



PERTURBATION DES RÉSEAUX CRIMINELS

Il est plus efficace de perturber les réseaux criminels émergents.

Il est difficile d'élaborer des stratégies d'application de la loi efficaces pour contrôler et perturber les réseaux du crime organisé. Les données empiriques découlant d'analyses des réseaux sociaux montrent que bon nombre de réseaux criminels possèdent une fluidité et une flexibilité qui les aident énormément à résister aux stratégies traditionnelles d'application de la loi ciblant les dirigeants, ou « caïds », de l'organisation criminelle. La recherche illustre que les réseaux criminels se doivent d'être flexibles s'ils veulent se protéger des opérations visant à les perturber; or, on en sait peu sur la façon dont s'y prennent les réseaux criminels pour s'adapter à une attaque et s'en remettre.

Cette étude combine une analyse des réseaux sociaux avec une modélisation computationnelle afin de simuler le comportement d'un réseau illicite de culture du cannabis aux Pays-Bas. La culture organisée du cannabis par l'intermédiaire de réseaux illégaux est un problème auquel de nombreux pays sont confrontés, et les tentatives des responsables de l'application de la loi pour l'atténuer se soldent souvent par un échec. La recherche avait pour objectifs d'examiner la dynamique de la résilience des réseaux criminels face à la perturbation, ainsi que de déterminer la stratégie de perturbation la plus efficace. On a atteint ce dernier objectif en simulant les effets de cinq stratégies de perturbation différentes sur le réseau criminel à l'aide du modèle créé.

Les auteurs font la distinction entre deux approches courantes pour perturber un réseau criminel. L'approche axée sur le capital social cerne les acteurs au sein du réseau qui ont le plus de capital social, c'est-à-dire ceux qui occupent les postes ayant de

Dans ce numéro

Perturbation des réseaux criminels 1

Appliquer l'analyse des réseaux sociaux à la détection du blanchiment d'argent..... 2

Difficultés dans les opérations de lutte contre la cybercriminalité 3

La structure du marché des drogues synthétiques au Québec 5

Comprendre le développement des entreprises illégales 6

l'influence ou du pouvoir. Quoique cette approche soit utile, les réseaux criminels sont souvent dirigés par plus d'un acteur, dont certains n'occupent pas toujours les postes les plus centraux ou faciles à repérer. Quant à elle, l'approche axée sur le capital humain cerne les acteurs au sein du réseau criminel en fonction de leurs qualités individuelles, attaquant le réseau criminel en ciblant les acteurs qui possèdent les compétences et les connaissances les plus spécialisées et les plus utiles à la réalisation de l'activité illégale. Les auteurs emploient le terme « chaîne de valeur » pour désigner la structure rappelant une chaîne qui existe au cœur du processus opérationnel de tous les marchés criminels. Chaque étape d'une activité illégale nécessite différents niveaux d'information, de biens et de capital humain. Par conséquent, il est possible de cerner et de cibler les rôles qui sont utiles à la chaîne. Pour pallier ces stratégies, les réseaux criminels acquièrent la capacité de résister aux mesures visant à les perturber et de

s'adapter aux changements, s'il y a lieu. C'est ce qu'on appelle la résilience des réseaux criminels.

L'étude se fondait sur deux ensembles de données regroupés. Le premier ensemble se composait de renseignements recueillis par une unité travaillant pour la police néerlandaise de janvier 2008 à janvier 2012. Ces renseignements comprenaient des données au sujet du crime organisé collectées auprès d'informateurs et dans les rapports concernant les dossiers clos du crime organisé. Le deuxième ensemble se composait de dossiers d'arrestation dans la même région durant la même période. En combinant ces deux ensembles de données, les auteurs ont pu reconstituer la structure d'un réseau criminel exerçant des activités sur divers marchés criminels aux Pays-Bas.

