Le crime comme moyen de contrôle du cyberespace commercial

Criminologie, 39 (1), 63-81.

Article pour le numéro spécial de *Criminologie* sur le cybercrime
sous la direction de Marc Ouimet et Stéphane Leman-Langlois

5 970 mots
mots-clés : cybercrime; cyberterrorisme, criminologie, contrôle social, commerce électronique, criminalité, droit

Résumé

Cet article tente de clarifier la notion de cybercrime et de la situer dans un cadre criminologique où elle pourrait être utile dans la compréhension du processus d'incrimination de nouvelles conduites et de l'organisation de la réponse organisationnelle et individuelle à la criminalité. En limitant la catégorie de cybercriminalité aux conduites faisant appel aux réseaux informatiques des questions intéressantes sont soulevées au sujet du concept d'opportunité criminelle, de dommage, de victimisation, etc.

Abstract

This paper analyses the notion of "cybercrime" from a criminological point of view and proposes a number of ways in which it can be useful in the study of criminalisation and the organisation of official, organisational and individual responses. "Cybercrime" is defined as the use of computer networks in activities defined as criminal. This definition raises new questions regarding opportunity, harm, victimisation and other related concepts.

Introduction

Comme bien des sujets « chauds » de l'actualité, la notion de cybercrime est un puzzle formé de pièces hétéroclites produisant une image distordue dans laquelle il est de plus en plus difficile de différencier la réalité de la fiction. Dans la littérature spécialisée, les travaux de qualité très inégale s'accumulent, fixés au tracteur des mass-médias fascinés par l'effet « peur, incertitude et doute » (*Fear, Uncertainty and Doubt*, FUD; expression inventée par un cadre d'IBM pour décrire les tactiques de marketing de la compagnie visant à réduire la confiance que les clients potentiels avaient dans des technologies concurrentes) causé par des changements sociaux fondamentaux qui paraissent comme une conséquence inéluctable de l'adoption massive d'une technologie aussi puissante que mal comprise. Pour l'instant, l'immense majorité de ce qui a été écrit sur le cybercrime provient ou bien du secteur de la sécurité informatique ou de l'analyse juridique (Beardwood, 2003; Brenner, 2004).

L'exemple du « cyberterrorisme » illustre particulièrement bien la disproportion qui peut exister entre la quantité d'encre utilisée et le nombre infinitésimal d'actes empiriquement observables. Dans ce cas, tous les éléments de la panique morale classique (Cohen, 2003) sont réunis : des experts qui font la liste des vulnérabilités et offrent des explications sur les motivations de cyberterroristes éventuels (comme Branigan, 2005, Clarke, 2005 ou Furnell, 2005), des policiers et bureaucrates expliquant leurs préparatifs (MSP, 2004), une attention médiatique de plus en plus grande à la fois dans l'actualité et dans le divertissement (jeux comme *Splinter Cell*, séries télévisées comme *24*) et un public confondant de plus en plus les *hackers*, les *hacktivists*, les *crackers*, les pirates et les cyberterroristes (Thatcher, 2005). Ceci est peu surprenant puisque la construction de la menace par les gouvernements passe par l'amalgamation de nouvelles conduites au caractère flou à d'autres qui sont traditionnellement considérées comme des crimes. Le résultat est la construction sociale d'une menace exotique, internationale, diffuse et touchant chaque individu. À ce jour, bien peu de chercheurs se sont penchés sur cette question et ceux qu'il l'ont fait n'ont aucunement remis en question la notion de cybercrime elle-même (par exemple, Etter, 2001; Denning, 1999; Speer, 2000).

Le but premier de cet article est de différencier et de classer les différentes conduites identifiées sous le vocable de « cybercrime » selon une approche criminologique pour permettre une meilleure compréhension de leurs facettes techniques et politiques. Les criminologues s'intéressant au processus d'incrimination et de réaction sociale seront particulièrement intéressés par les difficultés soulevées par la définition des actes subsumés sous la catégorie « cybercrime » et par les activités des principaux acteurs tentant de tirer leur épingle du jeu juridique.

1. Les formes de « cybercriminalité » et de « cybercrime »

Commençons par dresser une carte plus rationnelle et surtout plus claire du phénomène — ou, en fait, *des* phénomènes objectifs couramment rassemblés sous l'étiquette de « cybercriminalité ». Pour ce faire, tournons-nous d'abord vers le vocable lui-même, qui renvoie à deux concepts fondamentaux. Le premier est la notion de criminalité ou de crime. Inutile de souligner ici les sempiternelles difficultés que la criminologie a pu avoir avec cette notion, qui sont ici multipliées. Nous pouvons toutefois remarquer d'emblée que tous les cybercrimes ne sont pas aussi avant-gardistes qu'il n'y paraît à première vue. On trouve bien sûr dans ce grand sac des conduites parfaitement nouvelles, sans aucune commune mesure avec des crimes établis de longue date par le droit traditionnel. Pensons par exemple à la criminalisation de la mise en échec d'une technologie anti-copie, introduite par le *Digital Millennium Copyright Act* (DMCA) étatsunien (Lessig, 2002) et en voie d'être adoptée par de multiples autres États, dont le Canada. À la fois, d'autres formes de cybercrime sont de nouvelles versions de crimes qui existaient bien avant l'avènement de l'informatique. Cette oscillation entre la nouveauté et le conventionnel soulève une certaine confusion quant à la nature du concept de cybercrime au niveau théorique-sociocriminologique. Ainsi, une première question importante semble

s'imposer : les conduites identifiées sous le vocable de « cybercriminalité » sont-elles réellement nouvelles ?

