Article

« La sécurité du jeu et le jeu de la sécurité : piratage, loi et politique publique »

John L. McMullan et David C. Perrier

Criminologie, vol. 39, n° 1, 2006, p. 83-106.

La sécurité du jeu et le jeu de la sécurité : piratage, loi et politique publique[1]

John L. McMullan
Professeur de sociologie
et criminologie
Saint Mary's University
Halifax, Nouvelle-Écosse, Canada
john.mcmullan@stmarys.ca

David C. Perrier
Professeur associé de
sociologie et criminologie
Saint Mary's University
Halifax, Nouvelle-Écosse, Canada
david.perrier@stmarys.ca

RÉSUMÉ • Le présent rapport est l'objet d'une étude du lien entre les organisations criminelles et le contrôle social dans le domaine de la criminalité informatique. D'abord, nous examinerons quelques attaques montées contre des appareils de jeu électronique. Ensuite, nous analyserons de quelle façon ces cyberattaques ont été commises et quelle est la capacité de l'État et du secteur industriel à les combattre. Enfin, nous comparerons nos conclusions à celles tirées d'autres études sur le piratage dans l'industrie des jeux de hasard et nous discuterons de l'importance de nos conclusions pour les systèmes d'application de la loi, de sécurité et de protection des consommateurs.

MOTS CLÉS : jeux de hasard, criminalité informatique, application de la loi, piratage, politique publique

ABSTRACT • This paper studies the relationship between criminal organization and social control in the area of computer crime. We examine a "cheat at play" scheme that hacked into electronic gambling machines. We focus on how these cyber-attacks

1 Traduit par Ève-Marie Racette.

were committed and on the ability of the state and the industry to control them. We compare and contrast our findings with the research on hacking and the gambling industry and conclude by discussing the implications that our research has for law enforcement, security and public policy.

KEY WORDS: Gambling, Computer Crime, Law Enforcement, Hacking, Public Policy

Les jeux de hasard sont un phénomène relativement récent au Canada (Azmier *et al.,* 2001 ; Campbell et Smith, 1998 ; Marshall et Wynne, 2004 ; Smith et Azmier, 1997). Chaque année, les Canadiens misent 18 milliards de dollars, pour un revenu net (c'est-à-dire, le produit, déduction faite des lots, des frais et des commissions) de 6,5 milliards de dollars, somme qui a quadruplé depuis 1992. De même, le nombre d'emplois dans ce secteur est passé de 12 000, en 1992 à 50 000, en 2003, augmentation de loin supérieure à celle affichée dans tous les autres secteurs industriels. Le revenu net des jeux de hasard pour les provinces, déduction faite des frais fixes et autres dépenses, est passé de 2,1 % de l'ensemble des recettes, en 1993 à 5,6 %, en 2002 et les dépenses qu'il représente sont passées de 147 $ par habitant (âgé de 18 ans ou plus), en 1993 à 483 $, en 2002 (Marshall et Wynne, 2004).

Au Canada, on retrouve actuellement 38 652 appareils de loterie vidéo (ALV) dans 8 309 points de jeu, 37 050 appareils à sous, 1 805 tables de jeu, 27 063 terminaux de loterie en ligne, 1 880 bingos, 74 casinos et casinos-hippodromes (*racinos*), 70 hippodromes et 107 téléthéâtres. Il y a, en moyenne, un appareil de jeu de hasard électronique pour 329 adultes, un ALV pour 599 adultes et un point d'ALV pour 2 668 adultes au Canada (KPMG, 2004). Les moteurs de cette croissance ont été les casinos et les ALV. En 2003, les loteries rapportaient 25 % des revenus nets de jeux de hasard (organismes caritatifs exceptés), les casinos, 33 % ; les ALV, 23 % et les appareils à sous hors casino, 19 % (Marshall et Wynne, 2004). Si la prolifération des technologies de jeu électronique a donné naissance à de nouvelles activités récréatives, elle est également responsable de divorces, de pertes pécuniaires et de faillites, de pertes d'emplois, de troubles de la santé et de criminalité (Eadington, 1996 ; Goodman, 1995 ; MacDonald *et al.,* 2004 ; McMillan, 1996 ; McMullan et Perrier, 2003).

De plus, nous examinerons un stratagème de piratage organisé contre les ALV d'une province canadienne. Nous étudierons la façon par laquelle ces cybercrimes sont commis et la capacité de l'État à les contrer. Les

occasions de fraude sont-elles nombreuses ? Les produits sont-ils correctement protégés ? La sécurité est-elle au point ? La loi est-elle appliquée ; les sanctions, utilisées ? Malheureusement, nous ne possédons pas d'information sur la psychologie des pirates (par ex. : déni de victime, abdication de responsabilité, recours à des intérêts supérieurs, condamnation des lois, etc.). Par contre, les données disponibles nous permettent de croire que la persistance des cyberattaques est au moins partiellement due au régime législatif appliqué au secteur du jeu. Notre analyse se présente donc comme suit : premièrement, nous exposerons le point de vue des auteurs et la méthodologie adoptée ; deuxièmement, nous décrirons différentes sortes de cyberattaques commises sur des appareils de jeu électronique et nous situerons le présent rapport dans un contexte comparatif de jeu et de criminalité ; troisièmement, nous décrirons le régime d'application de la loi en vigueur et nous démontrerons que les structures policières et administratives sont inappropriées ; finalement, nous présenterons les répercussions de cette recherche sur la sécurité et la politique publique.

Perspective et méthode

L'hypothèse sous-jacente à notre recherche est que le piratage des appareils de jeu est une activité qui vise expressément à mener à bien cette opération illégale. L'explication du cybercrime organisé résiderait donc dans l'activité même et les problèmes légaux qui s'y posent. Cette approche explicative fait ressortir ce qui suit : 1) d'abord, qu'à un certain stade de l'évolution technologique, toute activité illégale se bute à des problèmes techniques et sociaux qui doivent être surmontés pour être menée à bien ; 2) ensuite, que l'on peut cerner les types d'organisation les plus aptes à résoudre ces problèmes ; 3) enfin, que ces organisations sont plus ou moins aptes à négocier avec les agences d'application de la loi. Dans la foulée des rapports Cressey (1972) et McIntosh (1973 ; 1975), on se pose les questions suivantes : Quelles difficultés techniques ont dû être surmontées pour réussir des cyberattaques contre des appareils de jeu ; Comment la division du travail s'est-elle faite et comment a-t-on résolu les problèmes liés à la planification, la sécurité, la protection des biens, la surveillance du site et la lutte anticriminalité ; Quel était le niveau de sécurité des produits et environnements de jeu ; Enfin, quelles sont les répercussions politiques de *la sécurité du jeu et le jeu de la sécurité* ?

Nous avons adopté la définition d'une étude de cas proposée par Orum *et al.* (1991 : 2) : « une enquête approfondie, pluridimensionnelle, fondée sur des méthodes de recherche qualitative, d'un phénomène social précis ». L'objectif, ici, est donc de décrire comment un réseau de piratage a pu surmonter les écueils des règlements, des lois et des sanctions et de comparer le comportement organisationnel de ce réseau à celui d'autres groupes criminels qui ont déjà piraté d'autres sites et produits de jeu et qui ont fait l'objet de recherches distinctes. L'étude de cas qui nous concerne nous a été suggérée par un organisme de loterie provincial dont le réseau d'ordinateurs avait été compromis par une série d'attaques Internet contre leurs ALV. Voici ce qu'avait à dire un représentant de la loi :

> Nous avons dû faire venir un spécialiste afin de découvrir comment le criminel avait infiltré notre réseau [...] Pour ma part, j'avais un intérêt très particulier dans toute cette affaire : si je pouvais convaincre ce malfaiteur, en coopération avec la GRC, de nous expliquer sa méthode, alors j'en saurais autant que lui et je pourrais faire en sorte que ça ne puisse plus se reproduire.