Après avoir créé un sociographe du réseau criminel, les auteurs ont éliminé tous les acteurs n'ayant rien à voir avec la culture du cannabis. Ils ont alors établi une chaîne de valeur qui décrivait les rôles et le flux du capital humain dans le réseau de culture du cannabis. Ils ont constaté que certains rôles au sein de la chaîne étaient courants et étroitement liés (c.-à-d. facilement remplaçables), tandis que d'autres ne l'étaient pas. Selon leurs observations, les rôles de « coordonnateur » et de « propriétaire d'une installation de culture » constituaient des liens importants soudant la chaîne de valeur, ce qui en faisait des cibles vulnérables pour les deux méthodes de perturbation. Les auteurs ont également cerné comme étant vulnérable le rôle de « spécialiste », c.-à-d. une personne assumant un rôle hautement spécialisé comme la manipulation de l'alimentation électrique de l'installation de culture.

Les auteurs ont exécuté les simulations à partir des ensembles de données combinés, afin de mettre à l'essai les stratégies de perturbation couramment employées par les responsables de l'application de la loi et de déterminer la résilience du réseau criminel, dans le but de mesurer les effets sur le réseau. Ils ont utilisé deux méthodes axées sur le capital social, deux méthodes axées sur le capital humain et une méthode aléatoire. Pour modéliser les différentes façons dont les réseaux criminels se remettent d'une perturbation, les auteurs ont fait appel à trois algorithmes simulant différents moyens mis en œuvre par les réseaux criminels pour se remettre d'une perturbation. Ils ont ainsi observé qu'aucune des stratégies employées ne

réussissait à perturber le réseau. En fait, l'efficacité du réseau a augmenté dans certains cas, les stratégies de perturbation venant renforcer la résilience du réseau de trafic de drogue. Ces résultats illustrent la flexibilité et la structure adaptative du réseau de culture du cannabis, des qualités qui lui octroient une bonne capacité de résister aux stratégies de perturbation appliquées par les responsables de l'application de la loi.

L'étude révèle qu'il est plus efficace d'intervenir dans un réseau criminel récemment établi que dans un réseau en place depuis longtemps. Le phénomène où les stratégies de perturbation accroissent la résilience du réseau criminel s'explique probablement par le fonctionnement inefficace du réseau original, qui n'avait pas besoin d'évoluer ou de prendre de l'expansion : la stratégie de perturbation entraîne des conséquences qui forcent le réseau à se réorganiser d'une manière plus productive, d'où son efficacité accrue.

Les auteurs notent qu'« en pratique, il faut déployer un effort d'intervention constant à long terme pour arriver à perturber un réseau criminel » [Traduction] (14). Bien que les stratégies de perturbation puissent accroître l'efficacité du réseau à court terme, elles augmenteront graduellement sa visibilité au fil du temps, l'obligeant à sortir de l'ombre (14). Le réseau criminel sera alors moins bien protégé et offrira de nouvelles possibilités de surveillance et de collecte de renseignements aux responsables de l'application de la loi, qui pourront cerner et cibler les éventuels remplaçants des acteurs centraux du réseau. « Des fissures finiront par apparaître dans la structure du réseau à long terme » [Traduction] (14), facilitant la mise en œuvre de stratégies de perturbation plus précises et délibérées.

Duijn, P. A. C., Kashirin, V. et Sloot, P. M. A. (2014). The relative ineffectiveness of criminal network disruption. *Scientific Reports*, 4(4238), 1-15.

APPLIQUER L'ANALYSE DES RÉSEAUX SOCIAUX À LA DÉTECTION DU BLANCHIMENT D'ARGENT

L'analyse des réseaux sociaux peut améliorer la rapidité et l'exactitude des enquêtes relatives au blanchiment d'argent.

L'analyse des réseaux sociaux (ARS) est une approche multidisciplinaire qui peut schématiser et mesurer les

relations entre les entités d'un réseau social, comme les personnes, les groupes et les organisations. Elle représente également un outil d'analyse utile pour les responsables de l'application de la loi. Lorsqu'elle est utilisée efficacement, elle peut repérer les réseaux criminels sophistiqués, en plus de détecter les rôles de leurs membres ainsi que les liens entre eux.

Dans le cadre de cette étude, l'ARS a été appliquée à la détection du blanchiment d'argent, une infraction criminelle où les produits de la criminalité sont déguisés de manière à paraître légaux. Cette pratique permet aux criminels de contrôler librement leurs biens issus de la criminalité, et elle dissimule aux autorités l'identité des personnes impliquées dans des pratiques illégales. Les auteurs appliquent les algorithmes de l'ARS à un système de détection du blanchiment d'argent (SDBA), un module conçu pour détecter le blanchiment d'argent en analysant les transferts d'argent dans un système bancaire.