La deuxième partie du vocable fait référence à l'informatique, à travers un vocabulaire inventé par l'écrivain de science-fiction William Gibson, connu pour avoir lancé la vague *cyberpunk* avec son livre *Neuromancer* (1984). Gibson est le père de l'expression « *cyberspace* », ou cyberespace et, en quelque sorte, le parrain du lexique foisonnant des cyber-mots et phrases, dont bien sûr « cybercriminalité ». Il est désormais inutile de s'étendre bien longtemps là-dessus : le cyberespace s'oppose à l'espace conventionnel au sens où il est affranchi de toute localisation physique ou géographique. Ce n'est pas un endroit mais un point de rencontre de flux informationnels portés par des réseaux informatiques interconnectés. En fait, c'est une notion assez proche de celle de « site » utilisée dans certaines approches sociologiques. Comme nous le verrons plus tard, il existe certaine parenté entre ce cyberespace et l'« espace » culturel où ont toujours été construites les notions de criminalité, de criminel, de droit, de responsabilité, de bien, de mal, etc. Dans le cyberespace, les actes, les objets, les personnes ne sont qu'information, ce qui a des conséquences multiples et profondes sur les activités qui peuvent s'« y » dérouler — conséquences jusqu'ici peu examinées.

Si rien ne nous oblige à respecter la conception gibsonnienne des réseaux informatiques, le faire peut nous être très utile. En premier lieu, il est particulièrement important de faire une différence entre le simple « crime par ordinateur » (ou, ce qui est plus vague encore, « à l'aide d'un ordinateur ») et le « cybercrime ». Le premier est une catégorie trop large comprenant toute forme d'incrimination impliquant l'utilisation d'un ordinateur — la possession de pornographie juvénile numérique ou de logiciels piratés, la reproduction de cartes de crédit ou le maintien d'une liste de clients de substances illicites, par exemple. On le voit bien, l'omniprésence des ordinateurs (par exemple, la différence entre ordinateurs, agendas électroniques et téléphones portables va en s'amenuisant), rendra cette expression caduque, ou redondante, d'ici peu. Réservons donc le vocable de « cybercrime » aux actes impliquant l'utilisation de *réseaux* informatisés, Internet principalement.

Évidemment, dans son usage courant, le mot « cybercrime » ne fait référence à aucune virtualité : on n'utilise jamais l'expression pour mettre en doute ni l'existence concrète des actes ni leur « nature » criminelle. Il est donc primordial de se demander si le préfixe « cyber » ajoute quelque chose à notre compréhension du phénomène, mise à part son intégration au panthéon de la jargonnerie médiatique. À ce niveau, il semble utile de tenir compte du rôle des réseaux informatiques dans différentes formes de crime. Dans certains cas, ils sont simplement accessoires à la commission d'un acte criminalisé, alors que dans d'autres, ils se trouvent au coeur même des activités visées — qui seraient irréalisables, voire impossibles à conceptualiser dans un monde non « branché ».

La suite de cette section est structurée autour d'une typologie de la cybercriminalité objective fondée sur ces deux questions. Le tableau 1 résume cette structure, fondée sur a) l'époque de l'incrimination des actes, selon qu'elle précède ou suit l'arrivée d'Internet, et b) la fonction des réseaux dans la forme

que prennent les actes. Dans ce second cas, il s'agit de différencier entre i) les cas où l'existence des réseaux ou du « cyberespace » déclenche ou rend possible les actes incriminés; ii) les cas où elle accélère ou décuple la gravité ou la fréquence des actes et iii) les autres cas où le côté « cyber » est un simple accessoire. Quelques analyses ont déjà utilisé la variable « rôle » (Wall, 2003) mais en laissant de côté la question de la criminalisation, pourtant cruciale dans l'exploration de conduites présentées comme nouvelles ou sans précédent. D'autres, surtout dans les études juridiques, divisent le cybercrime selon que l'ordinateur est *cible*, *outil* ou *périphérique* à la commission du délit (un des premiers fut Carter, 1995). Ceci ne cadre pas avec la réalité, où « cible » et « outil » sont souvent indissociables.

Tableau 1 : la cybercriminalité en fonction des incriminations et de l'impact des réseaux

réseaux / cyberespace ont un rôle :	incrimination des actes	
	traditionnelle (pré-Internet)	émergente/imminente (post-Internet)
déclencheur	(non applicable)	attaques distribuées; vandalisme virtuel
multiplicateur	pornographie juvénile; vol d'identité; fraudes; incitation à la haine	échange de fichiers; pourriels
accessoire	appâter des victimes; terrorisme et sabotage	terrorisme (support)

On le comprendra, notre approche ne vise pas à évaluer la gravité, la prévalence ou encore l'efficacité ou le bien-fondé du contrôle ce ces conduites. Il s'agit plutôt de tenter de cerner la nature de l'objet « cybercrime » et de le mettre en perspective. Pour donner une idée de la prévalence de ce type de criminalité, notons que le Service de police de la Ville de Montréal (SPVM) a fait enquête sur 200 cybercrimes en 2001, la Sûreté du Québec (SQ) sur 309 (dont certains en collaboration avec le SPVM) et la Gendarmerie Royale du Canada (GRC) sur 800 (Statistique Canada, 2002). L'impact semble donc minime. Cependant ces statistiques sont moins intelligentes qu'il ne paraît, flottant sur des définitions variables et douteuses de leur objet, sur un problème aigu de cas non-déclarés et très fortement influencées par les activités des unités policières spécialement conçues pour faire face au problème.

