité et l'instabilité de la confiance entre cyberdélinquants qui en paient le prix par une performance réduite.

LE DILEMME DE LA CONFIANCE POUR LES RÉSEAUX DE DÉLINQUANCE EN LIGNE

Les schémas de co-délinquance observés parmi des groupes aussi diversifiés que des gangs de rue (Densley, 2012), des jeunes sans domicile fixe (McCarthy et al., 1998), des réseaux informels de cambrioleurs (Shover, 1973 ; Hobbs, 1995) ou des groupes criminels organisés de type mafieux (Kleemans et van de Bunt, 1999) font apparaître le rôle prépondérant joué par certains lieux de convergence permettant à des individus à la recherche d'associés ou d'auxiliaires de recruter ces derniers parmi un bassin de personnes présélectionnées et répondant à certains critères de fiabilité. Certains quartiers urbains marginalisés où se concentrent pauvreté et délinquance, les écoles où sont scolarisés les enfants de ces communautés en difficulté, les lieux de socialisation que sont les bars, cafés et autres clubs sportifs, ou encore de plus ou moins longues périodes de détention commune (Clear, 1996) constituent autant de terrains de recrutement privilégiés insérés dans une vaste toile relationnelle permettant d'évaluer par le bouche-à-oreille la réputation locale de chaque

individu, en fonction de son expertise, de son expérience et de sa fiabilité. Ces mécanismes de conversion de la réputation en confiance, qui s'avèrent déterminants dans un environnement hostile où les échecs, les erreurs, et les actes de malveillance se soldent par des arrestations policières et d'éventuelles condamnations à des peines d'emprisonnement (Tilly, 2005), ne sont pas aussi aisément accessibles aux délinquants en ligne dont les réseaux de collaboration se déploient à l'échelle internationale et incluent des complices qu'ils ont rarement eu l'occasion de côtoyer en personne. Pourtant, cette délinquance par projet à forte intensité technologique repose sur la capacité d'inconnus à nouer des relations de coopération durables dans un contexte où les incitatifs économiques plaident plutôt en faveur de comportements opportunistes et utilitaristes. Pour y parvenir, des mécanismes formels de garantie de la confiance ont été adoptés par les communautés de hackers malveillants afin de décourager les plus prédateurs d'entre eux et favoriser ainsi l'émergence de marchés fonctionnels de produits et de services illicites.

De la délinquance artisanale à la délinquance par projet : l'impératif de la coopération

Dans un court ouvrage consacré à l'organisation de la délinquance et à son histoire, la sociologue Mary McIntosh (1975) délaisse l'approche individualiste et psychologique chère à de nombreux criminologues pour se focaliser sur la dimension organisationnelle des crimes acquisitifs, proposant notamment une typologie quadripartite qui distingue des modes d'organisation artisanaux, picaresques, par projet, et entrepreneuriaux. Cette typologie relativement sommaire et principalement élaborée à l'aide de sources documentaires nous aide néanmoins à comprendre les transformations organisationnelles que la Révolution industrielle, puis la Révolution numérique, ont fait subir à l'organisation sociale de la délinquance. On peut résumer son propos à l'évolution de formes de délinquance mobilisant des équipes réduites de brigands, pirates et fraudeurs généralistes commettant des vols à petite échelle vers des structures plus structurées de délinquants spécialisés disposant d'expertises techniques complémentaires et s'attaquant à des projets plus ambitieux requérant une importante planification comme la fraude massive, l'extorsion ou la contrebande. Cette évolution reflète en grande partie les transformations sociales et économiques liées à la concentration du capital qui ont fait des entreprises des cibles de choix du fait de leur statut de productrices, dépositaires ou protectrices de richesses en grande partie dématérialisées. Bien qu'elles offrent des opportunités beaucoup plus intéressantes de profit aux délinquants, ces organisations déploient également des ressources considérables pour assurer leur sécurité, ce qui explique le recours à des formes d'organisation délinquante plus élaborées.

Si les mafias représentent probablement la version la plus aboutie, quoiqu'imparfaite, d'une transposition des valeurs, des structures et des mécanismes entrepreneuriaux à des activités illicites, rien ne permet d'affirmer que les groupes ou les communautés de délinquants en ligne remplissent les conditions requises pour être définies comme des groupes criminels organisés au sens de la littérature criminologique (Grabosky, 2013 ; Lusthaus, 2013). La difficulté de maintenir des liens hiérarchiques forts, le manque d'emprise exclusive sur certains territoires ou marchés criminels, ou encore l'impossibilité matérielle de se prévaloir du recours à la violence physique comme outil coercitif

constituent des obstacles majeurs à l'émergence d'une cybercriminalité organisée de type mafieux. Les entrepreneurs en cybercriminalité privilégient donc la forme d'organisation par projet afin de mutualiser les expertises indispensables à la réussite des fraudes et des attaques qu'ils mènent à une échelle industrielle. Bien loin du mythe du hacker solitaire et omnipotent propagé par les stéréotypes de la production cinématographique hollywoodienne (Wall, 2010), les rares études empiriques menées sur les collectifs de cybercriminels ont en effet confirmé l'intuition de Mary McIntosh sur l'importance d'équipes et de collaborations éphémères constituées d'individus possédant des expertises techniques complémentaires et ayant négocié une répartition des profits selon des formules tenant compte de leur contribution respective au succès du projet.

Tom Holt (2013) et Anita Lavorgna (2015) ont ainsi étudié la configuration organisationnelle de réseaux de revendeurs de numéros de cartes de crédit volées et de trafiquants d'animaux de compagnie opérant en ligne. S'inspirant de la grille analytique de Best et Luckenbill (1994), qui vise à mesurer le degré de complexité d'associations criminelles à travers quatre dimensions (association mutuelle, participation mutuelle, division du travail, stabilité temporelle), ces deux auteurs mettent en lumière la prédominance de forums de discussion qui constituent de véritables marchés numériques clandestins vers lesquels acheteurs et vendeurs convergent. Les forums et les outils de communication qui y sont associés favorisent la coopération entre une multitude de délinquants mettant leur expertise au service de projets ponctuels. Les codeurs de logiciels malveillants peuvent ainsi y entrer en contact avec des pirates ayant découvert des vulnérabilités inconnues (les *0-day exploits*), des hébergeurs complaisants leur garantissant un accès anonyme et persistant à des infrastructures techniques, des opérateurs de botnets spécialisés dans l'infection de millions d'ordinateurs qui seront exploités à l'insu de leurs propriétaires légitimes, des fraudeurs cherchant à utiliser leurs services pour se procurer des informations personnelles de nature financière, des spécialistes en 'monétisation' qui sauront convertir ces informations en profits, ou encore des *mules*, ces participants plus ou moins volontaires qui permettront le transfert anonyme des fonds des pays des victimes vers ceux des délinquants (Ablon et al., 2014 ; Broadhurst et al., 2014). Cette forme d'organisation collégiale des schémas de collaboration est toutefois confrontée au défi majeur de la duplicité structurelle qui prévaut sur ces marchés.