Grâce à cette approche, les représentants de la loi ont obtenu de l'information détaillée sur les méthodes utilisées pour infiltrer les réseaux et contourner les dispositifs de détection et de contrôle, et nous avons pu obtenir l'accès à cette précieuse information. L'information donnée dans la documentation écrite portait sur l'organisation du réseau de piratage, le système de sécurité et d'observation de la loi du fournisseur de jeux de hasard et les méthodes de détection, de dissuasion et de sanction de l'agence d'application de la loi. Cette information a été complétée par 7 entrevues avec des agents qui ont travaillé sur l'affaire.

Le piratage et les jeux de hasard

Par criminalité informatique, on désigne, de façon très générale, la destruction, le vol, l'usage illicite ou illégal, la modification ou la contrefaçon d'information, de programmes, de services, d'équipements ou de réseaux de communication (Perry, tel que cité dans Rosoff *et al.,* 2002 : 417). Dans les paramètres de cette définition, nous pouvons catégoriser les crimes informatiques de façon plus précise : a) le vol pécuniaire ; b) le piratage d'ordinateurs ; c) la fraude électronique ; d) le sabotage malveillant ; et e) l'espionnage. Notre étude qui s'intéresse au vol et au piratage d'ordinateurs décrit une opération illégale bien pensée

conjuguant expertise informatique et ingéniosité à vaincre les mécanismes de sécurité afin de pirater des appareils et de dérober de l'argent aux commerçants et au gouvernement.

Les vols et fraudes contre les appareils de jeu électronique ne sont rien de nouveau. Normalement, y interviennent des gadgets maison comme des béquilles ou pommes de touline qui interfèrent physiquement dans les rouages des appareils de façon à payer un *gagnant* frauduleux. Le plus souvent, les fraudeurs démontent un appareil du même fabricant et mettent au point ces gadgets pour déjouer le logiciel ou matériel, selon le cas (Skolnick, 1980 : 264-267). Par exemple, les *baguettes magiques*, lampes miniatures alimentées par des piles d'appareil-photo, aveuglent le lecteur optique interne d'un appareil à sous et l'induisent à débourser. Les fraudeurs d'appareils à sous exploitent ces astuces depuis des décennies, travaillant en équipes mobiles de 2 ou 3 personnes et attaquant à petits coups de nombreux appareils à divers endroits pour *gagner* quelque 1 000 $ de l'heure (Crenshaw, 2003 ; The Gambling Magazine, 2004).

La première technologie d'attaque contre les ALV étudiée aux fins du présent rapport consistait à déjouer des codes de protection à l'aide de microprocesseurs, de microcontrôleurs, de matériel informatique et de langages de programmation. La bande criminelle en question avait réussi à découvrir l'algorithme de génération de nombres aléatoires d'un appareil à sous en créant un simulateur de générateur de nombres aléatoires, en étayant celui-ci d'une vaste base de données sur les combinaisons de jeu et en exploitant un programme de recherche informatisé. Un policier explique :

> Trois individus se rendaient à un point de jeu. Le premier restait dans le véhicule où il maniait un ordinateur portatif et un poste radio. Le deuxième et le troisième entraient dans l'établissement. Le joueur portait clandestinement une caméra vidéo, de l'équipement de communication, une oreillette et une pile. Il dirigeait la caméra sur l'écran de l'ALV et communiquait les mises et le comportement de l'appareil à son acolyte dans le véhicule qui, à l'aide d'un ordinateur haute vitesse, déterminait où l'ALV en était dans son cycle aléatoire. S'il était près du gros lot, il disait au joueur d'augmenter sa mise de 5 jetons à 50.

Cette technique *prédictive* a également été exploitée pour truquer des appareils de poker, comme c'était le cas récemment aux États-Unis. Une bande criminelle a acheté des appareils de jeu, les a désassemblés, en a disséqué le fonctionnement, appris comment des chiffres aléatoires se convertissaient en cartes à l'écran et comment et à quel intervalle les chiffres aléatoires revenaient, a conçu un programme tenant compte de

toutes ces variables et, enfin, a percé la séquence des gros lots. Les complices communiquaient entre eux à l'aide d'ordinateurs miniaturisés à commandes cachées dans leurs souliers et de vibrateurs silencieux dissimulés dans des oreillettes invisibles. La séquence des cartes à l'écran était entrée dans un ordinateur en code binaire, où elle était reconnue par une base de données contenant l'algorithme de l'appareil. Les pirates pouvaient dès lors savoir que 5 nouvelles cartes seraient données lorsqu'ils se déferaient des leurs. Comme l'explique l'un des complices : « Nous avions un avantage de 40 % pour chaque donne [...] c'est énorme, les meilleurs joueurs de black jack au monde n'ont qu'un avantage de 2,5 % [...] On pouvait facilement gagner 1 000 $ en à peine une demi-heure », (cité dans Mitnick et Simon, 2005 : 15). Les jeux de roulette en Australie et en Europe ont aussi été attaqués par des groupes de cybercriminels bardés de technologies portables. Par exemple, un individu calculait le jeu d'une roue à l'aide d'un ordinateur miniaturisé et envoyait des messages vocaux synthétisés à un complice portant des oreillettes dissimulées. Ensemble, les deux complices pouvaient deviner la vitesse de la roulette, déduire quels chiffres étaient susceptibles de gagner, et réduire les chances de la maison de gagner (The Gambling Magazine, 2005).

La deuxième technique d'attaque contre les ALV étudiée consistait à infiltrer la carte mémoire secondaire des appareils de jeu et d'y observer le comportement de la mémoire vive (RAM). À l'aide d'un contrôleur de codes machine, les malfaiteurs se livraient à une activité appelée *repérage des programmes d'initialisation* (*boot-tracing*). Ils retrouvaient le compteur de bonus dans la mémoire vive, y inséraient des instructions de modification de la carte de mémoire vive secondaire, puis manipulaient la mémoire et la logique du compteur de bonus de façon à déclencher des paiements sur demande. De même, ils avaient manipulé le compteur de paiements situé dans l'EPROM en enlevant celle-ci de l'appareil, en copiant l'information sur l'emplacement des grilles de paiements, en modifiant celle-ci et en la réinstallant sur une copie de l'EPROM de façon à augmenter les paiements pour les combinaisons gagnantes.