Dans la case multiplicateur/traditionnelle du tableau 1, nous trouvons des actes qui, bien que déjà criminalisés avant l'arrivée de l'Internet, sont décuplés par ce dernier. La diffusion de pornographie juvénile est l'exemple le plus évident. En Europe, le problème de sites incitant à la haine attire également beaucoup l'attention de nos jours (Juriscom, 2005; 01Net, 2005). La case accessoire/traditionnelle contient des activités typiquement criminelles qui ont peu changé avec l'arrivée d'Internet; par exemple, lorsqu'un agresseur sexuel appâte une victime sur un bavardoir (*chatroom*), ni la nature, ni la quantité ou fréquence des activités incriminées sont transformées significativement. La

case déclencheur/émergente contient des activités qui sont entièrement liées au cyberespace, qui n'auraient absolument aucun sens sans ce dernier, et dont l'incrimination est donc nouvelle. Les activités de la case multiplicateur/émergente sont particulièrement intéressantes; ce sont pour la plupart des actes préexistants dont l'incrimination procède uniquement de leur explosion sur Internet. Le phénomène de l'échange de fichiers musicaux sur la toile est l'exemple parfait : les mélomanes ont toujours échangé des fichiers, sauf que l'immense pouvoir des réseaux a donné une impulsion sans précédent aux lobbies des groupes industriels cherchant à faire criminaliser cette activité (Leman-Langlois, 2005). Enfin, la dernière case regroupe des actes fraîchement criminalisés pour une variété de raisons non reliées à l'Internet, comme le support au terrorisme, qui, dans certains cas, fait appel à Internet comme accessoire pour recruter, informer et comploter (voir Gagnon, dans ce numéro).

a. Les crimes « traditionnels » dans le monde virtuel

Une part sans doute énorme, mais difficile à évaluer précisément, des cybercrimes sont en fait des crimes relativement conventionnels dont les auteurs ont adopté des outils modernes pour arriver à leurs fins. On peut s'approprier une infinité de biens physiques, de valeurs symboliques et d'informations confidentielles dans le monde tangible et l'idée de le faire avec une technologie procurant de nouveaux outils et de nouvelles cibles n'est pas particulièrement difficile à formuler, ni à mettre en pratique. Cela dit, les variations les plus exotiques de ces actes ouvrent tout de même une porte fascinante pour l'étude de l'incrimination, du droit et du comportement humain en général. L'exemple des jeux multijoueurs à grande échelle en ligne (*Massively Multiplayer Online Games*, MMOG) est particulièrement révélateur. Il s'agit de jeux de rôles de longue durée auxquels s'adonnent des millions de joueurs (plus de 110 millions internationalement en 2005) qui entrent en interaction les uns avec les autres à travers leur personnage virtuel dans un monde fantaisiste (par exemple, *playonline.com*; *shadowbane.com* ou *cityofheroes.com*). En règle générale, les participants doivent défrayer des coûts mensuels d'abonnement pour pouvoir jouer, et donc la progression dans le jeu correspond à une dépense monétaire souvent non négligeable pour le joueur. La plupart de ces jeux récompensent leurs participants par l'octroi de « prix » virtuels, sous forme d'objets, d'attributs ou de pouvoirs utilisables dans le monde du jeu, par exemple des armes spéciales, de l'argent, etc. Ces prix peuvent être transférés, vendus (dans certains cas, pour plusieurs centaines de dollars) à d'autres joueurs qui désirent progresser rapidement dans le monde du jeu sans avoir à y passer des dizaines d'heures (et plusieurs mois d'abonnement). Ces objets ou attributs virtuels ont donc une valeur, difficile à évaluer clairement mais certainement bien réelle et plusieurs cas de vol ont été rapportés, dont un cas en mars 2005 où la victime a tué le voleur à coups de couteau pour le punir (*News.com*, 2005). À Taiwan, où les MMOG sont extrêmement populaires, les crimes liés au jeux forment déjà 37 % des cas de cybercriminalité identifiés par les autorités (1 300 cas en 2001; Chen, Chen, Ronggong et Korba, 2004). La difficulté, on le devine, est que le droit reste

souvent nébuleux quant à savoir si s'approprier un « sabre magique de niveau 11 » par tricherie est bel et bien un crime.

Notons également que seuls les participants à un MMOG peuvent être victimisés par ce genre de crime. Au Canada et aux États-Unis, les crimes dont se plaignent le plus souvent les usagers ordinaires (entre 60 et 80 % des plaintes) sont également les moins « high tech » : ce sont des ventes entre particuliers (typiquement, sur eBay) où une des deux parties ne remplit pas ses obligations (Statistique Canada, 2002; FBI, 2005).

Les réseaux informatiques sont d'abord et avant tout des systèmes de conservation et de distribution de l'information, dont on peut reconnaître deux grands types. Le premier correspond à l'ensemble des fichiers — audio, photo, texte, logiciels — qui constituent un site sur la toile et qui sont d'accès libre (voire *forcé*, quand il est question de contenu publicitaire). Certains, peut-être la plupart — tout dépend de l'interprétation de la loi et de l'endroit où réside l'usager — des fichiers disponibles en accès libre pour consultation sont toutefois protégés par copyright ou par une entente explicite ou implicite entre l'opérateur du site et le visiteur. Bien sûr, en général, ces fichiers sont utilisés à toutes sortes de fins au mépris entier des règles du droit d'auteur, par des millions d'utilisateurs (par exemple, simplement sauvegarder localement une page consultée sur Internet peut constituer une dérogation). Au Canada, ceci ne constitue pas encore un crime, bien que la Loi sur le droit d'auteur soit maintenant sous révision et que cette situation risque fort de changer (pour l'instant ce type de violation du copyright reste du domaine civil). Il est toutefois important de noter que les règles du droit d'auteur sont nébuleuses même pour les juristes et même dans les cas les plus évidents (par exemple, on dut se rendre à la Cour suprême pour savoir si la présence de photocopieurs était légale dans la bibliothèque de la Société du barreau du Haut-Canada).

