LA COÉVOLUTION DE LA TECHNOLOGIE ET DE LA DÉLINQUANCE : QUELQUES INTUITIONS CRIMINOLOGIQUES

BENOÎT DUPONT ([1])

La révolution technologique numérique engagée dès le début des années 1990 a transformé par effet de cascade bien des sphères d'activité humaine, comme les transactions marchandes et financières, l'accès à l'information et à la culture, les relations entre services publics et citoyens ou encore le fonctionnement des infrastructures essentielles. À cet égard, les délinquants ont très rapidement su exploiter les nombreuses opportunités associées à cette vague d'innovations et de nouveaux services. Ils ont notamment identifié la profonde transformation des habitudes de consommation et les multiples possibilités offertes par la dématérialisation des moyens de paiement comme un réservoir intarissable d'opportunités frauduleuses. Pourtant, il est surprenant de constater que la criminologie reste encore peu intéressée par ces transformations et leurs implications sur les divers mécanismes de contrôle social. Que ce soit en tant qu'objet d'étude ou qu'outil de recherche permettant d'accumuler et d'analyser des quantités considérables de données portant sur des comportements délinquants 'classiques', il subsiste un décalage manifeste entre l'omniprésence des technologies de l'information et de la communication dans nos vies quotidiennes, d'une part, et la place qu'elles occupent dans la production scientifique criminologique, d'autre part. Près de vingt ans après la démocratisation de l'Internet dans les sociétés occidentales, un rapide recensement du nombre limité de communications proposées dans les conférences internationales ou d'articles publiés dans les principales revues scientifiques de la discipline met en évidence

[1] Directeur du Centre International de Criminologie Comparée, Université de Montréal.

la nature encore marginale de ces questions de recherche, même si par effet cumulatif, on commence à voir émerger un corpus criminologique examinant cette nouvelle réalité à l'aide d'outils conceptuels et méthodologiques adaptés[2]. Il en résulte une appropriation par d'autres champs disciplinaires tels que l'informatique ou l'économie, qui sont en train de façonner l'agenda de recherche et les méthodologies dominantes en matière de cybercriminalité, dans la plus totale ignorance des contributions passées et actuelles de la criminologie à la compréhension des phénomènes criminels.

Loin d'être fataliste, cette introduction désire attirer l'attention sur l'impératif pour la criminologie de redoubler d'efforts afin de développer une compréhension plus approfondie des processus par lesquels la délinquance exploite les opportunités créées par la transition d'une société industrielle vers une société numérique. Cet article désire donc attirer l'attention sur certains aspects importants de ce processus de coévolution socio-technique. Il est organisé en cinq sections : après avoir examiné le contexte économique permettant à la cybercriminalité de devenir une activité extrêmement lucrative, on examinera dans les deux sections suivantes quelques unes des principales manifestations de la délinquance numérique en s'appuyant sur une perspective canadienne. Dans une quatrième section, nous déplacerons notre regard vers la réponse que les institutions chargées du contrôle social, la police en l'occurrence, apportent à ce problème et sur les innovations possibles en matière de régulation des déviances numériques. Finalement, la dernière partie de cet article adopte une approche prospective inspirée de la théorie des brèches[3] afin d'essayer d'identifier les technologies émergentes de la prochaine décennie qui offriront des opportunités attractives aux délinquants.

1. L'environnement économique de la cybercriminalité

D'après une récente étude menée en 2010 sur l'utilisation d'internet au Canada, autant d'usagers se sont connectés en ligne pour lire ou regarder les nouvelles (68 %) que pour réaliser des opérations bancaires

[2] Holt, T. et A. Bossler (2014). « An assessment of the current state of cybercrime scholarship », Deviant Behavior, vol. 35, no. 1, pp. 20-40.

[3] Killias, M. (2006), "The opening and closing of breaches: A theory on crime waves, law creation and crime prevention", European Journal of Criminology, vol. 3, no. 11, pp. 11-31.

(68 %), et les achats en ligne ont concerné 51 % des utilisateurs, avec une moyenne de 10 commandes annuelles totalisant un montant de 1 362 dollars par personne. Rapporté à l'échelle de la population canadienne, cela représente un marché de 15,3 milliards de dollars. Le moyen de paiement privilégié est la carte de crédit, qui est utilisée dans 89 % des transactions de commerce électronique[4].

Inventée en 1950 par l'homme d'affaires américain Frank McNamara, la carte de crédit répondit à l'avènement, après la Seconde guerre mondiale, d'une société de consommation et de tourisme de masse qui devait trouver des moyens plus efficaces que les espèces ou les chèques pour fluidifier les échanges marchands[5]. Les cartes de crédit rencontrèrent au sein de la population et auprès des commerçants un succès immédiat : les détenteurs de carte bénéficient d'une facturation différée qui leur permet de financer un style de vie à gratification instantanée, d'une protection contre la perte et le vol à un niveau prédéfini, et peuvent également accéder à des systèmes de fidélisation qui leur donnent l'impression d'obtenir une meilleure qualité de service. Pour leur part, les commerçants sont protégés contre les défauts de paiement des consommateurs, transfèrent à une tierce partie le financement des ventes ne pouvant être payées comptant, allègent leurs tâches de comptabilité, réduisent leur exposition aux risques de vol et de malversation inhérents à la manipulation des espèces et des chèques, et peuvent accéder à des informations détaillées sur les détenteurs de cartes. En 2012, on comptait au Canada 74 millions de cartes de crédit en circulation pour un volume net annuel de transactions de 356 milliards de dollars. Le volume des fraudes recensées la même année par l'Association des banquiers canadiens s'élevait à 439 millions de dollars, ce qui peut sembler considérable, mais ne représente que 1,25 % des transactions totales réalisées à l'aide de ce moyen de paiement. Il apparaît néanmoins, à la lecture de ces chiffres, que de tels profits illicites potentiels représentent pour tout fraudeur une occasion irrésistible.

