Des effets perturbateurs de la technologie sur la criminologie

par **Benoît DUPONT*** (1)

Le futur est déjà là - il est juste inégalement distribué
William Gibson

Résumé
Les effets perturbateurs de la technologie, loin d'être cantonnés aux acteurs industriels et gouvernementaux, dont le quotidien se trouve bouleversé par une succession frénétique d'innovations, s'appliquent évidemment au monde de la recherche scientifique, en voie d'être profondément reconfiguré par la capacité différentielle des champs disciplinaires à prendre acte de ces changements et à s'approprier les nouvelles thématiques qui en découlent, ainsi que les nouveaux outils théoriques et méthodologiques qu'elles induisent. Dans un tel contexte, cet article vise donc à approfondir trois questions figurant au cœur du potentiel de transformation qui s'offre à notre discipline. La première question relève de la mise en chiffres des risques numériques et de l'intégration de ces statistiques à une mesure réellement globale de la délinquance. Elle s'interroge notamment sur la fiabilité des instruments de mesure traditionnels et sur les métriques requises pour mieux intervenir contre la cybercriminalité. La seconde question est d'ordre méthodologique et s'intéresse à l'intégration des méthodes qualitatives aux approches statistiques, dans une démarche mixte productrice de résultats prometteurs pour appréhender la complexité des phénomènes étudiés. Finalement, la troisième question traite des mécanismes de régulation, et propose de nous débarrasser des œillères théoriques qui nous empêchent de prendre toute la mesure du pluralisme des modes de gouvernance se mettant en place avec plus ou moins de spontanéité et de coordination pour prévenir et limiter les préjudices causés par la délinquance en ligne.

Mots-clés: cybercriminalité, risques numériques, statistiques criminelles, organisation sociale de la délinquance, pirates informatiques, méthodes mixtes, gouvernance de la sécurité, réseaux de sécurité.

Summary
The disruptive effects of technology, far from being limited to transforming private and governmental organizations through a barrage of innovations, also apply to research institutions, which are being radically reconfigured by the differential capacity of various disciplinary fields to embrace the new themes that have emerged in its wake, as well as the theoretical and methodological tools that are needed to study them. In that context, this article aims to examine three issues that are at the core of the transformations that our discipline will most likely experience. The first issue concerns the measurements of digital risks and the integration of those statistics to existing crime indicators. We will discuss the reliability of established measurement instruments and the missing metrics that are

* Centre international de criminologie comparée, Université de Montréal
Chaire de recherche du Canada en Cybersécurité

needed to better intervene against cybercrime. The second issue is of a methodological nature and focuses on a better integration of qualitative and quantitative approaches, to promote a mixed method strategy better suited to capture the complexity of the problem at hand. Finally, the third issue deals with changing regulatory mechanisms, and suggests that we discard the theoretical blinkers that prevent us from acknowledging the full extent of the plural modes of governance that are being implemented to prevent and respond to online harms.

Keywords: cybercrime, digital risks, crime statistics, social organization of delinquency, malicious hackers, mixed methods, governance of security, security networks.

La citation placée en exergue de cet article et communément attribuée à l'auteur de science-fiction qui fut le premier à utiliser le terme de «cyberespace» nous rappelle la nature à la fois fluide, chaotique et différentielle des innovations technologiques, rendant possibles par un processus cumulatif l'émergence d'outils, de produits et de services jugés improbables il y a encore quelques mois de cela. Pourtant, ce qui nous semble relever d'un futur bien hypothétique à Paris ou à Montréal est d'ores et déjà en voie d'expérimentation à Tokyo ou à San Francisco. Loin d'être cantonné aux acteurs industriels et gouvernementaux, dont le quotidien se trouve bouleversé par une succession frénétique de ruptures technologiques, ce constat s'applique évidemment au monde de la recherche scientifique, en voie d'être profondément reconfiguré par la capacité différentielle des champs disciplinaires à prendre acte de ces changements et à s'approprier les nouvelles thématiques qui en découlent, ainsi que les nouveaux outils théoriques et méthodologiques qu'elles induisent.

Si l'on ne s'inquiète pas outre mesure de l'avenir de l'informatique ou de la biologie, dont les découvertes propulsent une troisième révolution industrielle (Rifkin, 2013), le destin des sciences sociales en général, et de la criminologie en particulier, semble encore bien incertain sur ce point (2). Les criminologues manifestent encore une certaine réticence à intégrer ces profondes transformations à leurs questions de recherche. Le rôle que joue la technologie dans l'évolution du crime reste bien souvent cantonné à une conception réductrice et excessivement spécialisée qui se focalise sur le concept assez pauvre de «cybercrime», souvent présenté comme une nouvelle catégorie d'actes déviants. Ceux-ci se caractériseraient par la place centrale qu'occupe la technologie comme élément facilitateur et se déploieraient principalement dans un monde «virtuel» fantasmé, où les modes de régulation opérant traditionnellement dans le monde incarné seraient devenus obsolètes. Il n'est pas surprenant de constater qu'une telle approche, forgée à la fin du XX^{e} siècle, avant que l'informatique ne se démocratise et n'envahisse chaque facette de l'activité humaine, et qui repose essentiellement sur la description et la classification d'activités déviantes, éprouve de la difficulté à résonner (et également à raisonner) plus largement dans le champ criminologique et qu'elle demeure mar-

ginale dans la littérature scientifique. Offrant pas ou peu de passerelles théoriques et méthodologiques avec les thématiques de recherche mieux enracinées dans la discipline comme la délinquance des jeunes, la criminalité organisée, la victimologie, la criminologie clinique, la sociologie policière ou encore l'analyse des politiques pénales, cette démarche reste trop souvent perçue comme une excroissance disciplinaire causée par une exposition excessive et nocive à des questionnements issus de l'informatique.

Pourtant, faisant fi de cette approche fortement teintée d'insularité et de la quasi-indifférence que la délinquance numérique suscite auprès des branches établies de la criminologie, un nombre croissant de chercheurs, intrigués par les effets que produisent ces assemblages hybrides d'humains et de machines dans notre quotidien, se lancent dans des études dont l'ambition est d'identifier les contributions des nouvelles technologies à l'évolution de la délinquance. Qu'il s'agisse d'analyser les manifestations mondialisées ou au contraire localisées de ce phénomène, de comprendre les interactions prédatrices qui en découlent avec les flux dématérialisés de capitaux qui irriguent notre économie planétaire, ou encore de mettre à jour la diversité des modes de régulation déployés par un éventail élargi d'institutions de contrôle, de nouveaux chantiers de recherche s'ouvrent à la criminologie.