Le second type d'information comprend les fichiers qui sont spécifiquement protégés. Il s'agit d'une foule de fichiers destinés à être vendus (logiciels, vidéos, musique, etc.), de secrets industriels, nationaux, commerciaux, d'informations personnelles et d'une infinité de codes et de clés permettant de décrypter les contenus chiffrés. En général lorsqu'il est question d'accès illégal à un site, c'est du vol de ces types d'information dont il est question (attention : les vols virtuels diffèrent fondamentalement des vols conventionnels, en ceci que le propriétaire légitime des biens volés conserve un accès entier à ceux-ci; c'est une *copie* qui est volée). Par exemple, un des chiffres les plus souvent cités pour montrer l'ampleur du problème de la cybercriminalité est celui des attaques contre le Pentagone (22 000 par année), qui sont pour la plupart des tentatives d'accès à des contenus classés secret défense, dans l'immense majorité des cas par des hackers amateurs particulièrement excités par l'idée d'en découdre avec le plus puissant appareil militaire au monde. Dans d'autres cas, des compagnies en victimisent d'autres, comme lorsqu'en mai 2005 des agences de recouvrement ont réussi à soutirer 670 000 dossiers à Bank of America et Wachovia en soudoyant des employés (CNN, 2005). En avril 2005, le *Wall Street Journal* dévoilait que la compagnie ChoicePoint, spécialisée dans la vérification de dossiers de crédits et autres informations personnelles, a vendu plus de 145 000 dossiers personnels à des clients criminels qu'elle

croyaient être des firmes légitimes (voir ChoicePoint, 2005). Deux des acheteurs étaient des frères nigériens qui se sont servis de 7 000 numéros de carte de crédit pour se procurer pour 1 million USD de marchandises diverses (AP, 2005). LexisNexis s'est retrouvé dans la même situation avec 310 000 dossiers personnels en mars 2005. Dans ces cas, évidemment, la tâche des voleurs d'information est facilitée par le désir des compagnies de produire des revenus; dans les cas où des agences gouvernementales sont impliquées, l'irresponsabilité et l'insouciance suffisent. Entre février 2002 et juin 2003, la *Transportation Safety Administration* (TSA, agence du *Department of Homeland Security*, DHS) a laissé télécharger près de 20 millions de dossiers d'usagers des lignes aériennes (DHS, 2005).

Ici, identifier une victime est moins facile qu'il n'y paraît : est-ce la compagnie qui est fraudée par de faux clients, les individus dont les informations personnelles serviront à voler des marchandises, ou les compagnies de carte de crédit qui ne seront pas remboursées ?

Les usages criminels potentiels de ces informations sont multiples, mais c'est le vol d'identité qui prime; usurper l'identité d'une personne était relativement facile pré-Internet mais désormais on peut le faire de façon massive parce que les bases de données contenant les éléments d'identification resteront toujours vulnérables. Un autre moyen de plus en plus populaire est l'envoi massif de courriels trompeurs demandant au destinataires de « mettre à jour » leur dossier bancaire ou leur compte PayPal par exemple, technique couramment appelée hameçonnage, ou « *phishing* » (variation cyberpunk de *fishing*, aller à la pêche). En 2003, la GRC a reçu près de 14 000 plaintes concernant le vol d'identité, mais il est impossible de savoir combien d'entre elles résultent de cybercrimes et combien proviennent de méthodes plus classiques (interception de courrier, fouille de rebuts, arnaques téléphoniques, lecture non-autorisée de cartes de crédit (*skimming*), etc.).

En principe les fraudes financières sont également facilitées par la vulnérabilité des réseaux informatiques (évitons l'erreur répandue de confondre vulnérabilité, risque, menace et attaque réelle). À cause du contexte hautement sensible de ce genre de criminalité, il est pratiquement impossible de savoir combien il y a de cas ou combien d'argent est perdu annuellement à cause de cyberfraudes. Le FBI étatsunien publie annuellement un sondage de victimisation des entreprises en coopération avec le Computer Security Institute, une association corporative (CSI, 2005). Les 269 compagnies ayant répondu à la question auraient cumulé des pertes dues à la fraude de 7 millions USD en 2004, une baisse d'environ 25 % sur l'année précédente (il est imprudent d'extrapoler ces résultats à l'extérieur de l'échantillon). Dans ce total, ce sont les fraudes par carte de crédit qui forment presque l'ensemble des pertes et le nombre de détournements de fonds reste minimal. Une autre étude faite par le magasine SCO, le Carnegie Mellon Computer Emergency Response Team (CERT) et le Service secret étatsunien (*Electronic Crimes Task Force*, ECTF) fait à peu près le même genre de sondage mais en se permettant de considérer leurs 500 répondants comme un échantillon approximatif de l'ensemble. Aussi, leurs résultats sont différents : 666 millions auraient été perdus en 2003 par l'ensemble des entreprises étatsuniennes (CERT, 2004). Le chiffre

astronomique est souvent cité, mais il faut garder à l'esprit que la recherche du CERT utilise une définition beaucoup trop large du cybercrime : « toute infraction criminelle ayant impliqué l'utilisation de matériel électronique » (traduction). Ainsi, les entreprises sont invitées à comptabiliser des aspects « mous » de leur victimisation comme la perte en productivité des employés causée par les courriels non sollicités (qui ne sont pas des crimes). Rappelons que les experts de Carnegie Mellon sont aussi célèbres pour avoir affirmé, en 1995, que *la moitié* du contenu disponible sur Internet était de la pornographie — alors que la proportion réelle est bien au-dessous de 1 % (Wall, 2003 : 21).

Pour ce qui est de l'activité médiatique, qui, doit-on le rappeler, est un pilier essentiel à la construction de la menace auprès du public, il y a trois autres types de cybercrime dont il est fréquemment question : i) la pornographie juvénile (on parle souvent de pornographie tout court); ii) la diffusion de messages haineux; iii) le cyberterrorisme. Aucune des trois activités n'a attendu la création d'Internet, ou même des ordinateurs, pour voir le jour. Pour les deux premiers, les technologies de l'information et de la communication (TIC) ont permis l'explosion de la diffusion des contenus et les échanges entre individus qui, autrement, ne seraient jamais entrés en contact. Pour ce qui est de la pornographie juvénile, un autre facteur important à considérer est le développement rapide de technologies de *production* de contenu, surtout au niveau de l'image photo et vidéo. Pour l'instant, il n'existe pas de façon rigoureuse d'évaluer la progression de la pornographie juvénile ni des sites néo-nazis en excluant la progression spectaculaire des réseaux eux-mêmes, autrement dit de faire la part entre les questions technologiques et les questions criminologiques, qui restent inextricablement liées. Cependant, il semble pour le moins douteux de supposer qu'il y a davantage de pédophiles réels et l'hypothèse la plus économique est que ces derniers ont accès à une technologie qui multiplie leur présence virtuelle.