Duplicité, impunité et 'rippers'

Nous avons déjà indiqué plus haut que la délinquance en ligne se distingue des formes plus traditionnelles de criminalité par l'absence de recours possible à la violence comme mode de régulation des conflits. La distance géographique qui sépare physiquement ceux qui transigent sur ces marchés illicites mondialisés, ainsi que l'anonymat masquant leur véritable identité constituent en effet des obstacles structurels difficiles à surmonter pour tout participant mécontent désirant exercer des représailles contre un vendeur ou un fournisseur indélicat (Mell, 2012 ; Yip et al., 2013). Par ailleurs, ces caractéristiques d'extension du périmètre spatial et d'anonymat des interactions, combinées à un stock potentiellement illimité de co-délinquants interchangeables, viennent également affaiblir les trois autres mécanismes classiques d'incitation à la coopération criminelle que sont des

intérêts économiques communs, des liens personnels d'obligations réciproques ou une croyance partagée dans l'utilité de la collaboration (Gambetta 1988).

Dans un tel contexte, la duplicité s'avère souvent plus profitable que la coopération, ce qui explique que les marchés criminels en ligne soient infestés de 'rippers' (ou arnaqueurs), terme utilisé pour désigner les participants malhonnêtes qui ne fournissent pas les produits ou les services pour lesquels ils ont été dûment rémunérés (Herley et Florêncio, 2010). Les 'rippers' sont omniprésents sur les forums de discussion consacrés à la cybercriminalité, et représentent dans les cas les plus extrêmes jusqu'à 22% du volume des transactions offertes aux participants (Franklin et al., 2007). Le renouvellement constant d'une population de délinquants débutants attirés par le mirage de l'argent facile offre aux 'rippers' un réservoir important de victimes crédules, et l'impunité dont ils bénéficient constitue un facteur de motivation non négligeable. Cependant, pour les cyberdélinquants plus expérimentés et les administrateurs de ces forums, l'omniprésence des 'rippers' génère un fort sentiment d'incertitude et de méfiance qui affecte de manière négative le volume des échanges et paralyse les collaborations, rendant ces marchés illicites dysfonctionnels.

En d'autres termes, si la délinquance en ligne est en mesure d'exploiter pleinement les nouvelles technologies de l'information pour s'affranchir des contraintes spatiales et temporelles et monter rapidement des projets complexes faisant appel à des compétences spécialisées, elle souffre néanmoins d'une faiblesse structurelle se traduisant par la disparition des liens 'forts' qui unissaient les délinquants dans des réseaux de confiance les protégeant des erreurs, malveillances et échecs de leurs pairs (Tilly 2005). Ceux-ci ont été remplacés par des arrangements reposant sur des liens 'faibles' qui favorisent la flexibilité organisationnelle mais sont également plus vulnérables aux comportements opportunistes. Dans ce contexte, la confiance que l'on peut accorder à un co-délinquant devient une ressource précieuse qui détermine dans une large mesure la réussite d'un projet criminel. En l'absence d'informations pouvant être tirées d'épisodes antérieurs de sociabilité au démarrage d'un tel projet ou du bouche à oreille local, des mécanismes permettant d'évaluer de manière fiable la réputation d'un partenaire potentiel ou de limiter ses occasions de faire défection ou d'exploiter ses pairs s'avèrent indispensables.

Mécanismes de renforcement de la confiance

Afin de se prémunir contre les 'rippers', les responsables des communautés de cyberdélinquants s'appuient sur quatre stratégies principales leur permettant de minimiser les risques d'échec, d'erreur ou de malveillance et de maintenir ainsi fonctionnels des environnements où les niveaux de confiance entre participants sont structurellement faibles. En premier lieu, les administrateurs de forums de discussion peuvent jouer le rôle de certificateurs de réputation, en évaluant au nom de l'ensemble de la communauté la qualité des produits offerts par certains participants, ainsi que la fiabilité de ces derniers. Cette certification (*verified status* en anglais) est en général offerte contre rémunération et concerne une petite minorité de participants qui réalisent des transactions commerciales fréquentes sur ces forums (Holt et Lampke, 2010 ; Yip et al., 2013). Une alternative pour les groupes de hackers organisés de manière plus informelle ou les forums d'apprentissage et d'échange de procédés innovants est d'exiger la réalisation d'une prouesse technique

vérifiable par les autres membres de la communauté, ce qui permet d'établir la confiance de manière indirecte (et imparfaite) par la validation d'un niveau minimal d'expertise (Lusthaus, 2012).

En deuxième lieu, les administrateurs d'un forum peuvent offrir des services de fidéicommis aux participants en jouant le rôle d'intermédiaires entre les deux parties à une transaction, ne libérant les fonds de l'acheteur que lorsque les obligations du vendeur ont été remplies à la satisfaction des deux protagonistes (Holt et Lampke, 2010 ; Yip et al., 2013 ; Holt et al., 2015). En troisième lieu, la confiance peut être encouragée de manière indirecte par l'existence de mécanismes semi-formels de résolution des conflits offrant à des participants insatisfaits la possibilité d'obtenir réparation de la part des administrateurs du forum. Une plainte est alors déposée devant un arbitre qui évalue les éléments présentés par les deux parties à la dispute (messages privés et journaux des conversations), et qui rend une décision auxquelles doivent se plier toutes les parties (comme la restitution des fonds, la suspension d'un compte utilisateur ou le bannissement pur et simple du forum). Bien entendu, la nature contraignante est relative, puisque la partie fautive peut abandonner son profil et revenir sur le forum sous une nouvelle identité sans grande difficulté (Lusthaus, 2012 ; Holt et al., 2015).

Finalement, les administrateurs peuvent adopter des systèmes automatisés de réputation inspirés des mécanismes d'évaluation des transactions en vigueur sur les sites marchands tels que eBay, Amazon ou TripAdvisor. Ces outils permettent d'agréger à grande échelle les expériences positives ou négatives accumulées par les acteurs d'un marché qui sont ainsi en mesure d'explorer de manière relativement transparente les comportements passés de partenaires potentiels. Cela augmente la qualité et la quantité d'informations dont ils disposent pour anticiper la propension de ces derniers à respecter leurs engagements, ou au contraire à les renier. Pour être efficaces, ces systèmes doivent rendre disponibles des informations d'une qualité suffisante pour permettre d'évaluer de manière consistante les vendeurs ou les acheteurs potentiels, encourager la participation régulière de l'ensemble des acteurs d'un marché à la divulgation systématique de ces informations, et dissuader les acteurs malintentionnés de prendre part aux transactions (Resnick et al., 2000). En rééquilibrant l'asymétrie de l'information qui caractérise les échanges entre inconnus, les plateformes de commerce en ligne ont su exploiter les systèmes automatisés de réputation afin de renforcer l'intégrité des échanges et rassurer ainsi leurs clients potentiels. Mell (2012) s'appuie sur la théorie des jeux pour formuler l'hypothèse que les systèmes de réputation peuvent procurer les mêmes avantages aux marchés, en dissipant la méfiance chronique qui caractérise les interactions entre participants anonymes pratiquant avec brio l'art de la duplicité.