Cette contribution n'a pas pour ambition de recenser cette littérature émergente, ni d'en réaliser une analyse critique, ce qui vient d'être réalisé de manière très complète par Benbouzid et Ventre (2016), ou avant eux, Holt et Bossler (2014). Elle espère plus modestement attirer l'attention sur trois questions figurant au cœur du potentiel de transformation qui s'offre à notre discipline. La première question relève de la mise en chiffres des risques numériques et de l'intégration de ces statistiques à une mesure réellement globale de la délinquance. Elle s'interroge notamment sur la fiabilité des instruments de mesure traditionnels pour appréhender une délinquance en mutation, sur l'indépendance des sources alternatives de données émanant du secteur privé et sur les métriques requises pour mieux intervenir contre la cybercriminalité. La seconde question s'intéresse également à la quantification, mais sous un angle plus méthodologique et de manière non exclusive. Face à de nouveaux objets de recherche bénéficiant d'une visibilité sociale sans précédent, on pourrait aisément céder aux sirènes du *big data* et appeler à l'élaboration de puissants instruments capables de collecter et de traiter de grandes quantités de données, dans un contexte où la recherche des liens de causalité s'efface au profit d'une hégémonie des corrélations (Mayer-Schönberger, Cukier, 2014; Chan, Bennett Moses, 2016). Pourtant, à travers quelques exemples tirés de mes propres recherches, je montrerai comment les méthodes qualitatives peuvent s'intégrer de manière tout à fait harmonieuse aux approches statistiques dans une démarche mixte productrice de résultats prometteurs (Latour *et al.,* 2013; Venturini *et al.,* 2014). Finalement, la troisième section propose de nous débarrasser des œillères théoriques qui nous empêchent de prendre toute la mesure du pluralisme des modes de gouvernance se mettant en place avec plus ou moins de spontanéité et de coordination pour prévenir et limiter les préjudices

causés par la délinquance en ligne. Loin de prétendre asséner des réponses définitives à des objets aux contours encore flous, les trois thématiques qui constituent la trame de cette contribution ont pour vocation principale de convier le lecteur à prendre au sérieux la révolution numérique, à s'interroger sur les mutations délinquantes et sécuritaires qu'elle entraîne, ainsi qu'à considérer les nouvelles thématiques de recherche découlant de la subtile dialectique qu'entretiennent ces deux univers.

1. Mettre les risques numériques en chiffres

Depuis le début des années 1990, les statistiques criminelles en Amérique du Nord et dans de nombreux pays d'Europe occidentale semblent refléter une diminution importante des crimes violents et des atteintes à la propriété (Levitt, 2004; Ouimet, 2002; Blumstein, Wallman, 2006; Rosenfeld, Messner, 2009; Farrell *et al*., 2011; van Dijk *et al*., 2012; ou pour une interprétation plus nuancée, Aebi, Linde, 2010), sans que les causes en soient encore bien comprises. Cette tendance s'avère d'autant plus énigmatique pour les criminologues qu'elle a fait suite à une explosion de la criminalité durant les quatre décennies précédentes et a précipité l'adoption de politiques pénales extrêmement répressives, d'une part, et qu'elle ne semble pas avoir été interrompue ou même ralentie par la crise économique majeure qui a progressivement touché l'économie mondiale à partir de l'été 2007, d'autre part. Les facteurs démographiques, économiques, ou culturels, ainsi que l'efficacité de politiques pénales répressives, la disparition des opportunités criminelles sous l'influence de dispositifs de prévention mieux ciblés, ou encore le rôle de plus en plus dissuasif joué par une sécurité privée omniprésente sont autant d'hypothèses formulées pour expliquer cette chute de la criminalité.

Ces bonnes nouvelles, dans une discipline qui n'est pas réputée pour sa propension à l'optimisme, reposent cependant sur des données incomplètes qui ne tiennent pas compte d'une forme de délinquance faisant depuis une vingtaine d'années un nombre exponentiel de victimes. L'absence dans les statistiques officielles d'indicateurs fiables relatifs à la prévalence de la délinquance numérique constitue une omission majeure qui remet sérieusement en question la théorie d'un déclin généralisé de la criminalité, du moins pour les deux grandes catégories des atteintes à la propriété et des crimes de marché. Il serait probablement abusif de spéculer sur une éventuelle migration de la délinquance traditionnelle vers des formes technologiquement plus avancées qui font appel à des compétences et s'inscrivent dans des contextes d'opportunités différentes (Farrell *et al*., 2015). On doit par contre s'interroger sur les raisons qui ont abouti à la marginalisation des délinquances numériques dans la comptabilité de la criminalité. Cette question est d'importance, puisque les statistiques officielles sont abondamment mobilisées par les criminologues pour élaborer des théories plus ou moins robustes sur l'évolution des diverses formes de déviance dans les sociétés contemporaines, et par les décideurs

publics pour justifier l'adoption de politiques publiques parfois excessivement intrusives et des investissements technologiques pas toujours adaptés à la nature objective des menaces.

Parmi les pays occidentaux, le Royaume-Uni est sans nul doute celui qui a consenti les efforts les plus conséquents afin de moderniser ses outils statistiques, après avoir dressé un constat assez navrant de la sous-déclaration chronique des actes de piratage informatique et de fraude en ligne, aussi bien de la part des individus que des entreprises (McGuire, Dowling, 2013). Les chiffres de l'enquête de victimisation annuelle menée en Angleterre et au Pays de Galles pour 2007 et 2012 montraient ainsi que seulement 1 % des particuliers avaient rapporté les actes de piratage informatique dont ils avaient été victimes à la police, contre un taux de déclaration de 81 % pour les cambriolages et de 34 % pour les actes de vandalisme. Les crimes en ligne étaient déclarés par seulement 2 % des entreprises victimes, avec pour comparaison des taux de déclaration dans les cas de fraude interne ou externe de 37 %. Aux États-Unis, le taux de déclaration relatif au vol d'identité est de moitié inférieur à celui concernant les formes traditionnelles de crime contre la propriété (Tcherni *et al*., 2016). Seuls les chiffres disponibles pour la France montrent des taux de renvoi importants, comparables à ceux observés pour l'ensemble des victimes, pour les escroqueries bancaires liées à l'Internet (Benbouzid, Peaucellier, 2016). Une nouvelle méthodologie de recensement incluant les crimes numériques fut par conséquent adoptée par l'édition 2015 de l'enquête de victimisation anglaise, et les résultats confirmèrent le déficit de validité des statistiques officielles. En effet, aux 6,5 millions de crimes traditionnels comptabilisés vinrent s'ajouter 7,6 millions d'incidents frauduleux et de cybercrimes, doublant instantanément le volume des chiffres officiels de la criminalité (Office for National Statistics, 2015). Cette fulgurante ascension des crimes numériques qui constituent dorénavant la majorité de la délinquance mesurable (NCA Strategic Cyber Industry Group, 2016) ne manqua pas de susciter un vif émoi dans l'opinion publique.