Le cas du cyberterrorisme est particulièrement fascinant. Le dernier rapport d'Europol sur le terrorisme en Europe pour l'année 2004 comporte une seule phrase sous la section, « cyberterrorisme » : « *No case of cyber terrorism has been reported by the Member States* » (Europol, 2004 : 19). Pourtant, une recherche Google de « *cyber-terrorism* » produit 243 000 fichiers. La menace du cyberterrorisme est sans aucun doute la plus surestimée de toutes, conséquence directe de l'attention médiatique disproportionnée qu'on lui accorde et de la création d'agences policières spécifiquement vouées à la combattre. Le cas du *National Infrastructure Protection Center* (NIPC) aux États-Unis est particulier. Incapable de se protéger lui-même contre le virus Melissa en 1999, une étude du *Government Accounting Office* (GAO) a montré que l'activité principale du NIPC était de lancer des alarmes sans fondement et sans suite (GAO, 2001). Au Canada, le Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC), équivalent du NIPC, soulève également la menace d'attaque cybernétique, soulignant que ce type d'attaque, contrairement aux attaques physiques, peut prendre source à l'étranger. En 2000, le Service canadien du renseignement de sécurité (SCRS, 2000) soulignait que :

> La situation géographique du Canada a contribué, dans une certaine mesure, à y limiter le nombre d'actes terroristes. Toutefois, comme nous sommes reliés directement au cyberespace mondial, il serait possible d'organiser une OI [opération informatique] à partir d'un pays étranger et d'attaquer une cible canadienne en quelques secondes.

Le BPIEPC et le SCRS présentent la planète comme un immense pool de 140 millions d'ordinateurs « zombies » prêts à l'utilisation par des attaquants potentiels — soulignant les incommensurables dégâts possibles (BPIEPC, 2003) tout en admettant qu'il n'existe aucun exemple d'une telle attaque. C'est la confusion du *risque* avec la *vulnérabilité*, alors que tout calcul de risque doit également tenir compte de la présence réelle d'une *menace* en mesure d'exploiter les vulnérabilités identifiées. Une porte déverrouillée constitue certes une « vulnérabilité », mais lorsqu'on demeure sur une île déserte le risque effectif reste à zéro.

b. Création de nouvelles formes de criminalité

Le concept de cybercriminalité couvre également des conduites dont l'existence est entièrement dépendante de celle des réseaux. L'exemple le plus évident est celui des attaques distribuées, qui consistent à submerger un serveur de demandes d'accès via un ensemble plus ou moins grand d'ordinateurs piratés au préalable (appelé « *botnet* », « réseau de robots »), qui finissent par l'empêcher de fonctionner correctement et de répondre aux demandes légitimes. Les clients du serveur perdent accès et ainsi l'entreprise visée perd ses revenus durant l'attaque et aussi longtemps qu'il faudra pour réparer, si le dommage est grave. Les dommages sont généralement évalués en additionnant i) le manque à gagner maximal des ventes possibles; ii) les coûts de réparation; iii) les pertes en productivité des employés durant la paralysie du site. Légalement, ce type d'attaque a été considéré comme équivalent à tout autre forme de dommage à la propriété, ce qui, pour un criminologue, est clairement inadéquat : ni les motifs, ni les moyens employés, ni les dommages, ni les cibles, ni les victimes sont comparables à ceux des délits conventionnels contre la propriété. Le cas « Mafiaboy » est particulièrement bien connu au Canada. L'adolescent de la banlieue de Montréal avait réussi, en 2000, à mettre à genoux les serveurs de plusieurs entreprises, dont Yahoo, CNN, eBay, Amazon, Dell et eTrade. Pourtant, le fait que le cas soit célèbre souligne surtout sa rareté (le ministère de la Justice des ÉU maintien une liste de toutes les causes fédérales de cybercriminalité à www.usdoj.gov/criminal/cybercrime/ccdocs.htm). Les pertes des entreprises, évaluées superlativement comme toujours, n'ont pas eu de conséquence sérieuse.

D'autres cas sont plus graves, par exemple lorsque des individus ou groupes font chanter des opérateurs de sites commerciaux en *menaçant* de les attaquer — ceci étant pratiquement impossible à distinguer de l'extorsion classique et ne demandant aucune compétence particulière en informatique. À l'occasion, il s'est avéré que l'attaque contre un site commercial avait été déclenchée par un site concurrent (PhillyBurbs, 2005). Bon exemple de la nébulosité juridique typique des attaques informatisées, la compagnie Lycos

employa en 2004 un économiseur d'écran installé par 110 000 de ses usagers pour s'attaquer à des serveurs appartenant à des firmes de dissémination de pourriel (voir makelovenotspam.com). Les raisons pour lesquelles les sites sont attaqués varient donc énormément, comme l'identité des victimes et des responsables. Dans le cas de Lycos, les attaques ne venaient pas d'ordinateurs piratés, mais de milliers de participants volontaires à l'attaque massive internationale; les victimes, des spammeurs invétérés, n'attirent pas non plus une sympathie particulière. D'ailleurs, ils sont eux-mêmes de plus en plus la cible d'efforts de criminalisation. Si on n'a jamais sérieusement considéré l'incrimination du pourriel en soi, plusieurs projets de loi récents dans les pays occidentaux ont tenté de l'encadrer plus rigoureusement et de criminaliser les violations éventuelles de cet encadrement (au Canada, le projet S-23 de 2003, *Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités*, criminalise certaines formes de pourriel, notamment le pourriel à contenu pornographique).