Cette technique n'est pas nouvelle ; en fait, elle avait été exploitée par des initiés dans les années 1980 et 1990 afin d'empêcher les paiements aux clients : American Coin, un fabricant d'appareils à sous, avait à sa solde des programmeurs dont la tâche était d'installer des puces informatiques truquées dans ses appareils. Ils avaient ainsi modifié 1 000 appareils de poker vidéo et de keno, les premiers pour ne pas

afficher de séquences royales et les deuxièmes pour ne pas donner de gros lot. Le subterfuge découvert, on a crié au plus gros scandale de l'histoire du jeu du Nevada. L'entreprise a perdu sa licence et a été condamnée à une amende d'un million de dollars. De même, Universal Distributing, fabricant d'appareils à sous du Japon, a programmé des scénarios de *quasi-gros lot* dans ses appareils vers la fin des années 1980. Les appareils affichaient deux symboles identiques sur la même ligne puis un troisième presque vis-à-vis pour inciter les joueurs à croire qu'ils y étaient presque et à continuer. À la longue, on a découvert la fraude et l'entreprise a dû reprogrammer 15 000 appareils (Bourie, 1999 : 5). Plus récemment, on a découvert dans des appareils de jeu au Canada et aux États-Unis certains codes de programmation donnant des options secrètes aux utilisateurs initiés. Ces codes avaient été implantés par des programmeurs possiblement à la solde des fabricants ou des distributeurs et, comme pour les cyberattaques contre les ALV, ils ont été exploités à des fins frauduleuses par les initiés qui pouvaient ainsi générer des paiements à volonté. Un fabricant d'appareils à sous a reconnu, il n'y a pas si longtemps, avoir vendu des *œufs de Pâques* à un casino pour l'amusement de ses clients fidèles, et un ancien propriétaire de casino Internet a démontré aux autorités comment il pouvait vider une machine en une minute et demie. Comme il l'a dit lui-même : « Il y a des brèches béantes dans la programmation d'appareils à sous », qui sont exploitées par « un souterrain du jeu au Michigan, en Iowa et en Illinois ». En effet, l'un des plus importants fabricants de produits de jeu au monde a admis que 300 de ses appareils ont perdu entre 1 et 2 millions de dollars en 3 mois (Blackwell, 2005 ; 2004 ; Mandel, 2000).

La troisième technique d'attaque contre les ALV sondée consistait à corrompre des appareils à l'aide d'interfaces et de programmes informatiques de façon à infiltrer, effacer et modifier la mémoire vive. Il s'agit d'une technique de *porte dérobée*, semblable au *gaffing* ou à la *programmation fantôme*, où la machine est manipulée de façon qu'elle ait l'air de fonctionner en réseau alors qu'en fait elle fonctionne en mode autonome. Soit dit en passant, toutes ces techniques ne sont pas particulièrement sophistiquées, et les appareils de jeu terrestres et logiciels de fraude sont assez faciles d'accès. Les pirates n'ont qu'à acheter un appareil auprès d'un fabricant légitime ou d'un revendeur illicite, en trouver les failles et inventer des moyens de les exploiter. Ensuite, ils échangent des idées et de l'information privilégiée dans des forums de discussion Internet privés de façon à décupler leurs connaissances. Un pirate de

dire : « J'ai été franchement surpris d'apprendre que nous pouvions nous procurer exactement les mêmes appareils qu'un casino [...] Nous l'avons tout simplement chargé dans notre auto. Nous sommes rentrés chez nous comme s'il y avait un bébé à bord » (Cité dans Mitnick et Simon, 2005 : 4).

Ce genre de cybercrimes sévit également dans les sites de jeux de hasard Internet. Cryptologic, entreprise de logiciels de jeux en ligne, a été attaquée par un pirate qui a infiltré l'un de ses serveurs et manipulé les jeux de dés et de sous de façon à ce que les joueurs ne puissent pas perdre. Chaque coup des appareils à sous virtuels donnait un coup parfait et, en quelques heures à peine, 140 joueurs différents ont gagné pour 1,9 million de dollars (Reuters News Service, 2001). Des sites de jeu Internet au Royaume-Uni, en Europe, en Amérique du Nord et aux Antilles ont également été victimes d'attaques de déni de service : à l'aide d'un virus, des pirates installent une *trappe* dans des ordinateurs personnels, par laquelle ils introduisent des *bots*. Ces ordinateurs manipulés, appelés *zombies*, peuvent être activés à volonté à l'insu de leur propriétaire. Des milliers de tels zombies sont mis en réseau et activés d'un coup pour submerger certains sites Internet qui n'ont d'autre choix que de refuser le service à des clients légitimes. Des entreprises comme Canbet, Harrods Casino, Inter Bingo, Inter Casino Poker, Totalbet, VIP Casino, William Hill, Paddy Power, Corals et Blue Square, pour ne nommer que celles-là, ont été obligées de fermer leurs sites et d'interrompre leur service pour des heures, voire des jours durant. Une équipe de pirates a causé notamment pour 70 millions de dollars de dommages aux preneurs de paris (*bookmaker*) britanniques. Ces cyberattaques sont étroitement reliées au cyberhameçonnage, où des pirates clonent un site de jeu, envoient des courriels à des joueurs les incitant à jouer sur ces sites frauduleux, ou encore se livrent à l'extorsion d'entreprises de jeu, exigeant des dizaines de milliers de dollars en paiement de protection contre de futures attaques (Biever, 2004 ; Kramerenko, 2004 ; Service canadien de renseignements criminels, 2000 ; Nuttall, 2004 ; Smith, 2004 ; Eriksson, 2004 ; Golubev, 2005 ; Germain, 2004 ; Reuters News Service, 2004). Comme le disait le directeur d'une entreprise de sécurité internationale : « Les gangs de malfaiteurs informatiques [...] collectent de l'argent de 10 % à 15 % des entreprises qu'ils menacent » (Cullingworth, 2004 : 3).

De nombreuses cyberattaques sont des *projets* en soi. Dans le cas du piratage des ALV, chaque attaque présupposait une planification parti-

culière, axée sur la réduction du risque de détection de l'événement criminel (McIntosh, 1975). Les pirates ont longuement sondé les forces et faiblesses des appareils et des sites Web avant de passer à l'acte et corrigé les défaillances de leurs propres logiciels de simulation de façon à réduire le temps d'attaque contre les appareils. Un agent de police a remarqué que les répétitions et l'utilisation de technologies puissantes ont permis à des pirates d'ALV de faire passer le délai de recherche des algorithmes de quatre heures à quelques minutes.

> Ils joueront trois ou quatre fois pour obtenir un échantillon qu'ils transmettent à leur complice dans la camionnette. L'ordinateur dans la camionnette était superpuissant, donc il y avait davantage de ressources pour déceler le code aléatoire... et ça n'a pris que quelques minutes du début à la fin. Une fois la machine ciblée, ils restent sur les lieux. Si ça prenait trop longtemps avant de commencer à gagner, ils changeaient de machine.

Les technologies de base exploitées pour trafiquer les ALV étaient partagées par un groupe de 12 ou 15 personnes qui établissaient les coûts d'exploitation, contrôlaient les échanges d'information et entreprenaient les attaques. On comptait dans ce groupe un expert technique qui planifiait les cyberattaques, des complices qui repéraient les appareils, communiquaient avec le centre nerveux (normalement, une camionnette garée stratégiquement ou une chambre d'hôtel), exécutaient les attaques et collectaient l'argent, et enfin des sentinelles. Les relations de travail étaient informelles et souples. Les membres ne participaient pas à toutes les attaques et les relations de parenté assuraient la confiance, le secret et la cohésion du groupe, de façon à maintenir les technologies de base dans l'ombre (Albini, 1971 ; Reuter, 1985 ; Smith, 1980).

Cette division du travail est semblable à celle de pirates d'appareils à sous qui sévissent à Las Vegas et à Atlantic City. Ils travaillent en groupes de 7 ou 8 personnes et combinent experts techniques et généralistes qui cernent et exploitent des parcours d'attaque relativement réguliers, profitables et à l'abri de toute inspection minutieuse (Crenshaw, 2003). Le piratage d'appareils en casino est également une affaire de famille, où l'on compte des experts dans les domaines de la programmation et de l'ingénierie. Ces équipes sont tricéphales : le premier vise un casino et un appareil de vidéo poker, le deuxième filme les images à l'écran à l'aide d'une caméra miniaturisée et les communique par ligne téléphonique au troisième qui consulte une base de données, calcule la périodicité des combinaisons gagnantes et transmet l'information au joueur en casino de

façon à ce qu'il puisse prévoir les gros lots. Leur méthode d'opération préconise une série de petits coups sur de nombreux appareils à différents endroits. Comme le disait un pirate : « L'essentiel de la logistique consistait à ne pas éveiller de soupçons et à se faire passer pour un joueur typique » (cité dans Mitnick et Simon, 2005 : 11).