Cette distorsion croissante entre des controverses criminologiques se questionnant sur les causes d'un déclin de la criminalité en Occident et l'explosion des formes de déviance numérique s'avère d'autant plus préoccupante qu'elle s'inscrit dans un environnement institutionnel où le secteur privé est devenu une source privilégiée de statistiques abondamment relayées par la presse généraliste, et instrumentalisées à l'occasion par les agences gouvernementales en charge des politiques publiques de cybersécurité. Chaque jour, de nouveaux chiffres produits par des entreprises commercialisant des biens ou des services en lien avec la sécurité informatique se faufilent dans les articles rédigés par des journalistes complaisants. Ces derniers signalent en effet rarement les conflits d'intérêts majeurs soulevés par l'origine de ces chiffres, leur sensationnalisme assumé, ou encore la qualité médiocre et la futilité de statistiques destinées à être oubliées aussitôt diffusées. Ils s'avèrent implicitement reconnaissants envers les services marketing de ces sociétés de leur fournir la matière première qui leur permet de rendre tangibles des risques

techniquement complexes et encore mal compris des profanes. Dans un article récemment publié, Côté *et al.* (2016) montrent ainsi que les treize principaux rapports annuels produits par des entreprises de sécurité informatique ou des associations professionnelles se caractérisent par la multiplicité des méthodologies utilisées pour recueillir les données (du sondage à l'utilisation de données internes collectées de manière automatisée par des capteurs installés sur les machines des clients) et l'opacité préoccupante de la démarche empirique employée (seulement deux des rapports décrivent en détail les protocoles suivis). Les auteurs soulignent aussi la triple hétérogénéité analytique qui caractérise ces documents: l'hétérogénéité structurelle observée révèle des différences importantes dans les stratégies analytiques en fonction de la culture organisationnelle de l'entreprise à l'origine du rapport et des priorités commerciales, alors que l'hétérogénéité conceptuelle soulève l'imprécision de la terminologie employée et de la définition des problèmes. Finalement, l'hétérogénéité prédictive de ces rapports fait référence à leurs prédictions vagues et parfois contradictoires. Pourtant, ce constat sévère n'empêche pas des agences gouvernementales canadiennes, françaises ou américaines de les mobiliser dans leurs propres documents et de s'en servir parfois afin de justifier des investissements majeurs ou l'adoption hâtive de mesures répressives dont les effets indésirables font rarement l'objet d'un débat public approfondi.

On se retrouve donc dans une configuration où les chiffres à notre disposition sont soit incomplets, soit biaisés et disparates, ce qui les rend difficilement utilisables. Dans le discours d'acceptation du prix Nobel qui lui fut attribué en 1971 pour ses travaux sur la croissance économique et l'élaboration d'outils statistiques capables de fournir une représentation globale des grands agrégats économiques, Simon Kuznets se livra à un vibrant plaidoyer en faveur des métriques manquantes qui permettraient de comprendre le phénomène de la croissance (et son absence) dans toute sa complexité (Kuznets, 1971). Kuznets appelle à une expansion des concepts et des outils statistiques mobilisés afin de rendre possible la mesure des coûts (pollution, urbanisation effrénée), mais aussi des bénéfices (longévité accrue, amélioration de la qualité de vie, réduction des inégalités) cachés associés à son objet d'étude. Cela permettrait selon lui de raffiner le pouvoir explicatif de la science économique en l'aidant à résoudre certains «puzzles» intellectuels et à se prémunir contre de mauvaises «surprises» liées à de brusques renversements de situation mal anticipés. Une démarche semblable serait bénéfique dans le domaine de la cybercriminalité, où les indicateurs à développer pourraient notamment se pencher sur le rôle que joue l'innovation technique dans la propagation et le contrôle des risques numériques, la confiance que les usagers accordent aux institutions publiques et privées pour gérer ces risques, le degré de protection dont peuvent se prévaloir des consommateurs qui réalisent toujours plus de transactions en ligne, les implications de nouvelles méthodes de lutte contre la cybercriminalité sur la banalisation de la surveillance, etc.

Si de nouveaux instruments s'appuyant sur des indicateurs précis doivent être élaborés pour capturer ces métriques manquantes, à l'instar de l'effort

consenti par le Royaume-Uni pour actualiser son enquête périodique de victimisation, de nombreuses bases de données déjà détenues par des organisations internationales (3) pourraient donner lieu à des analyses croisées potentiellement très riches en enseignements. Par exemple, des entités qui opèrent à l'échelle mondiale comme les entreprises qui commercialisent des antivirus ou les ONGs qui luttent contre le spam disposent par définition de données détaillées pour la plupart des pays connectés à Internet. Ces données permettent en théorie des comparaisons sur les niveaux de protection dont bénéficient leurs usagers de chaque pays, ainsi que des analyses plus poussées sur les mécanismes de prévention ou de contrôle pouvant expliquer cette exposition différentielle aux risques numériques.

De la même manière, les traces numériques laissées par les activités déviantes et leurs éléments précurseurs sont si aisément accessibles, et disponibles à une telle échelle (Giannasi *et al*., 2012; Décary-Hétu, Aldridge, 2015; Benbouzid, Ventre, 2016), que l'on peut envisager de les utiliser pour reconstituer des corpus de données permettant d'évaluer de manière approximative la taille d'un marché illicite, le nombre de ses participants, certaines de leurs caractéristiques, ou encore le volume des transactions effectuées. Ainsi, l'analyse systématique de 500 000 évaluations portant sur 94 000 travailleuses du sexe américaines tirées du principal forum en ligne utilisé par les clients de ce type de services permit à Cunningham et Kendall (2011) d'étudier l'impact des nouvelles technologies sur les pratiques prostitutionnelles. Si on ne peut qualifier la prostitution de crime, le stigmate moral qui y reste associé demeure bien réel, et cette activité reste judiciarisée dans de nombreuses juridictions, aussi bien en ce qui concerne les prestataires de services que les consommateurs. Adoptant une perspective de santé publique et de réduction des méfaits, les deux auteurs démontrèrent que la disponibilité accrue de relations sexuelles tarifées facilitée par l'avènement de l'Internet contribua à une expansion de ce marché plutôt qu'au déplacement des modes de sollicitation, même si les prostituées âgées de 30 et 40 ans semblent tirer un certain bénéfice de la publicité en ligne pour réduire leur visibilité dans les quartiers chauds des métropoles dans lesquels elles exercent. Les marchés de la drogue se prêtent également à ce type d'analyses: Aldridge et Décary-Hétu (2016) ont ainsi examiné les transactions réalisées sur la plate-forme Silk Road jusqu'au 15 septembre 2013 par 1 031 vendeurs mettant à la disposition de clients potentiels 10 927 types de produits stupéfiants différents. Ces auteurs identifient une part significative de transactions (25 %) qui relève de la vente en gros. Loin de se restreindre à de modestes transactions de détail, les cryptomarchés en ligne semblent ainsi jouer un rôle important d'intermédiaire à l'échelle internationale entre grossistes et revendeurs. Dans les deux exemples précédents, de nouvelles connaissances sur la structure et la dynamique des marchés en ligne, ainsi que leurs effets sur les marchés hors ligne, n'auraient pu voir le jour sans le recours à des procédés automatisés de collecte, de classement et d'analyse des données à grande échelle. Même si les critères du *big data* ne sont pas techniquement réunis selon l'interprétation qu'en ont les

informaticiens, on se trouve de toute évidence confronté à un changement radical d'approche et d'ordre de grandeur qui permet à la criminologie d'envisager des questions de recherche inédites, ou de traiter de manière novatrice des thèmes en apparence familiers.