Mais cette hypothèse ne fait malheureusement pas l'objet d'une validation empirique, et les débats sur la place que la confiance occupe dans les relations entre cyberdélinquants ou encore les mécanismes par lesquels cette confiance s'exprime, se renforce ou au contraire se dilue restent de nature très théorique. Il est toutefois possible de procéder à des analyses plus systématiques, comme on le verra dans les deux études présentées dans cet article. La première porte sur un réseau de dix pirates informatiques arrêtés au Québec en 2008, et sur les communications privées échangées entre les membres de ce réseau au cours des

deux années ayant précédé leur interpellation, alors que la seconde aborde la question de la confiance à travers l'analyse des scores de réputation attribués et obtenus par les membres du plus important forum de discussion en ligne consacré au piratage informatique, et plus particulièrement à la performance des pirates spécialisés dans la création de botnets. On verra à travers ces deux analyses que la question de la confiance constitue pour les hackers un dilemme quotidien qui mobilise une énergie considérable et érode de manière significative leur performance criminelle.

LA CONFIANCE COMME INSTRUMENT DE MUTUALISATION DES COMPÉTENCES: UN CIMENT FRIABLE

En février 2008, la police provinciale du Québec procéda à l'arrestation de 17 suspects dans le cadre d'une opération visant à démanteler un réseau de pirates informatiques contrôlant des *botnets* totalisant plus de 630 000 ordinateurs localisés dans 120 pays (Dupont, 2013). De manière simplifiée, un *botnet* est un ensemble de machines infectées par un logiciel malveillant à l'insu de leurs propriétaires et contrôlées de manière centralisée par un *botmaster*. Ces armées de 'zombies' informatiques sont utilisées afin de lancer des attaques par déni de service, de mener des fraudes massives aux clics publicitaires, des opérations de fraude bancaire, ou encore des campagnes de *spam* et de *phishing*. Les *botnets* les plus performants peuvent contrôler plusieurs millions de machines et génèrent des profits considérables pouvant dans les cas les plus extrêmes dépasser trois millions de dollars par an (McCoy et al., 2012). Les hackers interpellés dans le cadre de cette affaire opéraient à un niveau plus modeste, même s'ils réussirent à se procurer plusieurs milliers de numéros de cartes de crédit et de mots de passes dérobés sur les ordinateurs de leurs victimes. Dix d'entre eux furent formellement accusés et tous plaidèrent coupable, se voyant condamnés à des peines de détention à domicile de 15 à 18 mois et à des travaux communautaires. Seul le 'leader' du groupe reçut une peine de prison ferme de deux ans accompagnée d'une période de probation de trois ans, ce qui constitue certainement l'une des condamnations les plus sévères en la matière dans l'histoire pénale canadienne. Avec l'autorisation de l'unité d'enquête impliquée dans cette arrestation, et une fois toutes les procédures judiciaires menées à terme, il nous fut possible d'accéder au contenu des disques durs des ordinateurs saisis chez les dix pirates condamnés. Afin de faciliter l'analyse d'une telle quantité de données et de limiter les intrusions dans la vie privée des personnes étudiées, nous nous sommes concentré sur les conversations privées entre les dix hackers de ce réseau menées via le protocole de messagerie synchrone IRC (*Internet Relay Chat*), qui constitue notamment un outil privilégié de communication dans le monde des cyberdélinquants (Franklin et al., 2007). Au total, 202 fichiers contenant près d'un quart de million de mots furent extraits des disques durs, puis codés à l'aide du logiciel d'analyse qualitative QDA Miner. Les données ainsi structurées ont également été analysées avec le logiciel d'analyse des réseaux sociaux UCINET (Borgatti et al., 2002).

Distribution et mise en réseau des compétences

Les dix pirates incriminés dans cette affaire présentent un profil sociodémographique assez similaire : ce réseau était exclusivement composé de jeunes hommes dont l'âge moyen était de 20,4 ans au moment des faits (amplitude : 17-25 ans), et dont la moitié avait déjà été en

contact avec le système pénal pour des affaires mineures de trafic de stupéfiants, de vol ou de voies de faits. La consommation de drogues (principalement du cannabis) constituait une pratique régulière pour la moitié de l'échantillon. Le statut professionnel des personnes interpellées ne correspond pas à l'image du pirate reconverti dans la sécurité (Auray et Kaminsky, 2006), puisque seulement un des pirates disposait d'un emploi stable dans le secteur informatique, quatre autres occupant des emplois manuels précaires sur une ferme, dans l'industrie forestière, ou encore manufacturière. Des cinq autres pirates, un était sans emploi et bénéficiait de l'aide sociale, deux suivaient des études en informatique, alors que le statut des deux derniers n'a pu être établi avec certitude. Le stéréotype du pirate comme 'geek' explorant de manière indépendante les facettes cachées de technologies émergentes cède ici en partie la place à des individus en voie de marginalisation sociale au sens le plus classique du terme, reproduisant parfois des schémas familiaux déjà enracinés dans la délinquance (trois des pirates avaient grandi dans un contexte familial où l'un ou les deux parents disposaient d'un casier criminel pour des faits de violence aussi graves que des tentatives d'homicides), et trouvant dans les activités de piratage un échappatoire à un présent relativement morne.

Les premiers actes de piratage déclarés par les dix hackers lors de leurs entrevues avec les enquêteurs ont débuté pour les plus jeunes autour de huit ans, et la majorité s'est intéressée à la création et à l'utilisation de botnets au début de l'adolescence, laissant supposer des coûts d'entrée relativement bas pour ce type d'activités. Toutefois, une analyse plus approfondie du contenu des discussions entre les membres de ce réseau, et notamment des obstacles auxquels ils ont été confrontés au cours des deux années ayant précédé leur arrestation laissent entrevoir une réalité légèrement plus complexe où la réussite et la performance criminelle dépendent de la convergence de trois formes de compétences disponibles en quantité limitée. Il s'agit des compétences techniques, sociales et de rentabilisation. Inspirée des travaux de Copes et Vieraitis (2008), cette typologie rudimentaire nous permet de distinguer les expertises complémentaires indispensables à la réussite des projets criminels des cyberdélinquants.

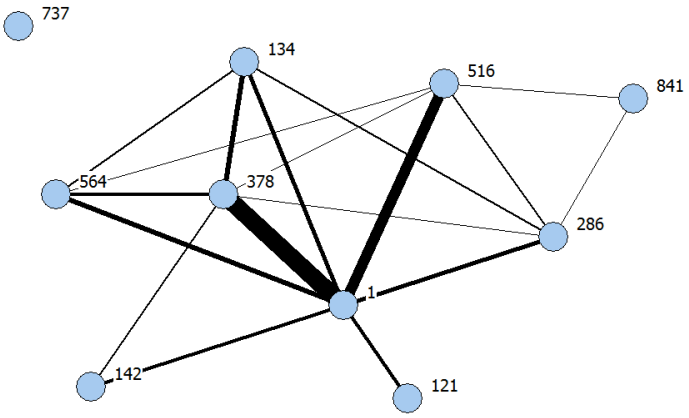
Comme son nom l'indique, la compétence technique reflète la capacité des pirates à programmer, déployer et maintenir en ligne de manière stable des botnets qui échapperont à la vigilance des mécanismes de sécurité tels que les logiciels anti-virus ou les solutions de gestion des évènements et des informations de sécurité (SIEM) qui protègent les systèmes informatiques. Neuf des dix pirates arrêtés utilisaient des souches de logiciels malveillants librement accessibles sur Internet depuis le début des années 2000, et manifestaient donc des aptitudes techniques limitées au codage ou à la personnalisation d'applications plus innovantes. Un seul des dix pirates (#378) disposait d'aptitudes techniques suffisantes à la modification de ces logiciels, et semblait également particulièrement talentueux dans la propagation de son code malveillant. Il contrôlait au moment de son arrestation la moitié des bots du réseau et jouait le rôle de mentor technique pour certains des membres du groupe, partageant parfois certains éléments de code et des ressources. Mais si les enquêteurs lui attribuent plus de 150 attaques par déni de service, il ne parvint jamais à rentabiliser les quelques centaines de milliers d'ordinateurs infectés sous son contrôle. Cette absence totale d'expertise de conversion des données volées en ressources financières découle de la difficulté pour les pirates de maîtriser les systèmes et les