Comme c'est souvent le cas, notre groupe de pirates encourait des frais de fonctionnement très modestes. Des ordinateurs portables, des composantes informatiques et des logiciels ainsi que des équipements vidéo et de communication étaient leurs plus grosses dépenses. Les mises, les frais de déplacement et d'hébergement représentaient des dépenses courantes mais mineures. Les groupes de pirates ne cherchent pas à réaliser des économies d'échelle, obtenir du financement externe ou annoncer leurs services (Reuter et Rubenstein, 1982). Ils travaillent plutôt à l'échelle locale, dans les corridors de fort trafic de la province (dans un rayon de 250 kilomètres) et dans des régions à forte densité de population. Les gains moyens par appareil se limitaient à un millier de dollars et les recettes totales pour quatre ans d'activité se chiffraient à quelque 500 000 dollars.

Bref, les criminels prônaient la multiplication de petites cagnottes faciles à prendre auprès d'un grand nombre d'appareils dispersés dans des endroits où ils pouvaient demeurer anonymes et revenir. Toutefois, comme c'est le cas pour tous les criminels, ils s'étaient entendus avec des marchands légitimes, les seuls capables de leur fournir des appareils de jeu dernier cri, des identificateurs de disque et des programmes capables de déchiffrer et manipuler les codes source et l'EPROM (Mitnick et Simon, 2005). Ces ententes entre marchands légitimes et hors-la-loi n'ont jamais atteint le stade d'*alliances dyadiques* stables aux fins de partage de profits, comme c'est le cas pour le négoce de drogues, de protection ou d'armes. De plus, comme tous leurs confrères également, nos criminels avaient mis au point des techniques qui leur permettaient de contourner et neutraliser les appareils policiers et législatifs. L'organisation sociale des fraudeurs d'ALV constituait une méthode de réalisation de modestes gains plutôt qu'une organisation complexe (Albini, 1971 ; Cressey, 1972). Selon un agent de police : « S'ils n'ont pas causé davantage de dommages, c'est qu'ils ne se rendaient pas compte de leur puissance, ou encore, qu'ils ne s'intéressaient qu'à gagner de petites sommes par-ci par-là pour se faire un peu d'argent d'extra ou pour voyager ».

La réponse réglementaire au piratage d'ALV

Le succès des opérations de piratage dépend de la compétence technique et du sens de l'organisation des malfaiteurs, mais aussi de l'incapacité de l'État et du secteur à les entraver. L'application de la loi est de compétence partagée : GRC, administrations provinciales ou interprovinciales des jeux, polices régionale ou municipale et agences de sécurité privées (par ex. : personnel de casinos ou propriétaires d'ALV et leur personnel). La GRC intervient en cas d'infractions de jeu criminelles, recueille des renseignements de nature criminelle et les partage avec d'autres agences d'application de la loi. Les polices municipale et régionale chargent leurs escouades mondaines et des mœurs de faire enquête en matière de jeu. Des commissions de jeu provinciales et interprovinciales réglementent les activités de jeu autorisées et font enquête sur les violations présumées pour assurer l'intégrité du secteur. Le personnel des points de jeu supervise l'aspect financier et participe aux opérations de sécurité (Smith et Wynne, 1999).

Cela dit, il y a chevauchement des rôles et peu de coordination. La GRC et les polices régionales manquent de personnel formé, et les rares escouades spéciales sont trop souvent sous-financées. Les stratégies policières préventives comme le contrôle des points de jeu sont inutiles en raison de la difficulté d'accès aux sites de jeu. Les commissions de jeu sont certes spécialisées et très compétentes, mais elles ont encore moins de ressources que les instances publiques (Smith *et al.,* 2003 : 89-91). Résultat : le contrôle de première ligne échoit à des employés du privé ou d'agences de sécurité qui travaillent sans formation particulière dans une myriade de clubs, bars, tavernes et autres locaux. Comme le soulignait un policier :

> La protection de l'équipement, à savoir des ALV, 649 appareils, des billets de loto ou n'importe quel autre actif, est une tout autre chose que la protection d'un casino, où tout se trouve sous un même toit [...] C'est une autre paire de manches. Certains nous décrivent comme un minicasino distribué sur 2 000 points de jeu [...] Il est donc très difficile d'assurer la protection des actifs dans de telles conditions [...] Le meilleur procédé est encore de sensibiliser les propriétaires des points de jeu. Lorsqu'on installe un ALV, le propriétaire des lieux doit en être responsable.

Des centaines d'exploitants, de gérants et d'employés de sites doivent assurer l'interdiction du jeu aux mineurs, enrayer la tricherie et le vol, et assurer la sécurité des clients. Certains sites d'ALV sont dotés de caméras

de surveillance à cet effet, mais dans la plupart, la surveillance se borne à être attentif et à l'affût de comportements suspects. Comme l'explique un agent de police :

> À la différence des casinos, dans les bars ou dépanneurs du coin, les appareils sont accessibles jour et nuit, et il est rare qu'on y trouve un agent consacré au contrôle et à la surveillance du jeu [...] Donc, où que se trouve l'appareil, les malfaiteurs y ont accès et peuvent tenter de le manipuler.

Bref, la structure d'application de la loi est décentralisée, réactive et éloignée des sites de jeu. Les autorités répondent aux plaintes et dénonciations, mais n'entreprennent pas d'enquête de leur propre chef (Smith et Wynne, 1999 : 75).

Le problème du déploiement des ressources est une autre entrave à la lutte contre le piratage des ALV. Tous les niveaux d'administration publique n'ont que de faibles ressources à consacrer aux activités liées au piratage : dépistage des activités illégales, enquête, constitution de dossiers de preuves, détermination des accusations, assistance aux procureurs et temps de témoignage devant les tribunaux. Pour cette raison, les agents spécialisés en enquêtes liées au jeu sont chose rare et le corpus de connaissances sur le piratage et la fraude est très maigre. Certes, le nombre de responsables chargés de la réglementation et d'enquêteurs provinciaux et interprovinciaux a augmenté à la suite de la popularisation du jeu légal, mais pas de façon proportionnelle et non sans heurts. Le nombre total actuel d'enquêteurs demeure modeste : ils sont 11 par province dans l'Ouest du Canada et seulement 6 en Atlantique. En Nouvelle-Écosse, il y a un enquêteur pour 539 ALV et 100 points de jeu. Dernièrement, les commissions de jeu provinciales ont pris sur elles des responsabilités qui incombaient à la police et assumé un rôle clé dans l'application de la loi sur le jeu. Malheureusement, cette initiative s'est soldée par la confusion dans les mandats et programmes réglementaires et l'immobilisme interagences. Enfin, malgré la multiplication des produits de jeu disponibles, il y a eu une diminution des contrôles sociaux et une réduction de l'intérêt pour la lutte contre les crimes liés au jeu (Smith *et al.,* 2003 : 89-90).

Autre problème : les ALV sont surveillés par les autorités et commissions provinciales et interprovinciales par voie électronique à l'aide de connexions Internet à accès commuté. Dans la région de l'Atlantique, la société des loteries approuve les propriétaires de points de jeu et les lieux, les fabricants et distributeurs qui vendent les appareils et en font

la promotion, ainsi que les normes d'exploitation et spécifications des jeux. La connexion Internet permet d'enregistrer les appareils et de contrôler les utilisations tant normales qu'irrégulières. Toutefois, ce contrôle n'est pas effectué en temps réel.