2. Nouveaux objets, anciennes méthodes

Les vastes corpus de données rendus disponibles aux chercheurs en sciences sociales et le développement concomitant d'outils de cueillette, d'analyse et de visualisation puissants, abordables et relativement simples d'utilisation ouvrent indéniablement la voie à l'étude de populations entières grâce à des approches de statistique avancée ou d'analyse de réseaux sociaux. Il serait cependant prématuré de reléguer les démarches qualitatives ou ethnographiques au cimetière des méthodologies obsolètes. En effet, une dépendance excessive envers les outils du *datamining* (le forage des données) risque de créer un déficit de *data-meaning* (la signification des données), si l'on ne prête pas une attention suffisante à la signification des données dont on peut dorénavant si facilement automatiser le traitement. Gabriella Coleman (2016) a fort bien démontré dans son ouvrage sur le groupe hacktiviste *Anonymous* comment l'observation participante et des pratiques artisanales d'analyse des données (au sens noble du terme) restent des outils méthodologiques privilégiés permettant d'explorer la richesse et la grande diversité des interactions sociales s'exprimant par le biais des plates-formes numériques.

Trois exemples tirés de mes propres recherches illustrent la nécessité de mobiliser des méthodologies d'enquête mixtes (quantitatives et qualitatives) pour bien saisir la complexité des risques numériques et se prémunir contre des interprétations superficielles, voire totalement erronées. Les travaux que je mène depuis une demi-douzaine d'années sur l'organisation sociale des pirates informatiques malveillants se focalisent sur le rôle que joue la confiance dans la construction de modes de collaboration efficaces entre individus qui ne se connaissent pas personnellement et ne se sont même jamais rencontrés *de visu*. L'émergence de formes numériques de délinquance marque en effet l'aboutissement d'un lent processus entamé au XIX^{e} siècle qui a vu les crimes contre la propriété se transformer sous l'effet de l'industrialisation de la société, et passer successivement du mode artisanal, puis picaresque, au mode entrepreneurial, avant d'aboutir à la délinquance par projet (McIntosh, 1975). Ce processus d'adaptation organisationnelle aux nouvelles opportunités de vol, mais aussi aux dispositifs de sécurité toujours plus sophistiqués mis en place pour en limiter le volume et les bénéfices, culmine avec l'automatisation et l'industrialisation de la délinquance acquisitive permises par la démocratisation de l'informatique et la mise en réseaux des machines. Toutefois, si des projets délinquants faisant appel à des compétences techniques de pointe dispersées à l'échelle planétaire peuvent être envisagés et mis en œuvre avec une aisance et une rapidité sans précédent, un défi majeur

à relever pour ceux qui planifient et exécutent ces projets consiste à établir des liens de confiance suffisamment robustes pour susciter la coopération et décourager les trahisons et les défections. L'anonymat et la dispersion géographique qui protègent les participants à ces projets criminels des arrestations policières constituent aussi un obstacle à la création de liens de confiance suffisamment forts pour surmonter les inévitables erreurs et échecs qui surviennent dans ce type d'activités. Par contraste aux délinquants opérant selon un schéma artisanal, picaresque ou entrepreneurial, qui s'appuient sur une proximité géographique, ethnoculturelle ou biographique pour générer des informations fiables issues du bouche à oreille, les délinquants numériques opèrent dans un environnement où les signaux permettant d'évaluer la fiabilité d'un complice potentiel sont rares, de faible qualité et relativement faciles à contrefaire. De surcroît, le prix à payer pour la tromperie et la trahison sont négligeables, ce qui rend toute collaboration potentiellement risquée.

Cette mise en contexte permet de mieux comprendre la nécessité de combiner approches quantitatives et qualitatives pour analyser les nouveaux registres de collaboration délinquante. Une première de nos études a porté sur un réseau de dix hackers démantelé par la police québécoise en 2008, et pour lesquels des conversations privées en ligne menées au cours des deux années précédentes ont pu être obtenues. La lecture et le codage des discussions entre chaque dyade du réseau selon le niveau de confiance ou de défiance exprimé a permis d'éviter les contresens interprétatifs qui auraient découlé du recours exclusif à la technique de l'analyse des réseaux sociaux. En effet, un simple décompte de la fréquence des conversations laissait entrevoir une relation privilégiée entre deux acteurs disposant respectivement du plus fort capital social et technique au cœur de ce réseau. L'analyse du contenu des conversations permit cependant de comprendre que cette fréquence ne traduisait pas l'existence de liens forts, mais reflétait au contraire une méfiance réciproque entre les deux têtes dirigeantes qui communiquaient donc fréquemment pour se rappeler mutuellement à l'ordre et évaluer leurs probabilités de défection respectives (Dupont, 2013; Dupont, 2016a).

Dans une seconde étude réalisée sur un échantillon beaucoup plus vaste de 299 985 hackers ayant échangé 449 478 commentaires destinés à évaluer la réputation de leurs partenaires, le recours à l'analyse qualitative de 259 000 commentaires sélectionnés au hasard permit de nuancer des résultats quantitatifs laissant entrevoir l'adaptation efficace du système de réputation automatisé popularisé par eBay aux communautés déviantes (Dupont *et al*., 2016; Dupont, 2016a). Le taux global de satisfaction de 83,3 % reflétant des scores de réputation positifs pouvait sembler très élevé pour une communauté de délinquants spécialisés dans l'art de la duperie, mais des analyses plus approfondies firent apparaître un fort biais de déclaration dans la distribution des évaluations. Alors que les nouveaux membres de cette communauté n'attribuaient jamais d'évaluations négatives à leurs pairs (pour 86,4 % d'évaluations positives et 13,6 % d'évaluations neutres), ceux figurant au sommet de la hiérarchie (les administrateurs du forum) semblaient opérer dans une réalité