procédures organisationnelles complexes que les institutions financières mettent en œuvre afin de protéger les comptes de leurs clients, mais aussi de la prolifération des 'rippers', qui augmentent considérablement les risques et l'incertitude pour ceux qui voudraient sous-traiter ces tâches à des partenaires dans lesquels ils ne peuvent avoir qu'une confiance superficielle. Même #378, qui n'a aucune difficulté à coder des bots de puissance modérée semble d'après les transcriptions de ses discussions avec des partenaires potentiels mal informé des mécanismes les plus communs de fraude bancaire. Dans certaines des conversations avec des partenaires potentiels intéressés par ses compétences techniques, il fait preuve d'une grande méfiance et ne semble toujours réticent à conclure une entente satisfaisante. S'il lui manque des compétences de rentabilisation que d'autres pourraient lui offrir, il ne dispose pas non plus des compétences sociales lui permettant de nouer et de maintenir des relations productives avec des co-délinquants potentiels. Par contraste, un autre membre du réseau (#1) fait preuve de bien meilleures aptitudes à la manipulation des situations sociales – même si dans ce cas, ces compétences ne semblent pas avoir amélioré de manière significative son accès à des complices capables de rentabiliser les données volées. Ces compétences sociales incluent, sans y être limitées, la disposition de certains individus à accorder et à susciter la confiance de leurs pairs. Dans ce contexte, les compétences sociales permettent la mise en relation et la stabilisation des compétences techniques et des compétences de rentabilisation indispensables à la réussite d'un projet criminel.

L 'instabilité des relations de coopération : les liens forts comme outil de gestion du soupçon

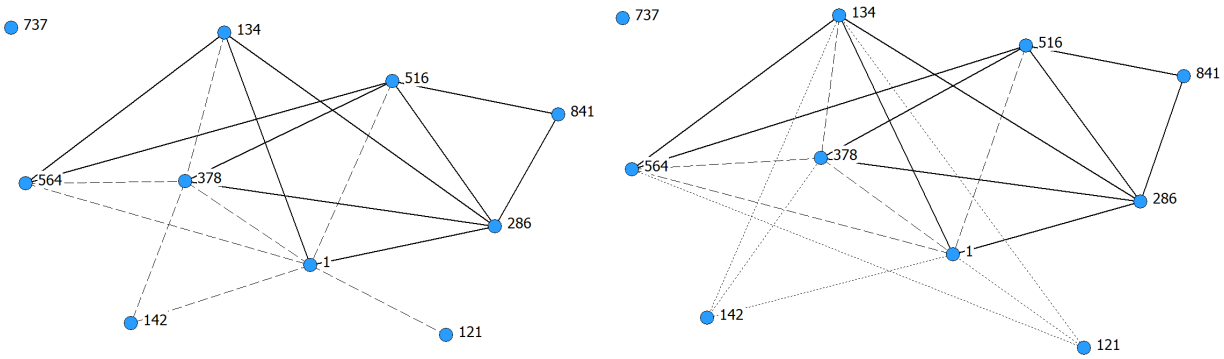
Il est possible de mesurer la présence de ces compétences sociales dans un réseau criminel et d'en suivre l'évolution à travers la méthode de l'analyse des réseaux sociaux. Dans cette étude, nous avons ainsi codé chaque interaction entre les membres du réseau durant deux périodes successives (année 1 et année 2) ayant précédé l'arrestation, afin de comprendre comment ces compétences sociales se distribuent entre les pirates et comment elles évoluent dans le temps. La figure 1 représente ainsi la carte du réseau, l'épaisseur des liens reflétant leur intensité calculée selon le nombre de discussions entre chaque paire de pirates pendant les deux années pour lesquelles les données sont disponibles. Les rôles centraux que jouent #378 et #1 en tant qu'éléments structurants du réseau apparaissent de manière évidente. Cette simple visualisation n'est toutefois pas suffisante pour mesurer le capital social dont disposent ces dix acteurs, et les outils statistiques du logiciel UCINET nous permettent d'établir que #1 est responsable de 37,6% de l'ensemble des échanges entre les membres du réseau, alors que la part de #378 représente seulement 22,1% des interactions. Qui plus est, #516 surpasse légèrement #378 pour la centralité d'intermédiarité, qui mesure le contrôle qu'exerce un acteur sur les relations entre autres paires d'acteurs, et par extension sa capacité à mettre des inconnus en contact (Lemieux, 2003).

Figure 1. Intensité des liens entre les membres du réseau de pirates (années 1 et 2 combinées)



Les mesures d'analyse des réseaux sociaux confirment l'intuition du rôle primordial que joue #1 pour la cohésion de ce groupe, ainsi que la nature privilégiée des liens qui l'unissent à #378, le détenteur de l'expertise technique au sein de ce groupe. Toutefois, l'introduction de la confiance comme qualificatif à la qualité des liens permet de dégager une image quelque peu différente. La figure 2 représente les liens entre chaque paire de pirates à deux moments de la vie du réseau (année 1 et 2) selon trois modalités de la confiance : la confiance forte ou résiliente (capable de résister à la défaillance de l'une des parties), la confiance faible ou conditionnelle (réévaluée à intervalles réguliers), et l'hostilité (exprimant explicitement l'absence de confiance). Si les liens de confiance forte se maintiennent peu ou prou d'une année à l'autre (de 56% à 48% des interactions), les liens caractérisés par la confiance faible se dégradent assez rapidement (de 44% à 24%) pour céder la place à des liens d'hostilité qui représentent 28% des interactions à la fin de la seconde année.

Figure 2. Évolution des liens de confiance et d'hostilité au sein du réseau (année 1 à gauche et année 2 à droite)



Légende: —— Confiance forte ; ---- Confiance faible ; ..... Hostilité

Autrement dit, l'intensité des liens observés à la figure 1 entre #378 et #1 n'exprime pas nécessairement une confiance privilégiée entre les deux acteurs clés du réseau, mais reflète au contraire l'existence d'une méfiance latente qui est en partie alimentée par la dégradation rapide et spontanée des relations dans leur environnement immédiat. L'intensité des liens entre #1 et #378 représente ainsi un mécanisme de contrôle réciproque indiquant une alliance semi-fonctionnelle plutôt qu'une collaboration prometteuse basée sur une confiance indéfectible. Nous ne disposons pas de suffisamment d'espace pour détailler les raisons de cette rapide détérioration, qui doit tout autant à l'immaturité des membres de ce réseau qu'au décalage probablement trop grand entre leurs compétences techniques respectives. Il est néanmoins important de rappeler que la nature éphémère des liens de confiance fragile caractérisant les interactions de ce réseau prend place dans un contexte relativement favorable où la police n'avait pas encore procédé à la moindre intervention et où la pression extérieure était donc minimale (Morselli, 2009). Si la taille réduite de ce réseau n'autorise évidemment aucune généralisation, des enquêtes journalistiques approfondies portant sur des groupes de pirates capables de générer des revenus criminels conséquents ou de lancer des attaques plus sophistiquées ont également fait apparaître des schémas semblables et relativement fréquents de méfiance et d'hostilité culminant en trahisons spectaculaires (Poulsen, 2011 ; Coleman, 2014 ; Krebs, 2014).