> Nous constatons les fraudes qu'avec jusqu'à 24 heures de retard, car nous ne vérifions les ALV qu'une fois par jour. Chaque appareil stocke chaque événement en mémoire en attendant le téléchargement de cette mémoire dans notre système central [...] Ainsi, si jamais il y a une irrégularité [...] nous pouvons examiner les données. Donc il (le système) est en mode contrôle plutôt que prévention. En d'autres mots, si quelqu'un accède au secteur logique de l'appareil, nous ne le savons pas immédiatement, mais plutôt après le fait [...] S'il n'y a rien qui saute aux yeux des techniciens qui vérifient la mémoire, alors nous (la Commission des jeux) pourrions être ignorants de tout problème jusqu'à l'apparition de certaines irrégularités, comme des paiements trop fréquents, par exemple.

Une récente arnaque menée par un groupe de 5 ou 6 malfaiteurs consistait à utiliser un ALV pendant une courte période, le temps d'obtenir des billets gagnants de 5 $ ou 10 $, à numériser et copier ceux-ci en changeant les montants pour 300 $ ou 400 $ et à retourner au point de jeu pour toucher la nouvelle somme. Aucun système de sécurité n'a pu repérer l'arnaque (Arsenault, 2005 : B2). Les dispositifs de sécurité sont aussi facilement contournés dans le cas de vols de produits de loterie :

> Parfois, on a des situations où il manque de l'argent, dans l'ordre des milliers de dollars [...] nous ne participons pas activement au dépistage du voleur [...] le plus souvent, ils ont la collaboration d'un complice au point de jeu qui reçoit nos feuilles de résultats et qui s'assure que l'argent y est. Ils ne conservent pas les bandes de vérification, ils détruisent les feuilles de résultats et, bien entendu, ils pigent dans la caisse.

Nous avons conclu à l'inefficacité des mesures préventives et dissuasives comme les normes mécaniques, les politiques d'utilisation, les spécifications techniques, les inspections (Bayley et Shearing, 1998 ; Reiss, 1984). En effet, plusieurs normes ont été compromises et des violations d'appareils de jeu n'ont pu être détectées par le système de sécurité des autorités. Par exemple : a) on a réussi à manipuler des boutons pour autoriser la continuation du jeu après que l'agent de réglementation en ait demandé la cessation : l'exploitant des lieux ne maîtrisait pas complètement ses appareils ; b) en enfonçant de façon continue les boutons de règles ou de mise, on a interrompu la transmission au responsable de

la réglementation des données sur les ouvertures des trappes d'accès de façon à ce que l'ALV demeure hors ligne et invisible aux autorités. En effet, les alarmes sonores protégeant l'accès aux trappes d'accès des appareils pouvaient tomber en panne et les appareils ne rétablissaient pas toujours les paramètres de fonctionnement avant l'ouverture de l'accès, ce qui facilitait la fraude ; c) les appareils ne respectaient pas la limite de versement de 1 000 $. Certains appareils autorisaient des versements bien supérieurs à ceux stipulés par la loi, de sorte que les fraudeurs renseignés pouvaient doubler leurs gains ; d) les produits ne suivaient pas les processus de vérification de signature à l'activation et l'acceptation. Les appareils passaient outre des vérifications continues de la mémoire morte et fonctionnaient de façon indépendante et contournaient leurs propres mesures de sécurité logicielles ; e) les appareils ne fonctionnaient pas toujours correctement après le remplacement de l'EPROM. Les vérifications de signature n'étaient pas bien effectuées par le logiciel qui passait outre des données de stockage et de protocole importantes. Les autorités n'étaient donc pas alertées des actes de piratage ; f) les appareils ne reconnaissaient pas les mémoires corrompues et ne les validaient pas après chaque partie, ce qui, une fois de plus, permettait aux fraudeurs de passer inaperçus ; g) les connexions de compteur n'étaient pas physiquement protégées, de sorte que quiconque pouvait les manipuler et se livrer à la fraude à l'abri de toute détection ; enfin, h) les puces informatiques échouaient aux tests aléatoires de deux façons : elle n'étaient pas fiables à 99 % pour la production de combinaisons de symboles aléatoires et pour l'indépendance des positions des chiffres d'une partie à l'autre. Sachant cela, les fraudeurs pouvaient exploiter les générateurs de chiffres aléatoires afin d'optimiser leurs gains.

L'échec des dispositifs de sécurité n'est qu'un aspect du problème : il y a aussi le mode d'opération des groupes frauduleux, qui neutralise la capacité de la police d'assurer une surveillance. En effet, les bandes de malfaiteurs préparent minutieusement leurs attaques. Les points, circuits et périodes d'attaque ne suivent aucune logique, ce qui empêche les autorités de prévoir les attaques et les entrave dans leur enquête (Griffiths *et al.,* 1999). De plus, les autorités ne disposent pas d'assez d'unités de crime informatique et celles-ci n'ont pas assez de soutien administratif ni d'outils d'enquête efficaces (Stambaugh *et al.*, 2001 ; Surin, 2005). Comme l'explique McIntosh (1975 : 42-50), ces criminels se caractérisent par la constitution d'équipes criminelles très compétentes pour attaquer des actifs de grande valeur et bien protégés, à tel point qu'ils créent

des organisations criminelles stables mais éphémères, résistantes à toute détection ou dissuasion.

Les cyberpirates ont enfin été détectés par des employés de bar qui ont accidentellement découvert les caméras miniaturisées et l'équipement de communication après qu'une modification du profil des paiements leur ait mis la puce à l'oreille. « On ne les aurait peut-être pas découverts [...] s'ils s'étaient contentés de cagnottes de 500 $, d'expliquer un agent de la loi, mais ils jouaient pour 1 000 $, même 1 900 $ à la fois [...] les commerçants ont flairé l'arnaque. » Ces soupçons ont donné lieu à une opération clandestine de neuf mois et à l'arrestation de deux pirates. L'un des agents en cause explique :

> Mon partenaire et moi devions franchir un pont pour atteindre les lieux, et nous y sommes arrivés assez vite [...] Nous avons observé l'un des suspects s'accoutrer d'équipements (veste, pile, oreillette, etc.) dans un stationnement. Nous avons aussi repéré un autre suspect à l'arrière d'une camionnette dans le même stationnement [...] Tandis que le premier suspect se dirigeait vers le commerce, nous avons posté un des nôtres à l'intérieur et nous avons pu observer qu'il jouait tout en se parlant tout seul. Peu après, l'écran de la machine a commencé à afficher d'importantes cagnottes.

La police a saisi la ligne téléphonique reliant l'appareil au registre central, gelé les comptes et confisqué l'équipement des pirates sur les lieux et à leur domicile. Par la suite, les pirates ont fait une démonstration de leur méthode pour des experts en sécurité et informatique qui ont tout enregistré sur vidéo. Un agent de police se rappelle comment « [...] ils nous ont prévenus de ne pas toucher à l'ordinateur, car nous l'aurions bloqué et perdu toutes les données [...] S'ils s'étaient tus, nous n'aurions pas pu les inculper de quoi que ce soit, car la preuve aurait été anéantie ». Les pirates ont été condamnés en vertu de l'article 342.1 (1) (b) du Code criminel pour utilisation illicite d'un ordinateur, de programmes informatiques, de données informatiques et d'équipements mécaniques en vue de frauder un ALV. Les 2 pirates ont reçu une libération conditionnelle et un an de probation. Comme l'explique un représentant des autorités, « nous avions ce que nous voulions, c'est-à-dire leurs connaissances ; les malfaiteurs ont été traduits en justice [...] il s'agissait d'accusations assez mineures et nous ne voulions pas ébruiter la chose ».