Le développement très rapide de nouvelles habitudes de commerce et de banque en ligne, d'une part, et la disponibilité d'un moyen de

[4] Statistique Canada (2011). « Utilisation d'Internet et du commerce électronique par les particuliers », Le Quotidien, 12 octobre, accessible en ligne à http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-fra.htm, consulté le 6 juin 2013.

[5] Dupont, B. (2010). « La coévolution du "vol d'identité" et des systèmes de paiement », Criminologie, vol. 43, no. 2, pp. 247-268.

paiement dématérialisé qui favorise la facilité d'utilisation au détriment de la sécurité, d'autre part, expliquent en grande partie pourquoi les fraudes en ligne ont connu un tel essor au cours des dernières années.

2. L'ampleur de la cyberfraude

Les rares statistiques dont le Canada dispose sur les fraudes commises en ligne proviennent de l'Enquête sociale générale menée en 2009 par Statistique Canada, et plus particulièrement du volet sur la victimisation. Pour la première fois, des questions portaient en effet sur les actes de délinquance en ligne auxquels furent exposés les Canadiens cette année-là. Le taux de fraude bancaire par internet s'est ainsi élevé à 4 % sur des Canadiens actifs en ligne au cours des 12 mois précédents, ce qui représente 872 000 incidents. Parmi les facteurs qui augmentent les risques d'être victime de fraude bancaire en ligne figurent la fréquence d'utilisation d'internet pour effectuer des opérations bancaires et le niveau élevé de revenus. Par contre, le fait d'être francophone diminue le risque d'être victime de 25 %, ce qui peut s'expliquer par les communications essentiellement en anglais provenant de fraudeurs qui opèrent à l'échelle internationale[6]. Les achats en ligne constituent également une source importante de fraude, puisque 14 % des consommateurs qui ont procédé à de tels achats dans les 12 mois précédents le sondage ont déclaré avoir rencontré un problème causé par des moyens frauduleux ou une erreur. Ce manque de précision entre la malveillance et la négligence est pour le moins problématique, mais il représente néanmoins un peu plus de 1,7 millions d'incidents, un chiffre considérable.

Une des particularités de la fraude en ligne, par comparaison avec les modes opératoires classiques des délinquants, est la facilité avec laquelle les victimes peuvent être contactées et dépossédées de leur argent de manière automatisée. D'après la même enquête, près de 40 % des internautes canadiens ont été les destinataires en 2012 de tentatives d'hameçonnage, qui prennent la forme de courriels frauduleux qui semblent provenir d'institutions financières légitimes, mais qui contiennent en réalité des liens vers des serveurs et des sites malveillants[7]. La fréquence élevée d'apparition de ces messages frauduleux dans nos boîtes aux

[6] Perreault, S. (2011). Les incidents autodéclarés de victimisation sur Internet au Canada, 2009. Ottawa : Statistique Canada.

[7] Ibidem

lettres électroniques est inversement proportionnelle à leurs coûts de distribution, qui sont devenus quasiment nuls du fait de l'exploitation par les délinquants de réseaux d'ordinateurs infectés par des applications malveillantes appelés « botnets ». Cette automatisation à grande échelle de l'identification et de la prise de contact avec les victimes distingue clairement la cybercriminalité des formes traditionnelles de délinquance. À titre d'exemple de l'industrialisation du crime auquel nous sommes en train d'assister, l'entreprise Microsoft et le FBI ont démantelé en juin 2013 le botnet *Citadel* qui comprenait environ cinq millions de machines infectées –et donc au moins autant de victimes– situées dans 80 pays.

Il n'est donc pas surprenant de constater que les fraudes sur internet sont en train de devenir l'une des principales formes de crimes contre la propriété, devant les vols de véhicules à moteur (453 000 incidents en 2009) ou encore les introductions par effraction (630 000 incidents)[8]. Ces chiffres viennent ainsi compléter les statistiques produites à partir des crimes déclarés à la police, qui indiquent une baisse constante de la délinquance contre les personnes et contre les biens au Canada depuis le milieu des années 1990. Même s'il est pour le moment impossible de démontrer un lien direct entre la réduction de la délinquance classique et l'augmentation de la cybercriminalité au cours des vingt dernières années, l'hypothèse d'une migration de l'une vers l'autre est plausible, du moins en ce qui concerne les crimes d'acquisition.