L'ILLUSION DE LA CONFIANCE DE MASSE: EFFICACITÉ RELATIVE DES SYSTÈMES AUTOMATISÉS DE RÉPUTATION EN CONTEXTE DÉLINQUANT

L'étude de cas du réseau présenté dans la section précédente ou encore les enquêtes journalistiques mentionnées plus haut concernent des groupes de taille limitée qui comprennent rarement plus de quelques dizaines d'individus capables de développer un certain niveau de familiarité, même si cette dernière peut rapidement prendre une forme antagonique. Toutefois, les forums de discussion consacrés au piratage et les marchés clandestins où s'échangent logiciels malveillants et informations volées composent des communautés beaucoup plus vastes qui réunissent des milliers d'individus à la recherche de partenaires potentiels. Il leur est donc nécessaire de mettre en œuvre des mécanismes favorisant la cristallisation rapide d'une confiance minimale entre inconnus à la fiabilité douteuse, à l'instar des stratégies présentées dans la première section. Nous examinerons donc ici plus particulièrement les systèmes automatisés de réputation, et plus spécifiquement celui utilisé par le plus important forum de discussion de piratage informatique actuellement en activité. Nous tenterons de répondre à deux questions : comment se distribue la confiance au sein des communautés de délinquants en ligne? Et les systèmes automatisés de réputation inspirés des services d'e-commerce sont-ils aussi efficaces pour assurer le bon fonctionnement des marchés criminels?

Nous mobilisons pour cela un corpus de données recueilli sur ce forum pendant 27 mois, d'octobre 2009 à décembre 2011, et contenant 285 690 scores de réputation attribués par 8 824 membres à 9 127 de leurs pairs ayant démontré un intérêt avéré pour les botnets. Au moment de la collecte de données, le forum comprenait environ 250 000 membres, alors qu'à la fin de l'année 2015, il annonce plus de 2,7 millions d'utilisateurs enregistrés. Ces chiffres peuvent sembler à la fois importants pour un forum de hackers, et incohérents au regard du décalage entre le nombre de membres proclamés et de contributeurs avérés au

système de réputation, mais la majorité des participants sont de simples observateurs qui ne prennent jamais part aux discussions et qui sont généralement qualifiés de 'lurkers' ou voyeurs par les membres plus actifs (Motoyama et al., 2011 ; Afroz et al., 2013).

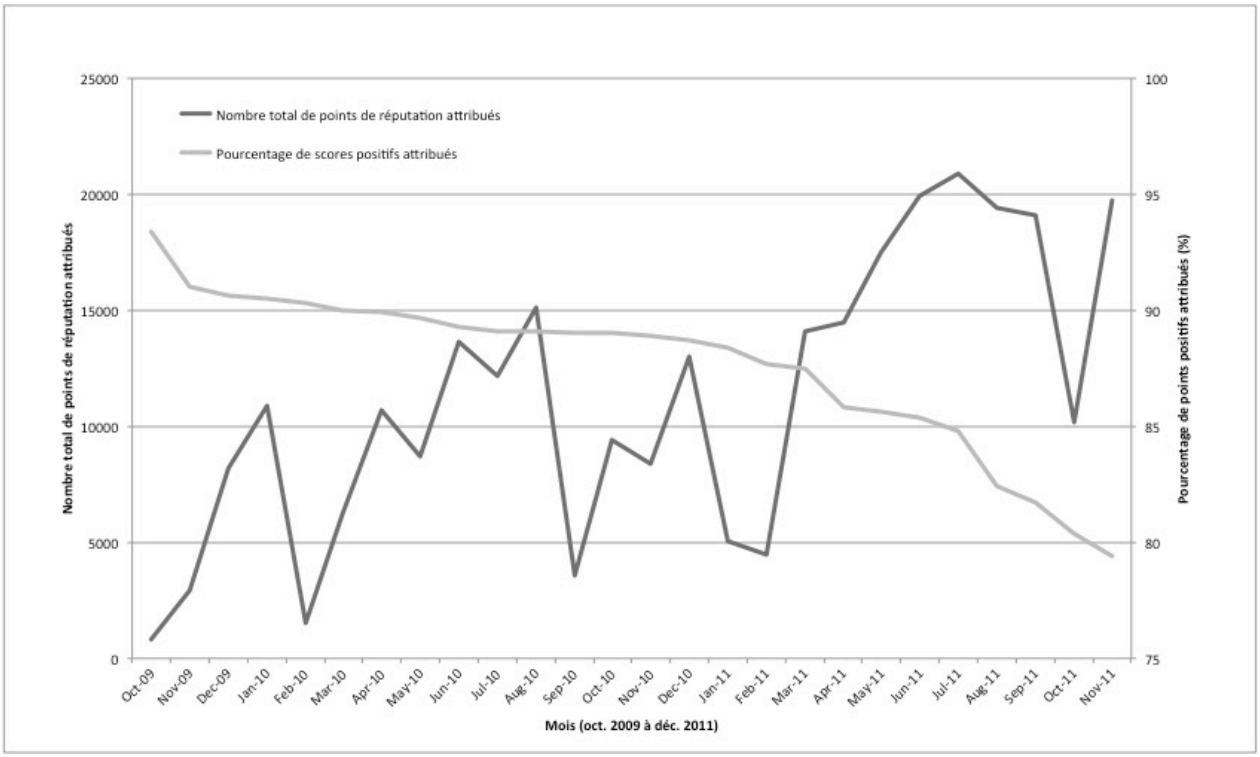
Comme pour la plupart des autres forums de piratage, les sujets abordés par les contributeurs sont d'une extrême variété et rien ne permet de penser que l'ensemble d'entre eux se livrent à des activités punies par la loi. Un très grand nombre d'activités de piratage informatique peuvent en effet parfaitement être menées de manière éthique et bien des membres de ces forums sont plus intéressés par la sécurité que par la cybercriminalité. Nous avons donc limité nos analyses au sous-forum dédié aux botnets, qui par sa nature même implique l'intrusion dans le système informatique de tierces parties, une activité impossible à mener sans violer de lois.

Croissance de la communauté et déclin de la confiance

Le système automatisé fonctionne de manière relativement classique : chaque membre ayant démontré une compréhension élémentaire des règles et des normes de comportement sur le forum peut attribuer à un autre membre un score de réputation positif, neutre ou négatif de valeur variable (1, 3, 5 ou 10 points, en fonction de sa position hiérarchique) accompagné d'un commentaire explicatif d'une ligne. L'accumulation des évaluations reçues par chaque membre donne ensuite lieu au calcul d'un score global. Ainsi, le *botmaster* possédant le score le plus élevé avait accumulé 2 330 points de réputation positive, alors que le plus mal noté semblait unanimement honni avec –708 points de réputation négative.