Sécurité, politique publique et protection du consommateur

La présente étude, ainsi que d'autres études sur le jeu illégal, la tricherie et la corruption soulèvent des questions importantes sur la capacité de l'État à réglementer et contrôler l'un des produits les plus lucratifs sur le marché du jeu. Jusqu'ici, les mesures d'application et de respect de la loi ont été si futiles qu'elles ont eu pour effet de protéger les intérêts des fabricants et des distributeurs avant ceux des consommateurs. Les joueurs n'ont reçu aucune information sur le piratage, les autorités n'ont diffusé aucun message d'intérêt public et les appareils n'ont pas été rappelés, et ce, même lorsque les fraudes présentaient un risque important et qu'elles auraient pu être entreprises par des pirates moins compétents. Bref, la considération *revenu* primait sur les dommages, et celle de la confidentialité sur la transparence. Pourtant, les clients ont droit à l'information lorsqu'ils font des achats relativement à des appareils de jeu, et un mécanisme de suivi et de contrôle transparent est à la base de tout système de dépistage et de prévention de la criminalité, de protection du consommateur et d'application de la loi. Les autorités devraient lancer une campagne de sensibilisation à la sécurité auprès des joueurs, du secteur industriel et du gouvernement, comme elles l'ont fait pour le jeu responsable et la réduction des dommages (Gray, 2005 : 1).

L'éclosion du piratage, de la fraude et de l'extorsion justifie le retrait des appareils de jeu du domaine public afin de les regrouper dans quelques points de jeu réservés. Cette solution comporte plusieurs avantages : réduction de la facilité d'accès ainsi que des risques de dépendance au jeu ; facilitation de l'installation et de l'utilisation de dispositifs de protection des consommateurs comme les cartes d'identification et les systèmes d'homologation et de suivi (Dickerson, 2003a ; 2003b) ; amélioration de la sécurité des produits, des conditions de jeu et de versements, ainsi que de l'environnement de jeu, par l'entremise de dispositifs de surveillance électronique et humaine ; capacité des autorités à dépister les pirates par des méthodes de vérification, de caméras en circuit fermé, de surveillance clandestine ; enfin, optimisation de la concentration, du partage et du déploiement des agents et ressources (McMullan, 2005 : 23).

Le piratage récurrent des appareils de jeu a des répercussions sur le montant et la fréquence des gros lots, puisque les joueurs légitimes n'ont plus les mêmes chances de gagner. Nos recherches nous ont permis de constater que, malgré les vérifications préliminaires et l'apposition d'un

sceau d'approbation, ce sont les autorités les premières à être trompées par leur propres générateurs de nombres aléatoires et que celles-ci ne s'en aperçoivent qu'après intrusion et prédiction. Donc, la question initiale se pose toujours : comment faire en sorte qu'un générateur de nombres aléatoires soit suffisamment aléatoire ? Comment assurer l'équité et garantir que le jeu demeure équitable après la vérification initiale ? Réponse : davantage de tests exhaustifs ! Les tests fondés sur les résultats, c'est-à-dire qui contrôlent statistiquement la production du générateur de nombres aléatoires, doivent être complétés de tests objectifs, soit une inspection interne méthodique du générateur de nombres aléatoires. Ces deux genres de tests conjugués sont la meilleure garantie de l'intégrité, de la fonctionnalité et de la protection des appareils, surtout lorsqu'on ajoute des tests annuels calibrés de mesures de base et des inspections annuelles aléatoires afin de repérer les terminaux illicites, les modifications illégales et les logiciels corrompus (Bourie, 1999 ; Technical System Testing, 2005). En fait, la sécurité est une question de rapidité, en raison des attaques éclair qui s'abattent sur la première cible qui s'y prête. À l'ère de la guerre informatique et de la cybercriminalité, les assaillants ont l'avantage de l'effet de surprise et n'ont donc pas besoin de technologies aussi évoluées que les victimes pour s'en prémunir. Les autorités chargées de la réglementation n'arrivent plus à faire face au problème (Kessler, 2000) et, comme le prévient le directeur de l'entreprise Internet Security Systems : « Les logiciels imprenables n'existent tout simplement pas. Il y aura toujours des brèches à la merci des pirates » (Gray, 2005 : 1). Paradoxalement, la plupart des recherches sur l'intrusion, les codes malveillants, les puces informatiques truquées, le déchiffrement et les attaques par déni de service distribué (*DDos attacks*) se font par des malfaiteurs pour pirater plutôt que par des institutions pour s'en défendre.

Toute stratégie de protection du consommateur doit se fonder sur la prémisse que le jeu peut représenter un divertissement à risque et que les appareils de jeu électronique peuvent fonctionner de façon inéquitable après leur installation dans un point de jeu. Les autorités doivent effectuer des tests directs, entreprendre des recherches pour déceler dans les appareils toute fonctionnalité qui puisse accrocher les joueurs ou les tromper quant à leurs chances de gagner ou de dominer le jeu. Pendant ce temps, les systèmes de surveillance en ligne s'avèrent le meilleur moyen de protéger les joueurs. En effet, ces systèmes renforcent les dispositifs de sécurité et autorisent un contrôle souple en temps réel, notamment la possibilité de vérifier les signatures de validation de logiciels et

matériels sur l'ensemble du système (par ex. : cage de protection de trappe d'accès, accès à la zone logique, EPROM et mémoire critique). Ces dispositifs protègent les consommateurs des risques et arnaques. Comme l'exprimait très justement un expert technique, mieux vaut pour le gouvernement « de subir une mise à niveau de logiciel que les critiques de la presse, la colère des groupes contre le jeu ou l'embarras d'une poursuite judiciaire », voire même la perte de sa police d'assurance (Technical System Testing, 2001 : 3). Lorsque des défaillances de produits sont découvertes, au lieu d'en faire un secret ou de détruire la preuve, il faut tout simplement retirer les appareils en cause, corriger le problème et, au besoin, conserver précieusement l'information à des fins de preuve ou d'avis au public.

Les gouvernements provinciaux ont un monopole sur le jeu en vertu de modifications apportées au Code criminel en 1969, 1985 et 1998. Les sections applicables du Code leur permettent de mettre sur pied et d'exploiter des loteries, y compris les jeux de hasard sur ordinateurs, appareils vidéo, ou appareils à sous, jeux par téléphone et jeux de dés. En tant qu'exploitants, ils doivent optimiser leurs revenus et en tant que chargés de la réglementation, protéger le bien public. Ce qui les met dans une position difficile : s'ils déploient de nouvelles mesures de sécurité, ils reconnaissent par le fait même que les jeux n'ont pas été assez protégés et que le coût du jeu devra augmenter, et les profits, diminuer. Par contre, si les revenus priment, les consommateurs risquent d'être mal protégés et le bien public en souffrira. Si les gouvernements tiennent à conserver et à exploiter des produits de jeu, ils devront remettre en question leur rôle de mandataire de la réglementation. Jusqu'ici, l'autoréglementation du jeu par les provinces s'est soldée par un manque de transparence, de responsabilité et d'uniformité de la sécurité et par l'évacuation de considérations comme l'impact à long terme sur les consommateurs et le public. Citons à cet effet Campbell et ses collaborateurs (2005 : 54) :

> L'intérêt des provinces dans les appareils de jeu électronique soulève des questions de conflit d'intérêts [...] Comme les corps de police n'ont pas l'expertise technique pour faire enquête sur l'intégrité des machines de jeu, ils se rabattent sur des conseillers des autorités de jeu provinciales, celles-là même qui approuvent les appareils, ou encore des fabricants. Il y a lieu de remettre en question la pertinence et l'indépendance du système de freins et contrepoids du processus de réglementation.