Une autre manière de mesurer l'impact de la cybercriminalité sur la société consiste à calculer les coûts directs et indirects induits par la fraude. Cela comprend évidemment les pertes directes assumées par les victimes et leurs institutions financières, mais aussi le temps passé par ces dernières afin de réparer les dommages causés, l'érosion de la confiance que les usagers placent dans les systèmes de transaction en ligne – qui affecte négativement le développement du commerce électronique, ou encore les frais associés à l'acquisition et au déploiement de solutions de protection contre les acteurs malveillants. Il n'est pas rare de lire dans la presse généraliste ou spécialisée les résultats d'études menées par des entreprises de sécurité qui font équivaloir les coûts de la cyberfraude à ceux du trafic de drogue, avec bien entendu l'intention de frapper l'opinion publique et de renforcer ainsi la demande pour leurs produits. L'entreprise Symantec a ainsi publié en 2009 une étude qui

[8] Perreault, S, & Brennan, S. (2010). « La victimisation criminelle au Canada, 2009 », Juristat, vol. 30, no. 2. Ottawa : Statistique Canada.

estimait les coûts globaux de la cybercriminalité à mille milliards de dollars[9], sur la base d'une méthodologie assez discutable. Une étude plus rigoureuse, menée en 2012 par un groupe d'informaticiens, d'économistes et de criminologues anglais aboutissait au chiffre plus modeste, mais néanmoins non négligeable, de 67,5 milliards de dollars[10].

3. Les autres formes de cybercriminalité

Si les fraudes en ligne et le vol de propriété intellectuelle constituent la préoccupation majeure des entreprises, d'autres formes de cybercriminalité touchent les individus dans leur intégrité physique et psychologique. Dans cette catégorie, on inclut notamment la production et les échanges de pornographie juvénile, le leurre informatique ou encore la cyber-intimidation.

En ce qui concerne la pornographie juvénile sur internet, les statistiques qui permettraient de connaître l'ampleur de ce phénomène restent rares. Dans un ouvrage récent, Fortin et Corriveau signalent ainsi que la police québécoise a traité 189 plaintes en 2010, contre 102 plaintes en 2007, soit une augmentation de 85 % en quatre ans[11]. Toutefois, comme le signalent les auteurs, cette augmentation peut résulter en partie d'une meilleure sensibilisation du public à cette forme de délinquance, de procédures de déclaration plus efficaces, ou d'obligations réglementaires de dénonciation comme celle à laquelle sont soumis les fournisseurs de services internet américains. En ce qui concerne les consommateurs de pornographie juvénile, si les contenus qui les intéressent sont moins facilement accessibles que nous le supposons, notamment afin d'échapper à la surveillance des unités d'enquête policière spécialisées, ils trouvent sur internet un terrain particulièrement favorable au renforcement de leur déviance. Les forums de discussion spécialisés qui font l'apologie de ce qu'ils désignent avec euphémisme comme le *boylove* ou le *girllove*

[9] Maass, P., & Rajagopalan, M. (2012). « Does cybercrime really cost 1$ trillion? », Pro Publica, 1er août, accessible en ligne à http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion, consulté le 8 juin 2013.

[10] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). « Measuring the cost of cybercrime », 11th Annual Workshop on the Economics of Information Security, Berlin: DIW Berlin, 25-26 Juin.

[11] Fortin, F. & Corriveau, P. (2013). « Pornographie juvénile et intervention policière », in F. Fortin (dir.), Cybercriminalité : Entre inconduite et crime organisé, Montréal : Presses Internationales Polytechniques, pp. 87-114.

permettent ainsi aux producteurs et aux consommateurs de pornographie juvénile de se constituer en communautés virtuelles qui développent des argumentaires de nature historique, sociologique et psychologique pour justifier ce type de pratiques et transmettre à leurs membres les plus novices des techniques qui leur éviteront d'attirer l'attention de la police[12].

Le leurre informatique est une infraction du Code Criminel (art. 172.1) qui désigne les communications informatiques initiées par un adulte avec un mineur afin de commettre un crime sexuel. La crainte matérialisée par cette incrimination créée en 2002 concerne une plus grande accessibilité à des victimes potentielles que l'internet conférerait aux prédateurs sexuels[13]. Face à la multiplication des plateformes électroniques permettant aux enfants et aux adolescents de communiquer et de partager des informations personnelles avec un nombre potentiellement illimité d'interlocuteurs à l'identité parfois incertaine, et de la difficulté pour leurs parents de superviser ces activités en ligne, la possibilité de rencontres avec des adultes mal intentionnés dans le cyberespace comme éléments précurseurs de crimes sexuels est devenue une préoccupation majeure de l'opinion publique. Au Canada, les statistiques officielles des services de police laissent penser que le leurre d'enfant fait partie des crimes qui connaissent l'une des plus fortes hausses (+10 % en 2011), dans un contexte de baisse généralisée de la délinquance[14]. Cependant, les crimes sexuels représentent l'une des catégories de crimes les moins déclarés à la police par les victimes, et il se peut que cette hausse reflète plus une augmentation du taux de déclarations que du nombre réel de crimes commis. En effet, une étude menée aux États-Unis indique que la grande majorité des victimes sont des adolescentes de 13 à 15 ans (75 % des cas) qui rencontrent leurs agresseurs en sachant pertinemment que ces derniers sont des adultes à la recherche d'une relation sexuelle, et que seulement 5% des cas impliquent le recours à la violence de la part des adultes incriminés[15]. La principale leçon à tirer de cette recherche est que

[12] Ibidem

[13] Loughlin, J., & Taylor-Butts, A. (2009). « Leurre d'enfants par internet », Juristat, vol. 29, no. 1. Ottawa : Statistique Canada.