D'autres incriminations émergentes partagent également cette caractéristique de flou moral, culturel et technologique. Le Canada a récemment criminalisé le support au terrorisme et plus particulièrement le fait de mettre des biens, services ou fonds à la disposition de terroristes. Dans la mesure où l'information est considérée comme un bien, plusieurs formes d'échanges sur Internet pourraient faire l'objet de poursuites criminelles. Il s'agit donc ici d'un comportement pré-Internet assujetti à une incrimination post-Internet procédant de la préoccupation des politiciens, des médias et du public par le terrorisme.

On appelle à l'occasion « vandalisme virtuel » les intrusions sur des serveurs visant non pas à voler de l'information ou à paralyser un site mais plutôt à changer l'aspect ou le contenu des fichiers html qui le constituent. Les motivations pour le faire sont multiples, du hacker « politique » (*hacktivist*) qui introduit sur un site gouvernemental australien une bannière traitant le premier ministre John Howard de « *US boot liker* » au hacker « sportif » qui collectionne les sites corrompus comme des trophées pour ensuite s'en vanter sur des groupes de discussion. Une large portion des vers et virus attaquant les ordinateurs personnels et les serveurs procèdent du même genre d'intention; c'est l'exploit en soit qui est visé, davantage que le gain. Le goût de l'exploit est également à la source de plusieurs virus. David Smith, auteur du macrovirus « Melissa », afficha son virus dans le groupe de discussion alt.sex dans un message promettant un accès gratuit à des sites pornographiques. L'infection se propagea ensuite automatiquement par courriel, causant éventuellement un ralentissement massif d'Internet pendant près d'une semaine et des pertes habituellement évaluées à 450 millions USD. Ceci est sans aucun doute une grossière surévaluation, étant donné que Melissa n'était pas un virus destructeur, seulement un macro Word s'adressant lui-même à d'autres correspondants trouvés sur la liste de contacts de l'ordinateur infecté.

L'aspect intéressant de ces affaires est la saveur infiniment variable qu'on peut leur donner. En général, ces narratifs sont offerts pour conscientiser les utilisateurs d'Internet à propos des menaces possibles qui pèsent sur eux, pour leur expliquer pourquoi ils doivent s'équiper de logiciels antivirus, installer

régulièrement les mises à jour de sécurité de leur système d'exploitation (ou se procurer une nouvelle version du dit système), d'éviter d'ouvrir des courriels d'envoyeurs inconnus, etc. Dans ce contexte, c'est le danger, la vulnérabilité des systèmes et des individus, le côté spectaculaire des dommages causés qui est souligné. À la fois, le très faible nombre de ces incidents montre que cette activité est peu répandue si on la compare à bien d'autres formes de criminalité. Ses effets sur le fonctionnement des réseaux informatiques sont aussi à relativiser si on tient compte du phénomène des pourriels, qui eux sont légaux et forment quelques 75 % du courriel transmis sur Internet, ou du téléchargement de contenu commercial obligatoire (fenêtres intempestives, intersticiels, supersticiels, pubs volantes, etc.) omniprésent et lourd d'images, d'animations et de son. Mais les concepts de cybercrime et de cyberterrorisme ont d'autres utilités qui peuvent expliquer leur importance disproportionnée.

2. Les usages du cybercrime

En tant que concepts, le cybercrime et le cyberterrorisme servent à structurer des relations de pouvoir entre individus, entreprises privées et institutions étatiques. L'exemple le plus fascinant de ces activités de structuration est le phénomène de l'échange non autorisé de fichiers musicaux en ligne (Leman-Langlois, 2005). Dès le départ, l'Internet promettait de multiplier les revenus en éliminant une large part du carcan de la vente au détail traditionnelle (entre autres, on pouvait fonctionner avec des ressources humaines minimales, à partir d'un simple méga-entrepôt dans une zone industrielle à loyer modéré — ou encore sans aucun inventaire, en commandant au besoin à ses fournisseurs). Cependant, il restait un piètre outil d'échange commercial, offrant peu de sécurité à la fois aux acheteurs qu'aux entreprises puisque conçu pour la libre circulation de l'information entre une infinité de points d'accès. D'un point de vue industriel, l'Internet comportait donc plusieurs « défauts » dont l'identification à la criminalité permit de mobiliser l'État pour le rendre davantage compatible avec la conduite d'échanges commerciaux sécuritaires et profitables. L'État répondit assez facilement, porté par le désir de montrer un contrôle efficace des nouvelles technologies et d'encourager une foule de secteurs industriels de pointe.

Un autre secteur industriel y trouvant son compte est celui de la sécurité informatique. Le système répandu de virus-inoculation est un grand générateur de revenus pour les firmes dominant le marché comme Symantec (Norton) ou Network Associates (McAfee). Une minorité de fabricants de ces logiciels offrent des produits qui ne nécessitent pas de mise à jour perpétuelle ni d'abonnement à ce genre de service. Pour les autres, le foisonnement garanti de nouvelles menaces constitue un des fondements de leur stratégie de mise en marché.

Dernier exemple, l'industrie des communications utilise également le cybercrime pour se distancer des usages controversés d'Internet que certains de ses clients peuvent faire et pour lesquels ses membres pourraient hypothétiquement être tenus responsables au civil. Les fournisseurs d'accès Internet (FAI) ont fortement augmenté leurs revenus en convainquant leurs clients de passer à l'accès haute vitesse par câble ou par DSL. Leur argument

de vente est la vitesse du téléchargement, qui est particulièrement critique pour ceux qui cherchent des fichiers musicaux et des films. Bien sûr, les FAI n'encouragent pas explicitement l'échange non-autorisé de ces fichiers, mais l'usager qui déciderait d'acheter la quantité de musique qu'une connexion haute vitesse peut potentiellement télécharger accumulerait rapidement une facture particulièrement salée. Ainsi, pour l'usager moins fortuné, télécharger massivement signifie « gratuitement », du moins en partie. Dans ce contexte, la notion de cybercrime permet aux FAI de rejeter la responsabilité des échanges sur ceux qui décident de commettre des *crimes*, niant tout effet systémique (la même logique s'applique aux compagnies qui commercialisent des lecteurs portatifs à grande capacité comme le populaire iPod d'Apple).