Des fraudes récentes en Alberta, en Colombie-Britannique, au Manitoba et en Saskatchewan ont été découvertes grâce à des audits provin-

ciaux, non pas par les corporations ou commissions de jeu provinciales. Pour supprimer les situations de conflit d'intérêts, réelles ou apparentes, il faut que des commissions de jeu indépendantes contrôlent la sûreté des produits autorisés, administrés, vendus et exploités par le gouvernement. Les responsabilités assumées actuellement par les commissions et corporations existantes doivent être cédées à des commissions indépendantes dotées de pouvoirs de surveillance semblables à ceux des vérificateurs généraux. Ces commissions seraient composées d'experts dans les domaines de la prévention, du droit et de la sûreté, de la thérapie, des services sociaux et de la recherche.

La principale responsabilité en matière de sûreté de la commission indépendante serait de concevoir et de contrôler des dispositifs de sûreté indépendants et objectifs qui répondraient de façon satisfaisante aux questions suivantes : a) *Conception, intégrité et fonctionnalité des jeux électroniques* : fonctionnent-ils correctement ? Sont-ils conçus de façon à favoriser la sûreté du jeu et à décourager le jeu compulsif ? Les codes source sont-ils vérifiés contre toute anomalie, par exemple, les *œufs de Pâques*, les codes malveillants, etc. ? b) *Emplacement des jeux électroniques* : sont-ils installés dans des sites exclusifs et sûrs favorisant le jeu responsable et décourageant les comportements risqués ou compulsifs ? c) *Signalisation et règles de jeu* : les affiches donnent-elles l'information exacte et sont-elles placées bien en vue ? d) *Procédures de relance des appareils* : le jeu reprend-il normalement lorsque l'appareil est éteint ou paralysé temporairement ? e) *Processus actuariels* : les paris, gains et pertes sont-ils tous bien comptabilisés ? f) *Processus de résolution des différends* : existe-t-il des processus et éléments de preuve pour résoudre les litiges ? g) *Protection des renseignements personnels* : les données personnelles sont-elles à l'abri du regard du gouvernement et d'autres intervenants ? h) *Protection des consommateurs* : existe-t-il des procédures de contrôle des paris, de désactivation des comptes joueurs et d'autoexclusion ? Les appareils sont-ils conçus de façon à encourager les comportements sûrs et non compulsifs ? i) *Processus de promotion et de publicité* : existe-t-il des garanties que les promotions et publicités sont justes et exactes et qu'elles ne contribuent pas aux pratiques malhonnêtes ou comportements à risque ? Cette restructuration organisationnelle favoriserait les vérifications indépendantes et assurerait que les autorités et responsables d'enquêtes se portent garants pour l'ensemble du public et pas simplement pour les gouvernements ou le secteur industriel.

Enfin, le problème de la sécurité soulève une question fondamentale sur le rôle du Code criminel quant aux jeux de hasard au Canada. Comme le jeu n'est plus l'objet d'interdiction criminelle et que des lois ont été adoptées pour consolider et légitimer les monopoles expansionnistes des gouvernements provinciaux (et ce sera de plus en plus vrai au fil de l'essor du jeu sur Internet), il n'y a plus de raison de contrôler le jeu comme par le passé (Campbell *et al.,* 2005 : 81-85). Il est temps que les gouvernements adoptent des lois sur le jeu responsable, qui reconnaissent que le jeu constitue un comportement à risque et qu'il devrait être interdit sans la prise de mesures comme le renversement du fardeau de la preuve et la réduction des dommages. On ne peut plus se contenter de mettre des produits de jeu à risque sur le marché et s'attendre à ce que le fardeau de la preuve, quant au niveau de risque, soit soutenu par des exploitants et des responsables de la réglementation sans ressources. La sécurité devrait passer en premier et le jeu responsable devrait être défini de telle façon que les consommateurs puissent s'y livrer de façon sûre, honnête et informée sans craindre de se faire arnaquer par des appareils qui les incitent à jouer à outrance. Les dommages, eux, doivent être définis de manière très large de façon à tenir compte de tout préjudice lié au comportement de jeu des joueurs, de leur situation personnelle, sociale ou économique, de la famille et des collectivités (Secker, 2005). Des lois de jeu responsable seraient un outil utile pour les ministères comme la santé, le bien-être et les services sociaux dans l'élaboration de stratégies de réduction des dommages et des traitements ; de plus, ils donneraient des pouvoirs exclusifs aux commissions indépendantes pour réglementer les exploitants d'appareils de jeu, les points de jeu, les normes mécaniques des appareils, les normes de casino, les règles de jeu et les enquêtes et vérifications de sécurité des produits et opérations de jeu. Sous ce régime réglementaire, les gouvernements ne pourraient pas accorder de permis sans la satisfaction préalable de normes de protection du consommateur, de réduction des dommages et d'assurance de l'équité.

À l'avenir, la sécurité du jeu sera tributaire du jeu de la sécurité. Le piratage et la fraude menacent ce secteur de l'intérieur et de l'extérieur. Pour assurer la sécurité, il faudra vaincre la culture du déni qui caractérise le secteur aujourd'hui. Les gouvernements, premiers bénéficiaires des profits du jeu, doivent défendre le bien public par un système de sécurité et de réglementation autonome, transparent et responsable, et par un système d'application de la loi sérieux et actif dans son devoir de

protéger les consommateurs. Enfin, le processus d'achat dans son ensemble devrait non seulement protéger les consommateurs de ce que Dickerson (2003a) appelle les *formes continues de jeu* qui leur nuisent, mais aussi de ce qu'on appelle les *défaillances de conception, d'intégrité et d'exploitation* qui les trompent.

Références

Albini, J. (1971). *The American Mafia : Genesis of a legend.* New York, Appleton : Century Crofts.

Arsenault, D. (2005, 27 avril). Scam Involves Crooks Altering Winning Tickets. *Halifax Chronicle Herald*, B-2.

Azmier, J., Kelley, R. & Todosichuk, P. (2001). *Triumph, Tragedy or Tradeoff? Considering the Impact of Gambling, Gambling in Canada Research Report. 14.* Calgary : Canada West Foundation.

Bayley, D. & Shearing, C. (1998). The Future of Policing. In G. Cole & M. Gertz (ed.), *The Criminal Justice System : Politics and Policies* (7e éd. : 150-167). Belmont, Canada : West/Wadsworth éditeurs.

Biever, C. (2004, novembre). *How Zombie Networks Fuel Cyber Crime.* Consulté le 5 juin 2005. www.newscientist.com.

Blackwell, T. (2005, 7 mars). Charges Raise Specter of VLT Cheating. *National Post*, A4.

Blackwell, T. (2004, 12 juillet). Easter Egg Cheats Cracking Casinos ? *National Post, Information Security News.* Consulté le 2 mai 2005. www.seclist.org.

Bourie, S. (1999). *Are Slot Machines Honest ?* Consulté le 20 mai 2005. www.americancasino.com.

Campbell, C., Hartnagel, T. F. & Smith, G. (2005, 7 mars). *The Legalization of Gambling in Canada.* Rapport préparé pour la Commission du droit du Canada, Ottawa.

Campbell, C. & Smith, G. (1998). Canadian Gambling : Trends and Public Policy Issues. *Annals American Academy of Political and Social Sciences, 556*, 22-35.

Crenshaw, D. (2003, 11 août). Slot Machine Cheat Bilked Casinos with Ingenious Gadgets, *U.S.A. Today.* Consulté le 24 mai 2005. www.usatoday.com/tech.