[14] Brennan, S. (2011). Statistiques sur les crimes déclarés par la police au Canada, 2011. Ottawa : Statistique Canada.

[15] Wolak, J., Finkelhor, D., & Mitchell, K. (2004). « Internet-initiated sex-crimes against minors: Implications for prevention based on findings from a national study », Journal of Adolescent Health, vol. 35, no. 5, pp. 424.e11-424.e20.

la prévention du leurre d'enfant doit avant tout passer par la sensibilisation aussi bien des adolescents qui y sont exposés, par une meilleure compréhension de tous les risques associés à ce type de rencontres, que de leurs parents, dont les pratiques de supervision dans l'utilisation d'internet sont déterminantes.

Le dernier thème abordé dans cette section concerne la cyberintimidation qui est fréquemment mise en lumière par les médias lors des suicides tragiques d'adolescents qui y sont exposés dans l'établissement d'enseignement qu'ils fréquentent. Les définitions de la cyberintimidation ne font pas consensus, mais nous nous contenterons ici de préciser qu'il s'agit du prolongement sur les plateformes numériques de comportements d'intimidation et de harcèlement qui portent atteinte à l'intégrité psychologique de la personne qui en est la victime. De nombreux auteurs estiment que la dimension numérique de la cyberintimidation introduit un certain nombre de caractéristiques qui accentuent la gravité de ce type de comportements. L'anonymat et la distance physique qui existent entre les utilisateurs des différentes plateformes de communication en ligne vont, par exemple, lever les inhibitions et diminuer le niveau général d'empathie en cas de conflit. Par ailleurs, les auteurs d'actes de cyberintimidation vont pouvoir diffuser leurs commentaires injurieux, des rumeurs désobligeantes ou encore des photos ou des vidéos humiliantes auprès d'audiences potentielles de milliers, voire de millions de personnes. Enfin, alors que les formes traditionnelles d'intimidation s'arrêtaient aux portes du domicile familial, qui constituait un refuge pour les victimes, la cyberintimidation implique une accessibilité accrue à ces dernières, qui peuvent y être exposées en tout lieu et en tout temps par leur téléphone intelligent, tablette électronique ou ordinateur personnel[16]. Les études menées sur la prévalence de la cyberintimidation auprès d'échantillons d'adolescents au Canada, aux États-Unis, au Royaume-Uni et en Australie livrent des résultats qui oscillent entre 14 % et 73 % de répondants qui déclarent en avoir été victimes[17].

L'enquête de victimisation conduite en 2009 comprenait quelques questions sur la cyberintimidation au sein du ménage. Il en ressort que 9 % des ménages où vivait un enfant avaient connaissance de cas de cyberintimidation, mais que ce chiffre montait à 41 % pour les ménages ayant un

[16] Ryan, N. (2013). « Intimidation à l'heure d'internet », in F. Fortin (dir.), Cybercriminalité : entre inconduite et crime organisé, Montréal : Presses Internationales Polytechniques, pp. 157-179.

[17] Ibidem

enfant âgé de 12 ou 13 ans, qui constitue la tranche d'âge la plus touchée. Les victimes étaient en majorité des filles (71 %), et seulement 14 % des cas connus étaient déclarés à la police[18], ce qui laisse penser que la cyberintimidation est principalement traitée à l'intérieur de la cellule familiale ou en lien avec des intervenants issus du milieu scolaire.

4. Le rôle de la police en matière de cybersécurité

Les chiffres présentés dans le paragraphe précédent, mais aussi dans la section sur la cyberfraude, laissent penser qu'une infime minorité seulement des cybercrimes sont rapportés de la police, alors qu'ils représentent une part sans cesse croissante de la délinquance globale. Ce constat d'un chiffre noir de la cybercriminalité n'est en soi pas nouveau, puisque les enquêtes de victimisation font régulièrement ressortir le décalage entre les crimes déclarés à la police et le nombre d'incidents criminels dont sont réellement victimes les répondants. Les principaux motifs d'une absence de signalement à la police comprennent la gravité de l'incident jugée mineure, le sentiment que la police ne sera pas en mesure de faire quelque chose, l'existence d'un mode de règlement alternatif de l'incident, le refus d'entrer en contact avec la police, l'impossibilité de se faire rembourser par les assurances, le manque de confiance dans le système pénal ou encore la peur de représailles de la part du contrevenant[19]. Dans le cas de la cybercriminalité, des défis technologiques et organisationnels supplémentaires viennent de plus limiter les capacités de la police à intervenir de manière efficace contre cette nouvelle forme de délinquance.

Tout d'abord, les ressources financières et humaines affectées à la cybercriminalité restent encore tout à fait insuffisantes pour traiter un volume d'affaires en croissance constante. En 2006, la Presse Canadienne recensait ainsi 245 enquêteurs spécialisés en cybercriminalité pour l'ensemble du Canada, ce qui représentait alors 0,4 % des effectifs policiers[20]. La situation est sensiblement la même en France, où la Gendarmerie Nationale dispose à titre d'exemple d'une soixantaine d'ingénieurs et de 250 enquêteurs en technologies numériques, pour des

[18] Perreault, S. (2011).

[19] Perreault, S. & Brennan, S. (2010).