De prime abord, les interactions dans ce sous-forum semblent extrêmement satisfaisantes, puisque 86,3% de l'ensemble des évaluations individuelles s'avèrent positives et que 77,9% des personnes évaluées disposent d'un score global positif (pour 17,4% de scores globaux négatifs) pour la durée de référence. De tels niveaux de satisfaction correspondent à la tendance observée sur d'autres marchés licites et illicites en ligne ayant déployé des systèmes équivalents, où les taux de scores positifs dépassent souvent 95% (Dellarocas, 2003 ; Christin, 2013). Cependant, l'examen des données sur une base mensuelle nuance quelque peu cette impression initiale.

Figure 1. Évolution temporelle du nombre de participants et des scores de réputation positifs attribués



R (-0.73**). P<0,01**

En effet, à mesure que le nombre de participants, et par extension le nombre d'évaluations échangées par ces derniers, augmente, le pourcentage des scores de réputation positifs régresse de manière inexorable. Cette relation statistiquement significative voit diminuer le taux d'évaluations positives de 18,7% en 27 mois, passant de 99,1% à 80,4% des scores attribués. Autrement dit, même si les usagers demeurent très largement satisfaits de leurs interactions, le système de réputation n'est pas suffisant pour stabiliser la confiance, et à mesure que le nombre de participants et de collaborations augmente, leur qualité semble s'éroder de manière quasi-mécanique. Il semble donc que les communautés en ligne dédiées aux activités illicites éprouvent beaucoup plus de difficultés que les entreprises de commerce en ligne à exploiter le potentiel de renforcement à grande échelle de la confiance des systèmes automatisés de réputation. À cette fragilité temporelle de la confiance s'ajoute une seconde déficience structurelle qui est intimement liée au statut que les divers participants occupent dans la hiérarchie de cette communauté.

Méfiance et positionnement hiérarchique

Loin de l'idéal égalitariste qui est souvent présenté comme le mode organisationnel par défaut des communautés de hackers, le monde du piratage informatique est par essence élitiste, et comme dans la majorité des forums de discussion, on retrouve dans celui qui est étudié ici une hiérarchie formelle conférant aux participants des privilèges plus ou moins étendus concernant la capacité d'interagir avec d'autres membres, de les évaluer, ou encore de suspendre ou de révoquer leur profil. Au moment de la collecte des données, cette hiérarchie comprenait cinq classes de membres. Les participants « 3pic » (terme abrégé pour *epic*) qui n'apparaissent pas dans nos statistiques sont de nouveaux venus dans la

communauté qui ne disposent que d'un accès limité aux fonctions du forum et ne peuvent pas évaluer leurs pairs. Les membres « L33t » (*elite*) se situent juste au dessus dans la hiérarchie et peuvent attribuer des scores de +1 ou -1, avant de progresser pour les meilleurs et sur invitation seulement vers le statut de « Ub3r » (*uber)*, qui confère le droit d'attribuer des scores pouvant aller de -3 à +3 et avec une limite de cinq évaluations par jour. Finalement, un petit groupe d'auxiliaires et d'administrateurs gèrent le forum et peuvent respectivement attribuer des scores de -5/+5 et -10/+10, ce qui confère à chacune de leurs évaluations un poids disproportionné. Le tableau 1 présente une distribution des scores de réputation attribués par les membres de cette communauté selon leur statut hiérarchique.

Tableau 1. Distribution des évaluations selon le statut

	L33t	Ub3r	Auxiliaire	Administrateur
% du nombre total des membres*	63.15	36.56	0.25	0.05
% du nombre total d'évaluations effectuées	27.26	71.76	0.79	0.18
Nombre moyen d'évaluations effectuées par individu	13.93	63.32	102.86	131.00
% d'évaluations positives	86.41	86.41	80.20	33.78
% d'évaluations négatives	0.00	11.96	17.10	61.64
% d'évaluations neutres	13.59	1.63	2.70	4.58

Note : * seuls les membres ayant la capacité d'évaluer leurs pairs sont comptabilisés.

En termes de représentativité de chaque catégorie de membres dans le volume global des scores de réputation attribués, les membres les plus récents (les L33t) sont clairement sous-représentés, alors que les Ub3r, qui ne constituent qu'un peu plus du tiers de cette communauté, sont néanmoins responsables de 71,76% des évaluations. Cette tendance reflète l'augmentation constante du nombre moyen d'évaluations réalisées par les membres selon leur position hiérarchique, les quelques administrateurs du forum étant ainsi les auteurs de 131 évaluations pendant la période de référence, soit dix fois plus que les L33t. L'utilisation différentielle du système automatisé de réputation n'est pas seulement d'ordre quantitatif, mais implique aussi d'importantes variations qualitatives. En effet, plus le statut d'un participant est élevé et plus la proportion de scores positifs qu'il attribue se réduit, pour aboutir dans le cas des administrateurs à une véritable inversion du ratio, les évaluations négatives représentant plus de la majorité (61,64%) des scores attribués. On note également l'absence d'évaluations négatives provenant des contributeurs novices (le L33t), en dépit du nombre considérable d'évènements concernés (77 611 évaluations disponibles pour cette catégorie de membres). Cette propension à la bienveillance dans l'évaluation du comportement des pairs s'explique probablement de manière instrumentale par le souci des L33t—et dans une moindre mesure des Ub3r—de gravir les échelons hiérarchiques de cette communauté, en s'appuyant notamment sur la réciprocité des évaluation positives et en évitant à tout prix l'attribution de scores négatifs pouvant susciter en retour des évaluations de rétorsion ternissant leur propre image et limitant ou retardant leurs chances d'ascension vers un statut plus élevé. Les administrateurs et leurs auxiliaires, qui opèrent au sommet de cette hiérarchie, ne sont pour leur part plus soumis à cette pression collective et se trouvent également investis d'un mandat de protection de la communauté qui les force à dispenser leurs évaluations de manière beaucoup plus

coercitive afin de sanctionner les pirates qui abusent de la confiance de leurs pairs. Ce ratio inversé et l'énergie considérable que les administrateurs investissent dans l'étiquetage public des membres à faible valeur ajoutée, de ceux dont l'attitude laisse à désirer, et des 'rippers', semble suggérer que le système automatisé de réputation utilisé par ce forum est incapable d'auto-réguler à lui seul les niveaux de confiance entre participants. Une intervention complémentaire par le haut est requise afin de maintenir la cohésion des échanges.