Cressey, D. (1972). *Criminal Organization : Its Elementary Forms.* Londres : Heinemann.

Cullingworth, B. (2004, avril). *Distributed Denial of Service Attacks No Joke.* Consulté le 5 juin 2005. www.winjneronline.com.

Dickerson, M. (2003a). *Exploring the Limits of "Responsible Gambling" : Harm Minimisation or Consumer Protection ?* Actes de la 12e conférence annuelle de la National Association for Gambling Studies, Melbourne, Australie.

Dickerson, M. (2003b). *What if there were no Problem Gamblers?* Rapport présenté en mai à la 12e Conférence internationale sur le jeu et les risques, Vancouver, Canada.

Eadington, W. R. (1996). *Ethical and Policy Considerations in the Spread of Commercial Gambling.* In J. McMillan (ed.), *Gambling Cultures* (243-262). New York : Routledge.

Eriksson, H. (2004). Russian Hackers Nearly Ruined British Bookmakers, *Gambling Gates.* Consulté le 21 avril 2005. www.gamblingates.com.

Germain, J. M. (2004, 23 mars). Global Extortion, Online Gambling and Organized Hacking, *TechNewsWorld.* www.technewsworld.com.

Golubev, V. (2005, mars). *DOS Attacks : Crime without Penalty.* Consulté le 5 juin 2005. www.crime-research.org.

Goodman, R. (1995). *The Luck Business : The Devastating Consequences and Broken Promises of America's Gambling Explosion.* New York : Free Press.

Gray, P. (2005). *Hackers : The Winds of Change.* Consulté le 5 juin 2005, www.iss.net.

Griffiths, C. T., Whitelaw, R. & Parent, R. B. (1999). *Canadian Police Work.* Scarborough, Ontario : International Thompson.

Kessler, G. C. (2000, novembre). Security at the Speed of Thought, *Information Security Magazine.* Consulté le 26 janvier 2006. www.infosecuritymag.com.

KPMG (2004). *Canadian Gaming Industry Highlights.* Toronto : KPMG.

Kramerenko, D. (2004, 29 juillet). Russian Hacker Blackmailed Gambling Companies, *Computer Crime Research Centre.* Consulté le 21 avril 2005. www.Crime-research.org/news.

MacDonald, M., McMullan, J. L. & Perrier, D. C. (2004). Gambling Households in Canada. *Journal of Gambling Studies, 20* (2), 187-236.

Mandel, C. (2000, 23 juin). Revenge on the one armed Bandit. *Wired News.* www.wired-vig.com

Marshall, K. & Wynne, H. (2004). *Le point sur les jeux de hasard, L'emploi et le revenu en perspective.* Catalogue 75-001-XIF, Ottawa : Statistiques Canada.

McIntosh, M. (1973). The Growth of Racketeering. *Economy and Society, 2*, 35-69.

McIntosh, M. (1975). *The Organization of Crime.* Londres : MacMillan Press.

McMillan, J. (1996). From Glamour to Grind : The Globalization of Casinos. In J. McMillan (ed.), *Gambling Cultures : Studies in History and Interpretation* (263-287). Londres : Routledge.

McMullan, J. L. (2005, 31 mars au 1er avril). *The Gambling Problem and Problem Gambling : Research, Public Policy and Citizenry.* Rapport présenté à la *4th Annual Alberta Conference on Gambling Research, Public Policy Implications of Gambling Research*, Université de l'Alberta.

McMullan, J. L. & Perrier, D. C. (2003). Technologies of Crime : The Cyber-Attacks on Electronic Gambling Machines. *Revue canadienne de criminologie et justice pénale, 45* (2), 159-186.

Mitnick, K. D. & Simon, W. L. (2005). *The Art of Intrusion : The Real Stories behind the Exploits of Hackers, Intruders and Deceivers*. New York : Wiley.

Nuttall, C. (2004, 23 février). Hackers Blackmail Internet Bookies. *Financial Times*. Consulté le 21 avril 2005, www.ft.com.

Orum, A., Feagin, J. & Sjoberg, G. (1991). The Nature of the Case Study. In J. Feagin, A. Orum & G. Sjoberg (ed.). *A Case for the Case Study* (1-26). Chapel Hill : University of North Carolina Press.

Reiss, A. (1984). Selecting Strategies of Social Control over Organizational Life. In K. Hawkins & J. M. Thomas (ed.), *Enforcing Regulation* (23-36). Boston : Kluwyer-Nijhoff Publications.

Reuter, P. (1985). *The Organization of Illegal Markets : An Economic Analysis*. Washington, DC : US Government Printing Office.

Reuter, P. & Rubenstein, J. (1982). *Illegal Gambling in New York : A Case Study of the Operation, Structure and Operation of an Illegal Market*. Washington, DC : US Government Printing Office.

Reuters News Service (2001, 10 septembre). *Hackers Win High Stakes at Gambling Sites*. Consulté le 21 avril 2005, www.news.com.

Reuters News Service (2004, 17 mars). *Hackers Attack William Hill after $10,000 Blackmail Threat*. Consulté le 21 avril 2005, http://networks.silicon.com/webwatch.

Rosoff, S. M., Pontell, H. N. & Tillman, R. H. (2002). *Profit Without Honor : White-Collar Crime and the Looting of America*. Upper Saddle River, NJ : Prentice-Hall.

Secker, A. (2005, 31 mars – 1er avril). *How and Why New Zealand Revamped its Gambling Regulatory Scheme*, Rapport présenté à la *4th Annual Alberta Conference on Gambling Research*.

Service canadien de renseignements criminels (2000). *Technologie et criminalité, rapport annuel*. Consulté le 5 juin 2005, www.cisc.gc.ca.

Skolnick, J. H. (1980). *House of Cards : Legalization and Control of Casino Gambling*. Boston : Little, Brown and Company.

Smith, D. C. (1980). Paragons, Pariahs and Pirates : A Spectrum Based Theory of Enterprise. *Crime and Delinquency, 26*, 358-386.

Smith, G. J. & Azmier, J. (1997). *Gambling and the Public Interest*. Calgary, Alberta : Canada West Foundation.

Smith, G. J. & Wynne, H. (1999). *Gambling in Canada, Triumph, Tragedy or Trade-off?* Calgary : Canada West Foundation.

Smith, G. J., Wynne, H. & Hartnagel, T. (2003). *Examining Police Records to Assess Gambling Impacts : A Study of Gambling Related Crime in the City of Edmonton*. Edmonton : Alberta Gaming Research Institute.

Smith, K. (2004, 8 mars). Extortionists Target Online Gaming Sites. *Interactive Gaming News*. Consulté le 21 avril 2005. www.riverheard.com.

Stambaugh, H., Icove, D. J., Beaupre, D. S., Baker, R., Cassaday, W. & William, W. P. (2001). *Electronic Crime Needs Assessment for State and Local Law Enforcement*. Washington, DC : National Institute of Justice.

Surin, A. J. (2005). *To Catch a Cybercriminal*. Consulté le 5 juin 2005, www.crime-research.org.

Technical Systems Testing (2005). *Is your RNG taking YOU for a Ride : Why RNG Results may not always be what they appear to be*? Consulté le 31 mai 2005, www.tst.com.

The Gambling Magazine (2004, 27 novembre). *Sophisticated Gangs : Cheating Slot Machines across Country*. Consulté le 22 mai 2005, www.gamingmagazine.com.

The Gambling Magazine (2005, 15 mars). *Shoe Sparks Casino Probe*. Consulté le 22 mai 2005, www.gamingmagazine.com.