À l'aide du module SDBA, les auteurs présentent un système qui construit des réseaux sociaux à partir de relevés bancaires et des données du registre national juridique (en polonais, KRS). Le KRS est une base de données informatisée accessible au public qui contient de l'information sur les entités enregistrées, notamment des registres détaillés d'entreprises, d'associations, d'autres organisations, de fondations, d'établissements de soins de santé publics et de débiteurs insolvables. Les auteurs ont formulé une série de questions afin de mieux définir les rôles au sein du réseau, un élément nécessaire à l'ARS. Ils demandaient par exemple si plusieurs personnalités de l'entité avaient la même adresse commerciale enregistrée, et si cette adresse se trouvait dans un pays inscrit sur la « liste noire » des pays offrant des conditions fiscales avantageuses.

Grâce à l'ARS, les auteurs ont pu détecter les vulnérabilités du réseau et cerner les personnes particulières occupant des postes de leadership. Ils ont appliqué une série d'algorithmes afin de mettre au jour la structure des liens entre les rôles, et de déterminer si plusieurs comptes bancaires étaient enregistrés au même nom. Ils ont aussi eu recours à d'autres méthodes statistiques, à savoir des techniques d'analyse par grappes et d'exploration de formes fréquentes, pour définir les rôles des individus au sein du réseau. Les grappes sont des ensembles de transferts d'argent qui sont traités comme des opérations

soupçonnées de blanchiment d'argent parce qu'ils remplissent des critères précis. L'idée consiste à chercher des formes et des séquences fréquentes dans les grappes trouvées afin de détecter le blanchiment d'argent et de déterminer le rôle des entités impliquées. Cette approche en particulier a permis aux auteurs de mettre au jour les activités suspectes au sein du réseau de même que les groupes de délinquants.

Les auteurs concluent que l'ARS peut s'avérer utile dans les enquêtes relatives au blanchiment d'argent. Grâce aux données disponibles telles que les relevés bancaires et les registres renfermant des données pertinentes, cette technique peut repérer les schémas dans les activités des délinquants ainsi que les rôles des délinquants au sein du réseau criminel. Les auteurs insistent en outre sur l'importance d'autres techniques d'analyse avancées telles que l'exploration de données, l'apprentissage machine et le regroupement des données, comme outils pouvant aider les responsables de l'application de la loi et les décideurs à élaborer des stratégies en vue de prévenir le crime organisé que représente le blanchiment d'argent.

Drezewski, R., Sepielak, J. et Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences*, 295, 18-32.

Voir également :

Drezewski, R., Sepielak, J. et Filipkowski, W. (2012). System supporting money laundering detection. *Digital Investigation*, 9(1), 8-21.

DIFFICULTÉS DANS LES OPÉRATIONS DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Les opérations de lutte contre la cybercriminalité se heurtent à nombre de difficultés techniques et d'obstacles juridiques.

Pour lutter contre la cybercriminalité à l'ère moderne, les responsables de l'application de la loi et la magistrature doivent posséder une connaissance approfondie de la technologie informatique et se tenir au courant des derniers développements en matière de sécurité des réseaux. La cybercriminalité est un phénomène mondial en constante expansion, puisque les connaissances et les outils nécessaires pour perpétrer des actes de cybercriminalité sont devenus facilement accessibles à Monsieur et Madame Tout-le-Monde. Les criminels se sont donc sophistiqués, se dotant d'un savoir-faire et d'outils souvent équivalents ou supérieurs aux capacités des responsables de

l'application de la loi. Or, les techniques employées pour lutter contre la cybercriminalité sont imbriquées dans une procédure criminelle qui doit invariablement être adaptée aux nouvelles circonstances.

Cet article examine les difficultés auxquelles se heurtent les responsables de l'application de la loi et les organismes Signals Intelligence (SIGINT) dans les opérations de lutte contre la cybercriminalité. L'auteur présente l'étude de cas d'une opération d'application de la loi réalisée contre le marché noir en ligne « Silk Road ». Dans son article, il aborde les obstacles qui se sont dressés durant cette opération, puis il souligne les limites juridiques et les instruments utilisés pour surmonter les difficultés techniques. Enfin, il renseigne sur les organismes SIGINT et leur rôle dans les opérations de lutte contre la cybercriminalité.