radicalement différente. En effet, la majorité de leurs interactions (61,6 %) était caractérisée par la remise en question de la fiabilité de leurs interlocuteurs et seulement 33,8 % des scores de réputation attribués à leurs pairs étaient positifs. Il est donc fort probable que le statut au sein de la communauté, et la volonté des nouveaux arrivants de s'insérer à tout prix dans ce groupe en évitant soigneusement tout conflit avec les autres membres, ont influencé de manière disproportionnée la nature largement positive des commentaires formulés. Autrement dit, le désir de conformité et la puissance nocive de la réciprocité dans l'attribution de commentaires négatifs ont produit des scores de réputation dont la fiabilité semble très incertaine et qui se sont donc révélés d'une utilité relative pour les participants. Cette première fissure dans l'image idéalisée de réseaux délinquants stimulés par le pouvoir émancipateur de la technologie s'est trouvée accentuée par l'analyse qualitative d'un échantillon représentatif de commentaires servant à justifier les scores numériques attribués *via* le système de réputation du forum. Derrière l'apparence d'harmonie et d'efficacité reflétée par les scores positifs quantitativement très majoritaires, et contrairement à ce qui était attendu, ce n'étaient ni la compétence technique, ni les capacités entrepreneuriales, ni les contributions altruistes au bon fonctionnement de la communauté qui constituaient la raison principale à l'attribution d'un score de réputation positif ou négatif. La première place dans chacune de ces deux catégories était en effet occupée par des commentaires sarcastiques ou hors contexte relevant de ce que Gabriella Coleman (2016) appelle le *lulz*, cet humour potache teinté de méchanceté et d'absurdité qui résonne parfaitement avec la contre-culture transgressive des hackers. Ainsi, lorsque plus du tiers des scores de réputation attribués étaient justifié par des explications dont il est impossible de tirer un sens, on peut légitimement douter de l'utilité du système reposant sur des données aussi inconsistantes. Cette fragilité, et la volatilité de la confiance qu'elle induit pour les communautés des hackers malveillants, auraient probablement échappé à l'analyse si on s'était contenté de procéder à un simple décompte destiné à alimenter des modèles statistiques, dont la complexité dissimule parfois une méconnaissance fondamentale des phénomènes étudiés.

Le troisième et dernier exemple d'une méthodologie mixte provient d'une étude en cours de réalisation sur le forum *Darkode*, démantelé par le FBI en juillet 2015 (FBI, 2015). Composé des 400 à 500 pirates malveillants les plus actifs dans la sphère anglophone, ce forum était exclusivement accessible sur invitation et servait de marché illicite principal à la vente de logiciels malveillants tels que *Zeus*, *SpyEye*, *Phoenix*, ou encore *Blackhole*. Des bases de données de numéros de cartes de crédit volées ou de renseignements personnels étaient également disponibles à l'achat. L'un des principaux participants condamnés à la suite de ce démantèlement (même si son arrestation en Thaïlande et son extradition aux États-Unis précédèrent le démantèlement technique du forum) est Hamza Bendelladj, un pirate algérien connu en ligne sous le nom de *Bx1*. Dans le rapport présentenciel (4) rédigé par les procureurs afin d'aider le juge à déterminer la peine devant lui être infligée, le département

de la Justice américain utilisa une formule relativement simple pour évaluer l'ampleur des préjudices causés par Hamza Bendelladj à ses victimes. Ayant établi qu'il avait notamment revendu plus de 200 000 numéros de cartes de crédit à des fraudeurs sur ce forum, et estimant que chaque carte de crédit pouvait générer en moyenne un profit criminel de 500 dollars, une simple multiplication aboutit à un montant total d'au moins 100 millions de dollars de pertes (Horn *et al.,* 2016). Ce type de calculs alimente de manière routinière les rapports publiés par les entreprises de sécurité ou les services d'enquêtes spécialisés afin de démontrer les millions, voire les milliards, de profits générés par la cybercriminalité. Un examen attentif de la transaction en question produisit toutefois des résultats bien différents. Les conversations entre membres de *Darkode* qui nous sont accessibles indiquent que *Bx1* a offert le 3 décembre 2011 à la vente 140 000 cartes de crédit fraîchement volées provenant des États-Unis et du Canada (voir figure 1).

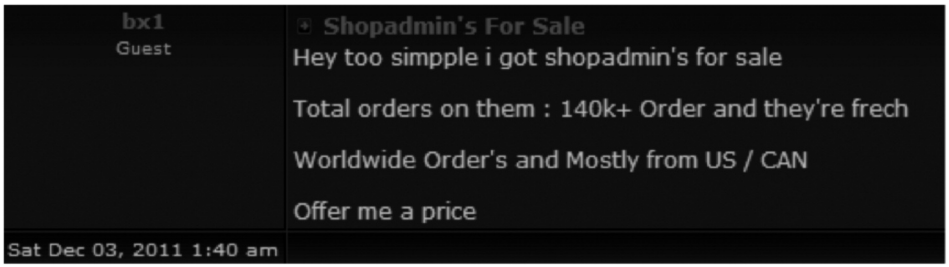

Figure 1. Offre initiale de Bx1 concernant la vente de 140 000 cartes de crédit volées

Il s'agit de la plus grosse transaction réalisée par *Bx1* sur *Darkode*, et d'après le mode de calcul officiel des procureurs américains, cette transaction aurait dû lui faire gagner 70 millions de dollars. Malheureusement pour lui, la lecture des réactions et des offres suscitées par son annonce reflète la difficulté pour les hackers de monétiser les données volées qui prolifèrent sur les marchés clandestins. Un hacker expérimenté nommé *Jumbie* lui demande d'abord de proposer un prix de base afin de lancer les enchères. *Bx1* suggère alors une offre de départ de 20 000 dollars, qui reçoit une contre-offre beaucoup plus modeste de la part de *Donchicho* de 300 dollars. Tentant de relancer les enchères, *Bx1* explique que valoriser chaque carte à seulement 0,5 dollar lui rapporterait 50 000 dollars (*sic*). Peut-être sensible à son plaidoyer, *MrGold* lui offre alors 2 000 dollars, ce qui reste bien en deçà des attentes de *Bx1*. Une nouvelle tentative afin de trouver un acheteur plus généreux l'amène à préciser qu'il a testé six des cartes offertes et que toutes ont fonctionné sans problème. À cela, *Sven* lui répond qu'après avoir tenté d'utiliser plusieurs milliers de cartes volées, les bases de données des banques et des émetteurs de cartes Visa, MasterCard et Amex vont bloquer de manière automatisée les transactions, et que les taux de réussite baisseront à 20 %, ce qui doit donc être pris en compte dans la détermination du juste prix. La discussion concer-

nant cette vente se conclut finalement quelques jours plus tard sur l'offre la plus haute formulée par *MrGold* au prix de 3 000 dollars. Ne disposant pas des messages privés échangés par les hackers, il est possible que *Bx1* ait reçu de manière confidentielle une proposition plus proche de ses attentes, mais on ne peut s'empêcher d'être frappé par l'écart —ou plutôt le gouffre— qui sépare le montant calculé par les autorités américaines de celui que semblent prêts à payer les entrepreneurs criminels actifs sur *Darkode*. La lecture et l'interprétation attentive des conversations qui structurent le fonctionnement de cette communauté de hackers s'avèrent de toute évidence beaucoup plus chronophages que ne le serait la cartographie automatisée des interactions sociales entre ceux qui la composent, ou encore l'étude historique des prix de vente exigés par les fournisseurs de biens et de services illicites qui transigent sur ce marché. Mais sans la première —et coûteuse— approche, les deux stratégies analytiques suivantes perdraient une part importante de leur force, restant hermétiques aux nuances, aux ambiguïtés, aux contradictions, aux incohérences et aux arbitrages qui permettent à la première de mieux saisir le fonctionnement parfois chaotique de ce type de communauté.