La menace du cybercrime a aussi été à la source de l'augmentation des dispositifs de sécurité informatique côté utilisateurs et opérateurs de réseaux, qui transforment non seulement l'usage de l'ordinateur en rendant certaines conduites nécessaires (utilisation de mots de passe, nécessité de s'identifier personnellement comme utilisateur) et d'autres impossibles ou plus difficiles (copie personnelle libre de logiciels, de CD, de DVD) mais aiguillent de plus en plus l'usager moyen vers des contenus payants nécessitant une connexion de plus en plus coûteuse.

Ainsi, à de multiples niveaux la notion de cybercrime sert à découper une identité de bon consommateur maximisant son utilisation d'Internet payant et cédant aux « tentations » offertes par le système seulement dans la mesure où il peut en défrayer les coûts (sur carte de crédit bien sûr). Le concept tente de produire une cassure radicale entre l'usage encouragé et l'usage possible qui, dans le cyberespace, n'existe tout simplement pas. Dans l'espace traditionnel, il est facile de voir une différence entre un objet gratuit, ou abandonné, et un autre qui se trouve dans une vitrine ou sur la banquette d'une voiture. Dans l'espace virtuel, il faut revoir entièrement la notion d'opportunité criminelle : dans un environnement où la notion de propriété se rapporte exclusivement à de l'information, copiée, échangée, modifiée, l'opportunité criminelle n'est plus rien d'autre que le revers de l'opportunité commerciale.

On l'aura remarqué, cette restructuration du cyberespace et l'étiquetage de ses usagers ressemble intimement au processus conventionnel d'incrimination qui a cours dans ce que tout cyberpunk qui se respecte appelle « l'espace-viande » (*meatspace*) concret. L'incrimination de conduites multiples vise à créer un espace où les activités de l'usager moyen sont de plus en plus canalisées vers la consommation de produits informatiques de production industrielle. Jusqu'à présent, les succès sont mitigés; aux États-Unis, qui sont à l'avant-garde à la fois de la technologie et de l'incrimination, il reste trop tôt pour conclure que les poursuites au civil et au criminel d'individus échangeant des fichiers sans permission ont poussé les internautes à retourner vers les magasins ou à visiter les services payants comme iTunes Music Store (ITMS). En parallèle se sont développés de nouveaux moyens, moins faciles à détecter, de continuer les échanges. Pourtant, selon les associations industrielles, les ventes de disques semblent être sorties de leur pente descendante des cinq dernières années (voir par exemple RIAA, 2005), et les ventes d'ITMS, bien que

moins importantes qu'initialement prévues par Apple, sont en forte augmentation malgré l'arrivée de services concurrents.

Conclusion

Il est fort probable que d'un point de vue objectif la notion de cybercrime, dans son état courant tel que reflété dans la majorité de la littérature, dans les médias, dans les discours politiques et dans les documents de source policière, se révélera à court ou à moyen terme comme une impasse scientifique totale pour les criminologues. La notion procède davantage d'impératifs commerciaux, de nécessités politiques et d'une panique morale nourrie par une mauvaise compréhension du fonctionnement et des possibilités de l'informatique réseautée, que d'une réflexion rationnelle. De surcroît, elle est trop séduisante par sa simplicité et sa conformité aux besoins institutionnels des agences de contrôle. Pour ces mêmes raisons, elle reste toutefois un sujet fascinant pour l'étude de la construction de problèmes sociaux ou de différents processus d'incrimination. Le criminologue intéressé par les actes généralement associés au cybercrime fera mieux de redécouper cette catégorie de façon plus rigoureuse. Bien sûr, les activités de pédophiles, de néo-nazis ou d'arnaqueurs sur Internet sont de fascinants sujets d'étude, tout comme l'impact potentiel des nouvelles technologies sur d'anciennes déviances; l'amalgamation de l'ensemble sous le vocable de « cybercriminalité », pourtant, ne contribue certainement pas à mieux les connaître.

Deuxième observation importante, l'étude de la construction sociale du cybercrime ne peut se faire sérieusement sans le replacer dans le contexte de la colonisation commerciale intensive du cyberespace.

Enfin, il semblerait utile de se pencher sur la nature même du cyberespace comme contexte d'activité criminalisée ou criminalisable. Il existe un corps de littérature qui se penche sur les conséquences culturelles, morales, pratiques de la virtualité informatisée (comme par exemple Herman et Swiss, 2000 et Benedikt, 1992) qui pourra apporter beaucoup à l'étude criminologique de l'interaction humaine désincarnée, de la notion de dommage, de la réaction sociale virtuelle et traditionnelle et de la politique pénale.

Références

01Net

(2005) *Les FAI mis en cause pour l'accès à un site révisionniste*, http://www.01net.com/editorial/279716/justice/les-fai-mis-en-cause-pour-l-acces-a-un-site-revisionniste.

Associated Press (AP)

(2005), *ChoicePoint Was Targeted Before*, http://www.wired.com/news/politics/0,1283,66767,00.htm.

Beardwood, John

(2003) « Creeping Law ? An Analysis of the Canadian Lawful Access Consultation Document and Its Approach to Implement the Council of Europe's Convention on Cyber-Crime », *Computer Law Review International*, 2003 (3), 77-83.