[20] Presse Canadienne (2006). « La police ne peut presque rien faire pour retracer les tueurs sur internet », La Presse, 14 septembre.

effectifs totaux de 98 000 employés[21]. Même si ces effectifs ont doublé ou triplé au cours des sept dernières années, ils restent encore tout à fait insuffisants pour répondre aux besoins d'une délinquance qui représente maintenant près du tiers des crimes contre la propriété et qui joue un rôle de plus en plus significatif dans les crimes contre la personne. À bien des égards, le modèle policier dominant, imaginé à la fin du 19ème siècle pour maintenir l'ordre public dans le contexte des profondes transformations sociales initiées par les deux révolutions industrielles semble avoir de grandes difficultés à s'adapter au passage à l'ère numérique des sociétés contemporaines. Alors que le travail policier reste territorialement ancré dans des juridictions locales ou nationales, la cybercriminalité s'affranchit des contraintes géographiques pour déployer ses réseaux à l'échelle planétaire. Cela implique le recours, par les organismes d'application de la loi, à des mécanismes de coopération internationale qui restent encore marginaux et limités par des cadres juridiques nationaux fragmentés qui n'ont pas encore été harmonisés. Une alternative serait certainement de déléguer une part des responsabilités en matière de lutte contre la cybercriminalité aux policiers de première ligne, ce qui soulagerait les unités spécialisées d'enquête et leur permettrait de se concentrer sur les affaires les plus complexes. Toutefois, ce changement radical impliquerait une refonte de la formation initiale reçue par les jeunes recrues, qui reste encore essentiellement consacrée aux techniques de patrouille automobile et d'usage de la force, à la connaissance du droit criminel et à la gestion bureaucratique des dossiers. Il résulte de ces limites organisationnelles que la grande majorité des ressources d'enquête disponibles se consacre aux affaires de pornographie juvénile produite et échangée sur internet, qui sont considérées, sur une échelle de gravité, comme prioritaires par rapport à l'ensemble des autres cybercrimes.

Un autre modèle particulièrement prometteur en matière de prévention et de lutte contre la cybercriminalité est celui des partenariats avec les acteurs privés. En effet, l'infrastructure technique de l'internet est entièrement contrôlée par le secteur privé, qu'il s'agisse des hébergeurs qui accueillent les sites des grandes entreprises et des organismes gouvernementaux sur leurs serveurs, des fournisseurs d'accès qui commercialisent

[21] Rastello, C. (2013). « Cyberpatrouilleurs et cyberinfiltreurs, les nouveaux experts », Le Nouvel Observateur, 28 janvier, accessible en ligne à http://tempsreel.nouvelobs.com/societe/20130127.OBS6831/cyberpatrouilleurs-et-cyberinfiltreurs-les-nouveaux-experts.html, consulté le 4 décembre 2013.

les abonnements au réseau à des usagers individuels, ou encore des grands opérateurs de télécommunication qui font circuler le trafic de données entre les continents. De même, de grandes entreprises multinationales comme Microsoft, Apple, Visa, Mastercard, Google ou Facebook détiennent des positions dominantes dans leur secteur d'activités qui leur donnent un rôle déterminant dans le renforcement (ou l'érosion) de la sécurité en ligne. Ainsi, une étude menée pour le compte de Sécurité Publique Canada en 2013 fait apparaître que les pays qui ont développé des partenariats entre agences gouvernementales, fournisseurs d'accès à internet et entreprises de sécurité informatique arrivaient à réduire de manière importante les taux d'infection des botnets parmi leurs internautes[22]. Au Canada, l'opération Chapitre qui aboutit au démantèlement en mai 2012 d'un réseau sophistiqué de 61 fraudeurs à la carte de crédit par la GRC, le SPVM et la SQ est le résultat d'une étroite collaboration avec l'Association des banquiers canadiens et les services d'enquêtes des principales banques du pays durant près de quatre ans. Cette approche partenariale, qui a pour immense avantage de faire bénéficier les services de police d'une expertise technique avancée et de renseignements privilégiés, nécessite cependant des ajustements de la part des organismes d'application de la loi. En effet, ces derniers ne doivent plus se limiter à considérer leur rôle comme celui de détenteurs exclusifs d'une expertise en matière d'enquête sur les cybercrimes, mais plutôt comme les coordonnateurs d'un vaste réseau de sécurité dont le mandat serait de garantir l'intégrité de l'écosystème numérique[23]. Ce rôle de coordonnateur implique le développement d'un vaste répertoire de stratégies de persuasion, mais aussi de coercition, afin de créer une structure d'incitatifs diversifiés qui favoriserait la collaboration d'acteurs aux intérêts parfois divergents[24]. Ce modèle de sécurité distribuée ou en réseau possède aussi l'immense avantage de conférer aux organisations policières une meilleure visibilité face aux formes émergentes de cybercriminalité, qui sont en général plus rapidement détectées par les acteurs privés, puisqu'elles découlent souvent de l'exploitation par les délinquants de leurs propres innovations techniques ou commerciales.

[22] Dupont, B. (2013). An international comparison of anti-botnet partnerships. Ottawa: Sécurité Publique Canada – Direction Nationale de la Cybersécurité.

[23] Dupont, B. (2004). « Security in the age of networks », Policing and Society, vol. 14, no. 1, pp. 76-91.