3. Des dispositifs de régulation inédits

Les réseaux délinquants ne possèdent évidemment pas le monopole de l'adaptation aux nouvelles conditions technologiques. Sous la pression des transformations provoquées par les risques numériques, on assiste depuis une vingtaine d'années à la reconfiguration des modalités du contrôle social. Celles-ci sont caractérisées par la place croissante accordée aux stratégies de gouvernance en réseaux et à l'implication d'acteurs organisationnels privés ou hybrides. Le rôle joué par la sécurité privée et les institutions non étatiques dans la prévention et la répression de certaines formes de criminalité ne constitue pas en soi une nouveauté (Ocqueteau, 2004; Wood, Dupont, 2006; Brodeur, 2010). Toutefois, la structure technique distribuée des réseaux informatiques et le fait qu'ils soient majoritairement détenus et gérés par des intérêts privés se déployant à l'échelle mondiale confèrent des caractéristiques inédites aux assemblages régulatoires chargés de prendre en charge ces nouveaux risques numériques.

Dans une recherche dont les résultats seront publiés à l'automne (Dupont, 2016b), j'ai ainsi tenté de recenser et de cartographier la structure polycentrique des acteurs institutionnels impliqués dans la lutte contre les crimes numériques et des initiatives de coopération auxquelles ils participent. Cette étude documentaire dont la collecte de données s'est déroulée durant l'été 2014 a permis d'identifier 657 acteurs institutionnels impliqués dans 51 initiatives de coopération internationale de lutte contre la cybercriminalité. Les services de police nationaux et les organisations internationales telles qu'Interpol, Europol, ou l'Union internationale des télécommunications occupent évidemment une place prééminente dans l'échantillon ainsi constitué avec respecti-

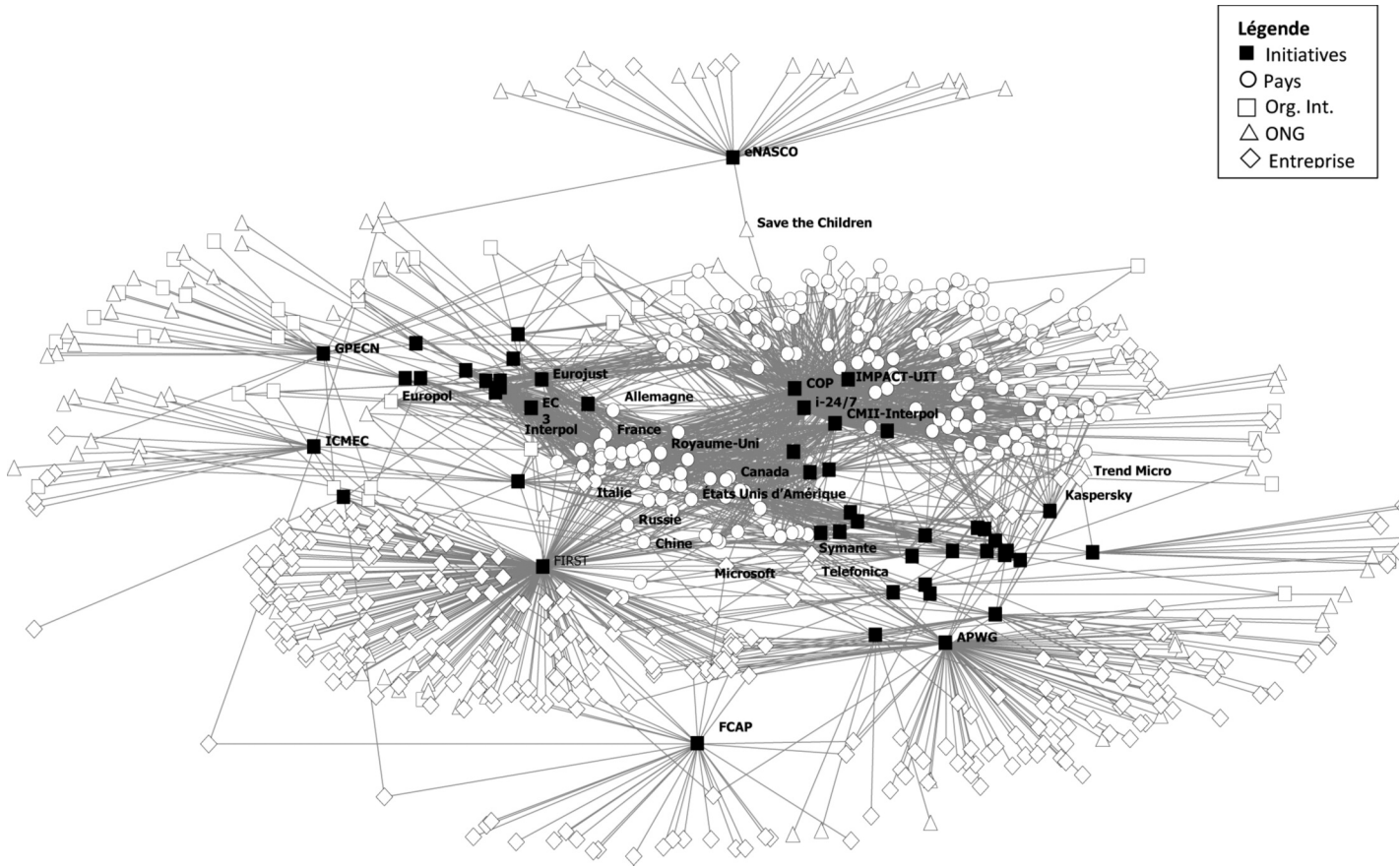

Figure 2. Le réseau de coopération internationale contre la cybercriminalité (2014)

vement 31 % et 6 % des acteurs identifiés. Mais des ONG et des associations professionnelles comme *Innocence en danger* ou le *Global prosecutors e-crime network*, fournissent un contingent d'acteurs non négligeable comprenant 16 % des organisations recensées. Les entreprises constituent quant à elles 47 % de l'échantillon, regroupant des multinationales de l'informatique et de la cybersécurité, telles que Microsoft, Symantec ou Kaspersky, mais aussi des «poids lourds» du secteur bancaire ou des télécommunications. Cette diversité institutionnelle est complétée d'une diversité fonctionnelle, puisque l'on peut répartir les 51 initiatives en cinq grands domaines d'activités n'étant nullement exclusifs les uns des autres: le renforcement des capacités à travers des programmes de formation (74,5 %), l'échange de renseignements sur les menaces et leurs auteurs (49 %), le soutien à l'harmonisation législative et réglementaire (37,2 %), les opérations répressives telles que les enquêtes criminelles et la collecte du renseignement (31,4 %), et enfin les activités de lobbysme (9,8 %).