Benedikt, Michael
(Éd. 1992) *Cyberspace : First Steps*, Cambridge (Mass.), Massachusetts Institute of Technology Press.
Branigan, Steven
(2005) *High-Tech Crimes Revealed : Cyberwar Stories from the Digital Front*, Boston, Addison-Wesley.
Brenner, Susan
(2004) « U.S. Cybercrime Law : Defining Offenses », *Information Systems Frontiers*, 6 (2), 115-132.
Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC)
(2003) *Les menaces aux infrastructures essentielles canadiennes*, http://www.ocipep.gc.ca/opsprods/other/TA03-001_f.pdf.
Cable News Network (CNN)
(2005), « Bank security breach may be biggest yet : Account info at Bank of America, Wachovia sold by employees; more arrests expected, N.J. police say », *CNNMoney*, http://money.cnn.com/2005/05/23/news/fortune500/bank_info/.
Canada
(2003) *Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités*, http://www.parl.gc.ca/37/2/parlbus/chambus/senate/bills/public/pdf/s-23_1.pdf
Carnegie Mellon Computer Emergency Response Team (CERT)
(2004) *2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes*, http://www.cert.org/about/ecrime.html.
Carter, David
(1995) « Computer Crime Categories : How Techno-Criminals Operate », *The FBI Law Enforcement Bulletin*, juillet 1995, http://nsi.org/Library/Compsec/crimecom.html.
Chen, Ying-Chieh, Patrick Chen, Ronggong Song et Larry Korba
(2004) *Online Gaming Crime and Security Issue – Cases and Countermeasures from Taiwan*, National Research Council of Canada.
ChoicePoint
(2005) *Response to 5/3 Article in The Wall Street Journal*, http://www.choicepoint.com/news/statement_050405_1.html.
Clarke, Richard
(2005) « Ten Years Later », *The Atlantic Monthly*, janvier-février, 61-77.
Stanley Cohen
(2003) *Folk Devils and Moral Panics : The Creation of Mods and Rockers*, (3e édition), New York, Routledge.
Computer Security Institute (CSI)
(2005) *CSI/FBI Computer Crime and Security Survey*, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.
Conseil de l'Europe
(2001) *Convention sur la cybercriminalité*, http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm.

Denning, Dorothy
(1999) *Information Warfare and Security*, New York, ACM Press.
Department of Homeland Security (DHS)
(2005) *Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data*, DHS, Office of the Inspector General, http://www.dhs.gov/inter-web/assetlibrary/OIGr-05-12_Mar05.pdf.
Etter, Barbara
(2001) *Computer Crime*, conférence donnée au 4e symposium sur le crime en Australie, Institut australien de criminologie, http://www.aic.gov.au/conferences/outlook4/Etter.pdf.
Europol
(2004) *Terrorist Activity in the European Union : Situation and Trends Report (TE-SAT)*, La Haye, Europol, #100927, 2 décembre 2004.
FBI
(2005) *IC3 2004 Annual Internet Fraud Report*, http://www1.ifccfbi.gov/strategy/2004_IC3Report.pdf.
Furnell, Steven
(2005) *Computer Insecurity : Systems at Risk*, New York, Springer.
General Accounting Office (GAO)
(2001) *Critical Infrastructure Protection Significant Challenges In Developing National Capabilities*, Washington, GAO, #01-323.
Gibson, William
(1984) *Neuromancer*, New York, Penguin Books.
Herman, Andrew et Thomas Swiss
(Éd. 2000) *The World Wide Web and Contemporary Cultural Theory*, New York, Routledge.
Juriscom
(2005) *Contenus illicites*, http://www.juriscom.net/txt/jurisfr/cti/resum.htm.
Larivière, Jules
(1998), *Les bibliothèques et la nouvelle loi canadienne sur le Droit d'auteur: un commentaire*, http://www.robic.ca/cpi/Cahiers/10-2/03LariviereW97.htm.
Leman-Langlois, Stéphane
(2005) « Theft in the Information Age : Music, Technology, Crime and Claims-Making », *Knowledge, Technology and Policy*, 17 (3-4), 140-163.
Lessig, Lawrence
(2002), *The Future of Ideas*, New York, Random House.
Ministère de la Sécurité publique (MSP)
(2004) *Rapport annuel de gestion, 2003-2004*, Québec, MSP, http://www.msp.gouv.qc.ca/msp/biblivir/rappann/2003/rapport_annuel_2003-2004.pdf
News.com
(2005) « Gamer Murdered Over Cyber-sword Sale », http://www.news.com.au/story/0,10117,12700877-13762,00.html

PhillyBurbs.com
(2005) *Hacker Teenager Pleads Guilty*, http://www.phillyburbs.com/pb-dyn/news/112-05142005-489320.html.
Recording Industry Association of America (RIAA)
(2005) *2004 Yearend Statistics*, http://www.riaa.com/news/newsletter/pdf/2004yearEndStats.pdf.
Service canadien du renseignement de sécurité (SCRS)
(2000), *Opérations informatiques (la « cybermenace »)*, http://www.csis-scrs.gc.ca/fra/operat/io2_f.html.
Sofaer, Abraham et Seymour Goodman
(Éd. 2001) *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford (Cal.), Hoover Institution Press.
Speer, David
(2000) « Redefining Borders : the Challenges of Cybercrime », *Crime, Law and Social Change*, 34, 259-273.
Statistique Canada
(2002) *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Ottawa, ministère de l'Industrie.
Thatcher, Sarah
(2005) *Public Policy and the Social Construction of Cyberterror: The Hunt for the Paper Tiger*, Londres, London School of Economics, Thèse de doctorat non publiée.
Thomas, Douglas et Brian Loader
(Éd. 2000) *Cybercrime : Law Enforcement, Security and Surveillance in the Information Age*, New York, Routledge.
Wall, David
(2003) « Cybercrimes : New Wine, No Bottles ? » D. Wall, *Cyberspace Crime*, Burlington (VT), Ashgate, 105-137.