[24] Mazerolle, L., & Ransley, J. (2005). Third party policing. Cambridge: Cambridge University Press.

5. Tendances émergentes et futures en matière de cybercriminalité

S'il est toujours hasardeux de tenter de prédire l'avenir, un certain nombre de tendances technologiques qui ont atteint divers degrés de maturité laissent entrevoir quelques-uns des défis auxquels les institutions chargées d'assurer la cybersécurité seront confrontées au cours des dix prochaines années. Un récent rapport réalisé en partenariat avec Sécurité Publique Canada recense neuf tendances sociotechniques dérivées d'une analyse approfondie de la littérature spécialisée[25]. La suite de cette section présente de manière succincte ces tendances, ainsi que leurs implications:

1. L'informatique dans les nuages (ou infonuagique) permet aux organisations publiques et privées de sous-traiter, à des entreprises spécialisées, la maintenance de ressources informatiques qui sont rendues disponibles à la demande. Les particuliers ont également accès à ce type de services par l'intermédiaire de fournisseurs tels que Dropbox ou Google Drive. En 2020, il est probable que le tiers des données informatiques mondiales transiteront par des systèmes administrés dans les nuages. Si elle offre de nombreux avantages aux usagers, l'infonuagique représente également un casse-tête en matière de cybersécurité, car les données ne sont plus sous le contrôle exclusif des entreprises et des services publics lorsqu'elles sont hébergées dans les nuages. En cas de piratage informatique, la concentration des données de nombreuses organisations dans de gigantesques « fermes de serveurs » crée également un risque accru de compromission massive d'informations confidentielles. Par ailleurs, la mondialisation de ce type de services, à la recherche permanente de l'installation d'une présence dans les pays aux coûts les plus bas, posera rapidement des problèmes importants aux enquêteurs spécialisés en informatique judiciaire, qui devront recueillir et analyser des preuves hébergées dans les nuages à l'étranger.

[25] Dupont, B. (2012). L'environnement de la cybersécurité à l'horizon 2022 : Tendances, moteurs et implications. Ottawa : Sécurité Publique Canada – Direction Nationale de la Cybersécurité.

2. Le terme « données massives » (big data) reflète l'apparition ces dernières années de fichiers de données qui contiennent des volumes gigantesques d'informations non structurées ou disparates. Pour les entreprises, ces flux massifs prennent la forme de données relationnelles internes qui proviennent des interactions avec les clients ou les fournisseurs via les sites internet ou les centres d'appel, de résultats de sondages et d'enquêtes démographiques, de coordonnées de géolocalisation mises à jour en temps réel, de toute information produite par un équipement numérique, mais aussi de contenus externes en provenance des sites de socialisation en ligne. Cette prolifération des données personnelles permet aux entreprises de profiler de manière toujours plus précise les individus, leurs habitudes et leurs envies, ce qui rend la notion traditionnelle de vie privée obsolète. Par ailleurs, le processus d'amalgamation et de réutilisation des données pour des analyses répétées engendre un phénomène d'éparpillement d'où résulte que la traçabilité des données, et particulièrement celles qualifiées de sensibles, devient de plus en plus difficile à établir. Cela multiplie donc les vulnérabilités, et par conséquent les opportunités pour les délinquants de s'emparer de grandes quantités de données personnelles potentiellement très profitables.

3. L'internet des objets fait référence à l'interpénétration croissante entre le monde physique et le monde numérique, par le moyen de capteurs et de senseurs intégrés aux objets qui nous entourent (des véhicules automobiles aux pacemakers en passant par les réfrigérateurs et les compteurs électriques), avec la capacité pour ces derniers de communiquer sans fil avec des réseaux informatiques. L'augmentation du nombre d'entités connectées à internet va mathématiquement augmenter le nombre de cibles disponibles pour les pirates informatiques, qu'il s'agisse de voitures, d'instruments médicaux, ou d'appareils domotiques. Cela sera d'autant plus aisé que les concepteurs et fabricants de ces objets connectés ne souhaiteront (ou ne pourront) probablement pas les équiper de dispositifs de sécurité trop contraignants afin de maintenir des coûts de production et de fonctionnement aussi bas que possible, avec pour conséquence de fragiliser l'internet dans son ensemble.

4. Le concept d'internet mobile désigne l'ensemble des technologies qui permettent l'accès à internet à l'aide d'appareils mobiles tels que des téléphones intelligents ou des tablettes électroniques (de type iPad). Pour l'année 2012, l'entreprise IDC prévoyait qu'il se vendrait deux fois plus d'appareils mobiles (895 millions d'unités) que d'ordinateurs classiques (400 millions d'unités). Les consommateurs profitent et profiteront des capacités techniques des téléphones intelligents et des appareils mobiles, combinées aux services offerts par les entreprises, pour effectuer des transactions financières ou bancaires en ligne, où qu'ils se trouvent et en tout temps. Au Canada, ce sont déjà 33 % des propriétaires de téléphones intelligents qui s'en servent pour consulter leur compte bancaire en ligne, et 16 % pour procéder à des paiements électroniques. Toutefois, les pratiques de sécurité qui sont maintenant courantes pour les ordinateurs, comme l'installation d'un logiciel antivirus, ne sont pas encore systématiquement appliquées aux téléphones intelligents et aux tablettes, qui sont trop souvent perçus par les utilisateurs comme des outils de communication et non comme des équipements informatiques. Cette technologie offre des perspectives particulièrement attrayantes pour les cybercriminels.