Le « Lulz » comme transgression à l'instrumentalisation de la confiance

Ce résultat pourrait paraître contre-intuitif pour une communauté aussi adepte du recours aux outils technologiques pour fluidifier les relations sociales et les rendre possibles à très grande échelle. Il faut alors chercher dans certains traits culturels transgressifs propres aux communautés de hackers l'explication de cette apparente contradiction. L'analyse qualitative de 25 000 commentaires sélectionnés aléatoirement dans notre échantillon nous permet en effet de mieux comprendre quels comportements et quelles compétences contribuent à la formation d'une réputation enviable et favorisent la confiance. Cinq raisons principales motivent l'attribution de scores de réputation positifs ou négatifs, et le tableau 2 présente la distribution de ces facteurs de confiance. Ces cinq précurseurs de la confiance ou au contraire de la défiance sont : 1) les relations d'affaires passées, qui correspondent aux compétences de valorisation mentionnées dans la section précédente et à la qualité des prestations marchandes offertes; 2) les contributions générales à la communauté, qui prennent souvent la forme de tutoriels ou de logiciels offerts à tous, et reflètent la valeur ajoutée que chacun est en mesure d'apporter au groupe par un partage altruiste des connaissances; 3) le comportement spécifique à l'égard de l'évaluateur, qui témoigne généralement de l'attitude adoptée dans les échanges bilatéraux et correspond aux compétences sociales de la section précédente; 4) les compétences techniques telles qu'établies dans un contexte de collaboration concrète; 5) des commentaires sarcastiques, humoristiques ou qui semblent dénués de contexte; 6) des commentaires illisibles, soit parce qu'ils sont écrits en caractères arabes, chinois ou cyrilliques, soit parce qu'ils comprennent une suite incohérente de caractères.

Tableau 2. Distribution des motifs d'évaluations positives, neutres et négatives

Catégories	Évaluations positives (%)	Évaluations neutres (%)	Évaluations négatives (%)
Relations d'affaires passées	9.38	13.00	11.72
Contribution générale à la communauté	13.41	28.00	22.95
Comportement spécifique à l'égard de l'évaluateur	24.58	42.89	20.57
Sarcasmes, humour ou hors contexte	29.65	10.77	36.74
Illisible	2.75	2.50	4.41
Total	100.00	100.00	100.00

Comme on le voit dans le tableau 2, le premier motif d'attribution des évaluations positives est de nature sarcastique ou humoristique, suivi de près par un comportement ou une

attitude spécifique à l'égard de l'évaluateur, alors que les dimensions plus techniques et marchandes se classent respectivement en troisième et cinquième position. Pour les évaluations négatives, le sarcasme sert également fréquemment de dispositif justificatif, alors que le déficit de compétences techniques semble être un facteur marginal d'insatisfaction. Le rôle prédominant joué par le sarcasme et l'humour, par nature ambigus et extrêmement difficiles à contextualiser vont à l'encontre des objectifs d'une évaluation transparente et efficace de la confiance que l'on est en mesure d'accorder à un inconnu.

Cet usage intensif d'un humour absurde entrelacé de références grotesques et outrancières en lieu et place de commentaires rationnels censés aider la prise de décision illustre parfaitement la manière dont les valeurs de subversion et d'indépendance du piratage informatique s'opposent par nature à l'implantation d'outils inspirés par une logique trop utilitariste. Gabriella Coleman (2014) utilise le concept de 'lulz', difficilement traduisible en français, pour définir cette disposition des membres du mouvement *Anonymous*, mais aussi de nombreux hackers et d'autres communautés marginales à valoriser « le rire aux dépends d'autrui », quel qu'en soit le prix, dans ce qui pourrait être l'incarnation d'une forme de bouffonnerie numérique. Dans ce forum de pirates, le 'lulz' qui émaille près du tiers des évaluations n'a pas pour principal objet de rendre l'exercice plus ludique. Il vient plutôt vider de sa substance le mécanisme trop bien huilé de mise en chiffre de la réputation des hackers, cherchant ainsi à restaurer l'équilibre compromis d'une culture valorisant une saine dose de chaos et de contestation. Ainsi, la logique du profit doit-elle cohabiter avec une rationalité d'inspiration libertaire rétive à toute forme d'ordre.

CONCLUSION

Les défis techniques et organisationnels auxquels sont confrontés les délinquants en ligne sont systématiquement sous-estimés par de nombreux chercheurs et une presse généraliste reprenant à son compte (et à peu de frais) les innombrables rapports d'entreprises de sécurité informatique qui façonnent depuis deux décennies le mythe d'un super-criminel omnipotent capable de générer sans grand effort des profits quasiment illimités. Si quelques hackers ingénieux ont effectivement su développer des schémas de fraude automatisés extrêmement lucratifs, eux-mêmes n'ont pu échapper au dilemme de la confiance qui afflige tout cyberdélinquant. Dans un environnement technique et financier complexe où les compétences requises pour mener à bien un projet criminel sont rarement détenues par un seul individu, l'identification, le recrutement et la rétention de partenaires fiables mobilise une énergie considérable et génère des coûts de transaction élevés. Ces efforts sont alourdis par un contexte défavorable où l'anonymat qui caractérise les échanges et la facilité avec laquelle une identité fictive peut être créée rend la réputation des co-délinquants disponibles fongible et difficile à garantir avec certitude. Il en résulte une accumulation des incitatifs à la duplicité et une prolifération des 'rippers', qui font peser sur l'ensemble des transactions un nuage toxique de défiance.

À travers l'étude empirique de deux groupes de hackers malveillants de tailles très différentes, on a tenté de montrer l'importance de ces mécanismes et les modalités concrètes selon lesquelles ils se déploient. Les analyses du rôle de la confiance (ou de son absence) dans l'articulation des différentes formes de compétence, de la volatilité des liens

de confiance fragile par rapport aux liens forts, de l'efficacité relative des mécanismes automatisés de substitution et leur incapacité à stabiliser la confiance à des niveaux élevés lorsque le nombre de co-délinquants augmente exponentiellement, des biais de reportabilité induits par une structure hiérarchique favorisant les comportements de réciprocité au détriment d'évaluations libres de toute contrainte, ou encore de la subversion de mécanismes utilitaristes de renforcement de la confiance par un humour transgressif garant des valeurs originelles des communautés de hackers nous permettent de comprendre la complexité des variables à l'œuvre. Elles constituent également autant de nuances apportées à une interprétation trop simplificatrice ou mécaniste des rouages par lesquels la confiance s'établit et se propage au sein des assemblages hommes-machines qui constituent l'essence des réseaux contemporains de délinquance.

De nombreuses études additionnelles restent à mener, notamment sur les marchés clandestins accessibles sur invitation seulement (où la confiance est gérée de manière beaucoup plus personnalisée), les communautés nationales de cyberdélinquants qui opèrent dans un environnement policier et judiciaire permissif (en Russie notamment), ou encore les corrélations pouvant être établies entre réputation, confiance et réussite criminelle (Morselli et al., 2006). Au-delà des questions théoriques, de telles recherches induisent également des efforts importants de collecte de données de première main. Bien que certains fichiers puissent être obtenus de manière opportuniste, au gré des piratages de forums de discussion ou de marchés clandestins par des hackers concurrents, ou via des accès privilégiés consentis par des services de police ou des entreprises de sécurité, des méthodes innovantes (et légales) de capture, d'analyse et de visualisation des données disponibles en ligne doivent également être élaborées, afin qu'une recherche universitaire indépendante puisse contribuer de manière informée aux controverses émergentes en matière de cybercriminalité et de cybersécurité. Il s'agit non seulement de faire entrer la criminologie dans l'ère numérique, mais aussi et surtout de la tirer de l'ornière anecdotique et sensationnaliste dans laquelle certains l'ont enlisée.

RÉFÉRENCES

ABLON L., LIBICKI M., GOLAY A. (2014), *Markets for cybercrime tools and stolen data*, Santa Monica, RAND Corporation.