L'analyse de la coparticipation des 657 acteurs institutionnels aux 51 initiatives permet alors de représenter visuellement la carte des liens de coopération qui unissent avec plus ou moins de force des acteurs aux capacités, aux intérêts et aux priorités extrêmement variables.

Les détails méthodologiques et les principales constatations de cette étude ne peuvent être présentés de manière plus approfondie ici, mais on doit quand même insister sur la mise en lumière d'assemblages hybrides émergents dégagés de cet exercice de cartographie, à travers lequel on peut nettement observer le rôle structurant joué par de grandes entreprises comme Microsoft ou encore Symantec, au même titre qu'Interpol et Europol. Des ONG comme *Save the children* ont également réussi à se positionner de manière centrale dans ce réseau malgré tout éclaté, sans que l'on comprenne encore vraiment la nature de l'influence que ces véritables entrepreneurs de morale exercent sur les politiques et les pratiques internationales de coopération. On peut certainement se réjouir que des organisations policières nationales manifestement dépassées par l'ampleur de la délinquance numérique puissent s'appuyer sur les compétences techniques et les ressources financières considérables d'intérêts corporatifs pour mettre en œuvre des mécanismes de régulation innovants (Dupont, à paraître). Néanmoins, on a aussi le devoir de s'interroger sur les limites d'une telle privatisation, ou à tout le moins sur les effets inédits de dépendance que de tels partenariats pourraient susciter et sur les foyers de divergence avec les intérêts des victimes individuelles et des consommateurs. L'équilibre délicat entre l'indispensable coopération policière pour lutter contre une cybercriminalité endémique et l'inévitable compétition opposant des pays engagés dans des activités d'espionnage numérique afin de renforcer leurs industries nationales doit également faire l'objet d'investigations beaucoup plus approfondies (Ventre, 2011). Attentifs à tous ces préalables, nous serons alors mieux en mesure d'évaluer la complexité et l'interdépendance des facteurs qui participent à la prolifération ou à la réduction des risques numériques.

Conclusion

Les théories de la criminologie administrative, qui s'appuient sur des logiques mécanistes de dissuasion ou d'incitatifs négatifs déployées contre des acteurs supposément rationnels, au même titre que celles inspirées par une criminologie plus critique, qui agitent l'épouvantail des technologies numériques comme vecteurs implacables d'une société de surveillance et de contrôle social absolus, offrent des modèles incomplets d'interprétation des transformations criminelles engendrées par la révolution numérique depuis un quart de siècle. Sans renier les précieuses contributions apportées par ces deux courants historiques, une troisième voie inspirée de la perspective écologique me semble plus robuste et fertile pour analyser de manière globale les interactions sociales, technologiques et organisationnelles qui donnent corps à l'environnement des risques numériques. Concevoir l'écosystème de la cybercriminalité comme la convergence d'acteurs industriels, délinquants et sécuritaires obéissant à des rationalités respectives uniques permettrait indéniablement de surmonter la confusion créée par la complexité de cette nouvelle architecture criminelle, en tenant simultanément compte des relations de coopération, de compétition et de prédation qui caractérisent cet écosystème. Une telle approche holistique ne se limiterait pas à la seule dimension géographique ayant inspiré l'École de Chicago (Wikström, 2009), pas plus qu'elle ne chercherait à imiter trop littéralement les travaux issus de la biologie (Felson, 2006). Elle viserait plutôt à exploiter la richesse du vaste répertoire des métaphores écologiques pour donner sens à une complexité sociale découlant de phénomènes d'interdépendance technique et institutionnelle sans précédent ayant inspiré l'imagination conceptuelle de nombreux sociologues (Elias Dunning, 1994; Latour, 2006; Grossetti, 2004; Granovetter, 1985). Restant encore largement à définir et à mettre en œuvre, cette écologie de la délinquance numérique permettrait trois avancées majeures: de mieux comprendre les raisons qui expliquent pourquoi les statistiques dont nous disposons restent aussi indigentes et quelles stratégies pourraient être envisagées pour en améliorer la qualité, d'une part. D'autre part, de mieux concevoir comment les réseaux de cyberdélinquants innovent et exploitent les technologies commercialisées avec un souci parcimonieux de la sécurité par des multinationales ou des startups plus préoccupées de leurs parts de marché que de la protection de leurs usagers. Et enfin, de mieux appréhender comment la structure des réseaux de gouvernance qui font éclore de nouvelles modalités du contrôle social recalibre le rôle des États dans ce domaine.

Alternativement, le risque pour la criminologie traditionnelle de continuer à se désintéresser des crimes numériques serait de voir ce champ de recherche colonisé par d'autres disciplines plus visionnaires quoique moins bien équipées théoriquement, comme l'informatique. Il est assez symptomatique de constater en effet que l'Université de Cambridge vient de créer un centre de recherche sur la cybercriminalité s'affichant comme interdisciplinaire, mais hébergé dans son département d'informatique, et dont sept des neuf membres

fondateurs sont également issus de cette discipline (5). L'unique criminologue dont le nom figure sur le site internet du centre ne s'est pour sa part jamais intéressé à la «délinquance numérique». Les outils et les données qui seront mises à la disposition de la communauté scientifique par cette initiative s'annoncent d'une grande valeur empirique, mais seul un véritable effort transdisciplinaire favorisant la création d'hybrides conceptuels aboutira à une réelle plus-value des connaissances nécessaires.

Bibliographie

Aebi M., Linde A., 2010, Is there a crime drop in Western Europe?, *European Journal on Criminal Policy and Research*, 16, 4, 251-277.

Aldridge J., Décary-Hétu D., 2016, Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets, *International Journal of Drug Policy*, doi:10.1016/j.drugpo.2016.04.020.

Benbouzid B., Peaucellier S., 2016, L'escroquerie sur Internet, *Réseaux*, 197-198, 137-171.

Benbouzid B., Ventre D., 2016, Pour une sociologie du crime en ligne: Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing, *Réseaux*, 197-198, 9-30.

Blumstein A., Wallman J. (eds), 2006, *The crime drop in America: Revised edition*, New York, Cambridge University Press.

Brodeur J.-P., 2010, *The policing web*, Oxford, Oxford University Press.

Chan J. Bennett Moses L., 2016, Is Big Data challenging criminology? *Theoretical Criminology,* 20, 1, 21-39.

Coleman G., 2016, *Anonymous: Hacker, activiste, faussaire, mouchard, lanceur d'alerte*, Montréal, Lux Éditeur.

Côté A.-M., Bérubé M., Dupont B., 2016, Statistiques et menaces numériques: comment les organisations de sécurité quantifient la cybercriminalité, *Réseaux*, 197-198, 205-224.