5. Les interfaces neuronales directes sont des technologies qui permettent de connecter directement des dispositifs informatiques externes au cerveau humain. Cela permet ainsi aux individus d'interagir avec des ordinateurs par la pensée. Les interfaces neuronales directes ouvrent la voie à de nouveaux risques de piratage du cerveau, d'autant plus que les effets à long terme de ces interfaces sur les sujets humains et les changements de personnalité qu'elles provoquent restent très mal connus. Nous pourrions alors envisager des attaques lancées depuis l'écosystème numérique, à partir d'ordinateurs, vers des cibles humaines, et qui auraient pour conséquences directes des lésions psychologiques ou physiques durables. Il est aussi possible que ces technologies soient utilisées comme substituts aux produits stupéfiants actuellement disponibles, et que de nouveaux marchés criminels similaires à ceux de la drogue offrent des expériences inédites d'addiction.

6. La technologie des paiements sans contact (NFC) exploite diverses technologies de communication sans fil afin de faciliter les transactions financières aux points de vente. Cette technologie est principalement installée sur des cartes de paiement et des téléphones mobiles,

qu'il suffit d'approcher à quelques centimètres d'un appareil récepteur équipé pour effectuer la transaction, ce qui accélère considérablement le passage aux points de vente. Les implications pour la cybersécurité sont très similaires à celles déjà soulevées pour l'internet mobile, mais, de plus, un problème de sécurité additionnel relève de la transmission non sécurisée de données bancaires qui entraîne un risque d'interception et de manipulation par des tiers malveillants. La technologie n'est en effet pas conçue pour des applications liées à la transmission de données sensibles.

7. La robotique mobile fait référence à des systèmes mécaniques polyarticulés capables de se déplacer de manière autonome ou semi-autonome et ayant la capacité d'influencer leur environnement immédiat. La robotique mobile se retrouve dans un nombre croissant de secteurs d'activités, comme les industries manufacturières, mais aussi les entreprises de services, le secteur de la santé, ainsi qu'en remplacement des humains afin de remplir des tâches dangereuses. Dans la mesure où les communications avec les robots mobiles reposeront sur des technologies sans fil, la multiplication de ces machines dans l'espace public va générer des opportunités pour leur prise de contrôle malveillante par des pirates informatiques. La multiplication de robots autonomes dans l'espace public va également faire apparaître de nouveaux risques pour la sécurité des individus, notamment si des robots adoptent des comportements indésirables ou commettent des erreurs à l'origine d'accidents.

8. L'informatique quantique s'appuie sur les lois de la mécanique quantique afin de traiter de grands volumes d'informations de manière beaucoup plus efficace que l'informatique traditionnelle. Pour l'instant, l'informatique quantique reste essentiellement au stade théorique, même si des solutions très spécifiques de cryptographie quantique sont déjà disponibles sur le marché. Les rares ordinateurs fabriqués restent confinés dans les laboratoires des grandes universités et des entreprises qui mènent des recherches dans ce domaine. L'informatique quantique trouve sa principale application en cybersécurité dans le domaine de la cryptanalyse (le déchiffrement de messages cryptés sans clé), puisque sa puissance de calcul permettrait, a priori, de casser sans grande difficulté les clés de chiffrement les plus puissantes et rendrait toute communication fondamentalement vulnérable. Ce type d'outil restera

toutefois principalement utilisé par les pirates informatiques qui travaillent pour le compte d'agences de renseignement gouvernementales.

9. Finalement, la militarisation de l'internet reflète l'évolution de la doctrine militaire, qui fait du contrôle de l'internet non seulement un enjeu de sécurité intérieure, mais aussi de sécurité nationale avec une multiplication des ressources consacrées au développement de capacités défensives et offensives. Le virus Stuxnet développé par les gouvernements américain et israélien afin de perturber le fonctionnement d'une usine iranienne d'enrichissement d'uranium est un exemple typique de cette tendance. La multiplication des capacités offensives décrites précédemment contribuera également à augmenter l'insécurité de l'internet par la prolifération incontrôlable d'armes numériques toujours plus sophistiquées. En effet, l'architecture ouverte et distribuée d'internet implique qu'une fois utilisées, ces armes numériques peuvent être analysées et recyclées par tous ceux qui disposeront de capacités techniques suffisantes de rétro-ingénierie. Dans l'écosystème particulier de l'internet, des applications malveillantes élaborées à des fins de sécurité nationale peuvent ainsi se retrouver rapidement entre les mains d'intérêts criminels, ce qui a déjà été observé avec le virus Stuxnet. En décembre 2010, des failles encore inconnues utilisées par ce virus sont apparues dans l'application malveillante TDL-4, un des plus importants botnets en fonctionnement à cette période.