AFROZ S., GARG V., MCCOY D., GREENSTADT R. (2013), « Honor among thieves: a common's analysis of cybercrime economies », *eCrimes Research Summit*. 16-19 Septembre.

AURAY N., KAMINSKY D. (2006), « Les trajectoires de professionnalisation des hackers : La double vie des professionnels de la sécurité », *Working papers in economics and social sciences*, Paris, Télécom Paris.

BEST J., LUCKENBILL D. (1994), *Organizing deviance*, Englewood Cliffs, Prentice Hall.

BORGATTI S., EVERETT M., FREEMAN L. (2002), *Ucinet for Windows: Software for social network analysis*, Harvard, Analytic Technologies.

BROADHURST R., GRABOSKY P., ALAZAB M., CHON S. (2014), « Organizations and cyber crime : an analysis of the nature of groups engaged in cyber crime », *International Journal of Cyber Criminology*, vol. 8, no. 1, pp. 1-20.

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*, Genève, Association for Computing Machinery.

CLEAR T. (1996), « Backfire : when incarceration increases crime », In *The unintended consequences of incarceration*, New York, Vera Institute of Justice.

COLEMAN G. (2014), *Hacker, hoaxer, whistleblower, spy: the many faces of anonymous*, New York, Verso.

COPES H., VIERAITIS L. (2008), « The risks, rewards and strategies of stealing identities », In M. McNally et G. Newman (dirs.), *Identity theft and opportunity, crime prevention studies*, Monsey, Criminal Justice Press.

DELLAROCAS C. (2003), « The digitization of word-of-mouth: promise and challenges of online feedback mechanisms », *Management Science*, vol. 49, pp. 1407-1424.

DENSLEY J. (2012), « Street gang recruitment : signaling, screening and selection », *Social Problems*, vol. 59, no. 3, pp. 301-321.

DUPONT B. (2013), « Skills and trust : a tour inside the hard drives of computer hackers », in C. Morselli (dir.), *Illicit networks*, Oxford, Routledge.

FRANKLIN J., PAXSON V., PERRIG A., SAVAGE S. (2007), « An inquiry into the nature and cause of the wealth of Internet miscreants », in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, New York, ACM.

GAMBETTA D. (1988), « Mafia: The price of distrust », in D. Gambetta (dir.), *Trust: making and breaking cooperative relations*, New York, Basil Blackwell.

GAMBETTA D. (dir.) (1988), *Trust: making and breaking cooperative relations*, New York, Basil Blackwell.

GLENNY, M. (2012), *Darkmarket : how hackers became the new mafia*, Londres, Random House.

GRABOSKY P. (2013), « Organised crime and the Internet », *The RUSI Journal*, vol. 158, no. 5, pp. 18-25.

HERLEY C., FLORENCIO D. (2010), « Nobody sells gold for the price of silver : Dishonesty, uncertainty and the underground economy », in T. Moore, D. Pym, C. Ioannidis (dir.), *Economics of information security and privacy*, New York, Springer.

HOBBS D. (1995), « Bad business : professional crime in modern Britain », Oxford, Calrendon Press.

HOLT T. (2013), « Exploring the social organization and structure of stolen data markets », *Global Crime*, vol. 14, no. 2-3, pp. 155-174.

HOLT T., LAMPKE E. (2010), « Exploring stolen data markets online: Products and market forces », *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, vol. 23, no. 1, pp. 33-50.

HOLT T., SMIRNOVA O., TING CHUA Y., COPES H. (2015), « Examining the risk reduction strategies of actors in online criminal markets », *Global Crime*, DOI : 10.1080/17440572.2015.1013211.

KLEEMANS E., VAN DE BUNT H. (1999), « The social embeddedness of organized crime », *Transnational Organized Crime*, vol. 5, no. 1, pp. 19-36.

KREBS B. (2014), *Spam nation: the inside story of organized cybercrime – from global epidemic to your front door*, Naperville, Sourcebooks.

LAVORGNA A. (2015), « The social organization of pet trafficking in cyberspace », *European Journal of Crime Policy and Research*, vol. 21, no. 3, pp. 353-370.

LEMIEUX V. (2003), *Les réseaux criminels*, Ottawa, Gendarmerie Royale du Canada.

LUHMANN N. (2006), *La confiance : Un mécanisme de réduction de la complexité sociale*, Paris, Economica.

LUSTHAUS J. (2012), « Trust in the world of cybercrime », *Global Crime*, vol. 13, no. 2, pp. 71-94.

LUSTHAUS J. (2013), « How organise dis organised cybercrime ?», *Global Crime*, vol. 14, no.1, pp. 52-60.

MCCARTHY B., HAGAN J., COHEN L. (1998), « Uncertainty, cooperation and crime : Understanding the decision to offend », *Social Forces*, vol. 77, no. 1, pp. 155-184.

MCCOY D., PITSILLIDIS A., JORDAN G., WEAVER N., KREIBICH C., KREBS B., VOELKER G., SAVAGE S., LEVCHENKO K. (2012), « PharmaLeaks: understanding the business of online pharmaceutical affiliate programs », *21st USENIX Security Symposium*, Bellevue, USENIX.

MCGUIRE M. (2007), *Hypercrime : the new geometry of harm*, Abingdon, Routledge.

MCINTOSH M. (1975), *The organisation of crime*, Londres, Macmillan Press.

MELL A. (2012), « Reputation in the market for stolen data », *Discussion Paper no. 611*, Oxford, Département d'économie de l'Université d'Oxford.

MORSELLI C. (2009), *Inside criminal networks*, New York, Springer.

MORSELLI C., TREMBLAY P., MCCARTHY B. (2006), « Mentors and criminal achievement », *Criminology*, vol. 44, no. 1, pp. 17-43.

MOTOYAMA M., MCCOY D., LEVCHENKO K., SAVAGE S., VOELKER G. (2011), « An analysis of underground forums », *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, New York, ACM.

NEWMAN G., CLARKE R. (2003), *Superhighway robbery: preventing e-commerce crime*, Cullompton, Willan.

POULSEN K. (2008), « 56 arrested in DarkMarket sting says FBI », *Wired*, http://www.wired.com/2008/10/56-arrested-in/.

POULSEN K. (2011), *Kingpin: how one hacker took over the billion-dollar cybercrime underground*, New York, Crown Publishers.

RESNICK P., ZECKHAUSER R., FRIEDMAN E., KUWABARA K. (2000), « Reputation systems », *Communications of the ACM*, vol. 43, no. 12, pp. 45-48.

SHOVER N. (1973), « Structures and careers in burglary », *Journal of Criminal Law and Criminology*, vol. 63, no. 4, pp. 540-549.

TILLY C. (2005), *Trust and rule*, Cambridge, Cambridge University Press.

VON LAMPE K., JOHANSEN P. O. (2004), « Organized crime and trust : on the conceptualization and empirical relevance of trust in the context of criminal networks », *Global Crime*, vol. 6, no. 2, pp. 159-184.

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

WALL D. (2010), « Criminalising cyberspace : the rise of the Internet as a 'crime problem' », in Y. Jewkes, M. Yar (dir.), *Handbook of Internet crime*, Londres, Routledge.

YIP M., WEBBER C., SHADBOLT N. (2013), « Trust among cybercrimnals? Carding forums, uncertainty and implications for policing », *Policing & Society*, vol. 23, no. 4, pp. 516-539.