Cunningham S., Kendall T., 2011, Prostitution 2.0: The changing face of sex work, *Journal of Urban Economics*, 69, 3, 273-287.

Décary-Hétu D., Aldridge J., 2015, Sifting through the net: Monitoring of online offenders by researchers, *The European Review of Organized Crime*, 2, 2, 122-141.

Dupont B., 2013, Skills and trust: A tour inside the hard drives of computer hackers, *in* Morselli C. (ed.), *Crime and networks*, New York, Routledge, 195-217.

Dupont B., 2016a, Les liens faibles du crime en ligne: écologie de la méfiance au sein de deux communautés de hackers malveillants, *Réseaux*, 197-198, 109-136.

Dupont B., 2016b, La gouvernance polycentrique du cybercrime: les réseaux fragmentés de la coopération internationale, *Cultures et Conflits*, 102, 139-164.

Dupont B. (à paraître), Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime, *Crime, Law and Social Change.*

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

Elias N., Dunning E., 1994, *Sport et civilisation: La violence maîtrisée*, Paris, Fayard.

Farrell G., Laycock G., Tilley N., 2015, Debuts and legacies: The crime drop and the role of adolescence-limited and persistent offending, *Crime Science: An Interdisciplinary Journal*, 4, 16, 1-10.

Farrell G., Tilley N., Tseloni A., Mailley J., 2011,. The crime drop and the security hypothesis, *Journal of Research in Crime & Delinquency*, 48, 2, 147-175.

FBI, 2015, Cyber criminal forum taken down: Members arrested in 20 countries. *Federal Bureau of Investigation*. Disponible en ligne [https://www.fbi.gov/news/stories/cyber-criminal-forum-taken-down].

Felson M., 2006, *Crime and nature*, Thousand Oaks, Sage Publications.

Giannasi P., Pazos D., Esseiva P., Rossy Q., 2012, Détection et analyse des sites de vente de GBL sur Internet: perspectives en matière de renseignement criminel, *Revue Internationale de Criminologie et de Police Technique et Scientifique*, LXV, 4, 468-479.

Granovetter M., 1985, Economic action and social structure: The problem of embeddedness, *American Journal of Sociology*, 91, 3, 481-510.

Grossetti M., 2004, *Sociologie de l'imprévisibilité: Dynamiques de l'activité et des formes sociales*, Paris, Presses Universitaires de France.

Holt T., Bossler A., 2014, An assessment of the current state of cyber-crime scholarship, *Deviant Behavior*, 35, 1, 20-40.

Horn J., Ghali K., Grimberg S., 2016, Sentencing memorandum. *United States of America v. Hamza Bendelladj (A.K.A. "Bx1")*. Disponible en ligne à [http://krebsonsecurity.com/wp-content/uploads/2016/04/bx1-gribboSM.pdf].

Kuznetz S., 1971, Modern economic growth: Findings and reflections, *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 1971*. Disponible en ligne [http://www.nobel-prize.org/nobel_prizes/economic-sciences/laureates/1971/kuznets-lecture.html].

Latour B., 2006, *Changer de société – Refaire de la sociologie*, Paris, La Découverte.

Latour B., Jensen P., Venturini T., Grauwin S., Boullier D., 2013, Le tout est toujours plus petit que ses parties, *Réseaux*, 177, 197-232.

Levitt S., 2004, Understanding why crime fell in the 1990s: Four factors that explain the decline and six that do not, *Journal of Economic Perspectives*, 18, 1, 163-190.

Mayer-Schönberger V., Cukier K., 2014, *Big Data: La révolution des données est en marche*, Paris, Robert Laffont.

McGuire M., Dowling S., 2013, *Cyber crime: A review of the evidence, Home Office research report 75*, Londres, Home Office.

McIntosh M., 1975, *The organisation of crime*, Londres, McMillan Press.

NCA Strategic Cyber Industry Group, 2016, *Cyber Crime Assessment 2016*, Londres, National Crime Agency.

Ocqueteau F., 2004, *Polices entre État et marché*, Paris, Les Presses de Sciences Po.

Office for National Statistics, 2015, *Improving crime statistics in England and Wales*, Londres, ONS.

Ouimet M., 2002, Explaining the American and Canadian crime «drop» in the 1990's, *Canadian Journal of Criminology and Criminal Justice*, 44, 1, 33-50.

Rifkin J., 2013, *La Troisième Révolution industrielle*, Arles, Actes Sud.

Rosenfeld R., Messner S., 2009, The crime drop in comparative perspective: The impact of the economy and imprisonment on American and European burglary rates, *The British Journal of Sociology*, 60, 3, 445-471.

Tcherni M., Davies A., Lopes G., Lizotte A., 2016, The dark figure of online property crime: Is cyberspace hiding a crime wave?, *Justice Quarterly*, 33, 5, 890-911.

Van Dijk J., Tseloni A., Farrell G. (eds), 2012, *The international crime drop*, Basingstoke, Palgrave Macmillan.

Ventre D., 2011, *Cyberattaque et cyberdéfense*, Paris, Lavoisier.

Venturini T., Cardon D., Cointet J.-P., 2014, Présentation, *Réseaux*, 188, 9-21.

Wikström P.-O., 2009, Social ecology of crime. *Oxford Bibliographies*, DOI: 10.1093/OBO/9780195396607-0027. Disponible en ligne à [http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0027.xml].

Wood J., Dupont B. (eds), 2006, *Democracy, society and the governance of security*, Cambridge, Cambridge University Press.

Notes:

1 Je tiens à remercier Bilel Benbouzid, Anne-Marie Côté et Frédéric Ocqueteau pour leur relecture attentive d'une première version de cet article et leurs judicieuses suggestions. Les erreurs restent évidemment de ma seule responsabilité.

2 Pour une réflexion beaucoup plus approfondie sur le sujet, voir le cahier de recherches en ligne tenu par Dominique Boullier à https://shs3g.hypotheses.org/.

3 Comme celles publiées par l'Union internationale des télécommunications (*World Telecommunication/ICT Indicators* et *Global Cybersecurity Index*), l'OCDE (Indicateurs-clés des TIC), la Banque mondiale (*Knowledge Economy Index*), l'OTAN (*International Cyber Development Review database*), ou encore de grandes entreprises de l'Internet (Microsoft, Symantec, Google, etc.) et des ONGs (Spamhaus, Anti-Phishing Working Group).

4 En Amérique du Nord, il s'agit du rapport préparé en vue du prononcé de la sentence lorsque la personne accusée a plaidé coupable. Ce rapport dresse le bilan de la situation de la personne à condamner, de ses antécédents criminels, de son potentiel de réinsertion et du risque pour la société. Il tient également compte des directives locales en matière de détermination de la peine (*sentencing*).

5 [https://www.cambridgecybercrime.uk/].