Conclusion

Si la dernière section de cet article comprend inévitablement une dimension fortement spéculative, il ne fait aucun doute que les délinquants sauront pleinement exploiter les nouvelles activités routinières des usagers d'internet, ainsi que les brèches qui s'ouvriront du fait de la commercialisation de biens et de services technologiques innovants[26]. L'exercice de cartographie prospective de la topologie des risques numérique esquissé plus haut fait toutefois ressortir une dimension nouvelle, qui est la convergence et l'entrelacement de technologies issues de secteurs industriels disparates. La frontière qui semblait distinguer le monde

[26] Killias, Op. Cit.; Cohen, L. et M. Felson (1979). "Social change and crime rate trends: A routine activity approach", American Sociological Review, vol. 44, no. 4, pp. 588-608.

social des humains du monde technique des machines, et qui s'incarnait par exemple dans une terminologie prolixe en préfixes tels que l'omniprésent 'cyber', destiné à renforcer cette démarcation, est en train de disparaître au profit d'assemblages hybrides où machines et humains interagissent de manière intégrée, produisant des flux de données dont l'utilité et la valeur restent encore incertains. Lorsque les robots autonomes occuperont une place croissante dans les espaces publics et côtoieront quotidiennement les humains, que des capteurs neuronaux permettront aux machines d'enregistrer et d'interpréter les pensées de ces derniers, que des objets tels les téléphones intelligents se transformeront en moyens de paiement, ou encore que l'internet des objets permettra le déploiement d'une nuée de senseurs facilitant la surveillance des moindres activités humaines, les cadres règlementaires propres à chaque sphère technologique et sociale entreront en collision. Le droit criminel, le droit des transports, le droit relatif à la protection de la vie privée, le droit commercial, le droit de la guerre ou encore les normes éthiques applicables aux activités médicales, pour ne prendre que quelques exemples, se verront connectés par des interdépendances inédites. Les nouveaux paramètres régulatoires qui émergeront de cette convergence socio-technique mobiliseront naturellement une expertise juridique pour tenter d'en saisir la portée, mais il reviendra également à la criminologie de se pencher sur ces transformations. En effet, ces évolutions devront non seulement prendre en compte l'élargissement et de la complexification des phénomènes criminels, mais aussi inspirer une conceptualisation renouvelée des modalités de mise en œuvre du contrôle social. Le rôle que l'institution policière sera amenée à jouer dans cette nouvelle architecture des risques semble marginal, à moins d'une réforme en profondeur, et ce sont donc les entreprises privées, en réseau avec diverses autorités nationales et internationales de régulation, ainsi qu'avec les agences de renseignement et les forces armées, qui assumeront l'essentiel des responsabilités en matière de prévention et de contrôle de la cybercriminalité—au risque de nous replonger dans un modèle féodal de contrôle socio-technique où l'État aura été dépouillé de sa fonction régalienne de protection des citoyens. Il nous paraît dans ce contexte indispensable que la criminologie se lance dans un effort soutenu d'analyse des configurations que prendront ces nouveaux dispositifs de sécurité numérique, ainsi que de leurs retombées sur les pratiques et les libertés individuelles, sans perdre de vue l'impératif normatif de justice, de transparence et d'équité qui anime notre discipline.

Summary

This article discusses several ideas on the socio-technical coevolution process that is characterized by the illegal exploitation of digital revolution technologies such as mobile telecommunications, the internet, robotics, big data, etc. It is organized in five sections: after having examined how the economic context makes cybercrime an extremely lucrative activity, the two following sections outline some of the main expressions of online offending, from a Canadian perspective. In a fourth section, the response of law enforcement institutions to this problem is analysed, as well as possible regulatory innovations in this field. Finally, the last section of this article adopts a forecasting approach partly inspired from the theory of breaches to try to identify emerging technologies that will generate criminal opportunities in the next decade.

Résumé

Cet article présente un certain nombre de réflexions sur le processus de coévolution socio-technique qui voit les technologies issues de la révolution numérique (téléphonie sans fil, internet, robotique, big data, etc.) faire l'objet d'exploitations systématiques à des fins délinquantes. Il est organisé en cinq sections : après avoir examiné le contexte économique permettant au cybercrime de devenir une activité extrêmement lucrative, on aborde dans les deux sections suivantes quelques-unes des principales manifestations de la délinquance numérique en s'appuyant sur une perspective canadienne. Dans une quatrième section, nous déplacerons notre regard vers la réponse que les institutions chargées du contrôle social, la police en l'occurrence, apportent à ce problème et sur les innovations possibles en matière de régulation des déviances numériques. Finalement, la dernière partie de cet article adopte une approche prospective inspirée de la théorie des brèches afin d'essayer d'identifier les technologies émergentes de la prochaine décennie qui offriront des opportunités attractives aux délinquants.

Resumen

En este artículo se presenta una serie de reflexiones sobre el proceso co-evolución socio-técnico que ve las tecnologías de revolución digital (inalámbrica, internet, la robótica, Big Data, etc.) ser utilizadas sistemáticamente para delincuentes. Está organizado en cinco secciones: para empezar, después de haber presentado el contexto económico que convierte la cyber-criminalidad en un actividad extremadamente lucrativa, se abordan en las dos secciones siguientes algunas de las principales manifestaciones de la crimen digital basada en una perspectiva canadiense. En un cuarto apartado, vamos a estudiar la respuesta de las instituciones de control social, la policía en particular. En este caso, abordaremos la cuestión de las posibles innovaciones en la regulación de la desviación digital. Por último, la última parte de este artículo adopta un enfoque pro-activo inspirado en la teoría des "brèches" en un intento de identificar tecnologías emergentes de la próxima década que crearan oportunidades atractivas para los delincuentes.