Les deux grandes mesures qui protégeaient l'emplacement du serveur de Silk Road et l'identité du propriétaire étaient l'utilisation du réseau Tor et la limitation des paiements à un seul système, Bitcoin. Tor est un logiciel extrêmement efficace qui masque les adresses IP de ses utilisateurs de manière à ce qu'ils puissent communiquer en tout anonymat. Bitcoin est une forme de monnaie virtuelle utilisée partout dans le monde. Elle est décentralisée et anonyme, ce qui signifie qu'aucune organisation n'en assume seule le contrôle et qu'on peut l'utiliser sans divulguer ses renseignements personnels. En plus des méthodes policières traditionnelles, on a fait appel à des méthodes d'enquête électroniques pour appréhender le propriétaire de Silk Road.

Plusieurs difficultés techniques et juridiques se sont présentées pendant l'enquête, notamment le problème des solutions de cryptage indéchiffrables utilisées par Tor. Ces solutions masquent les adresses IP et protègent les données, empêchant les responsables de l'application de la loi d'accéder à des preuves. Sans compter qu'à l'heure actuelle, il est mathématiquement impossible de déchiffrer certaines solutions de cryptage. Et même si on connaît la clé, plusieurs programmes de cryptage peuvent garder cachées les données incriminantes au cas où l'utilisateur serait forcé de décrypter les données. Ces obstacles obligent les responsables de l'application de la loi à contourner les solutions de cryptage indéchiffrables et à exploiter le comportement négligent des auteurs de crimes, comme dans l'enquête concernant Silk Road. En raison principalement de questions liées aux droits civiques, il

est actuellement très difficile de créer des instruments juridiques qui forcent les suspects à fournir les clés aux responsables de l'application de la loi; en bout de ligne, c'est au propriétaire de décider s'il veut décrypter les données.

Un autre problème survenu pendant l'enquête concernant Silk Road touche la légalité des techniques de perquisition à distance et l'autorité transnationale des mandats. Lors d'une perquisition à distance, les pirates informatiques du gouvernement obtiennent un accès à distance à des ordinateurs, contournant l'exigence de saisies physiques. À l'heure actuelle, la légalité des perquisitions à distance varie d'un pays à l'autre. Au Canada, la loi étend les mandats de perquisition à toutes les données entreposées sous forme numérique dans la zone de perquisition. Mais les règlements transnationaux posent d'autres questions : l'application de mandats de perquisition à l'extérieur des frontières d'un État, pour pirater des ordinateurs étrangers, soulève des préoccupations importantes sur le plan de la protection de la vie privée et de l'abus de pouvoir. Les organismes d'application de la loi ne sont que rarement autorisés à procéder ainsi. Par conséquent, selon l'auteur, il faudra augmenter le nombre de groupes de travail multinationaux et accroître la coopération internationale.

Enfin, l'auteur aborde la participation des organismes du renseignement à la lutte contre la cybercriminalité par l'analyse des documents diffusés par le dénonciateur Edward Snowden. Il indique que les organismes SIGINT disposent de ressources, d'expertise et de moyens techniques plus sophistiqués que les responsables civils de l'application de la loi. Ces ressources ciblent souvent les fils étrangers et les activités terroristes, et sont beaucoup trop secrètes et intrusives pour les organismes nationaux d'application de la loi. Pourtant, étant donné toute la publicité reçue récemment par ces organismes du renseignement ainsi que leurs capacités avancées, l'auteur prévoit une augmentation potentielle de leur participation aux opérations d'application de la loi dans un avenir rapproché. Il sera alors nécessaire d'instituer des règlements plus détaillés quant il s'agit d'autoriser le recours à ces organismes contre des cibles nationales.

Bojarski, K. (2015). Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations. *The European Review of Organised Crime*, 2(2), 25–50.

LA STRUCTURE DU MARCHÉ DES DROGUES SYNTHÉTIQUES AU QUÉBEC

Il existe un marché des drogues synthétiques concurrentiel au Québec.

Plusieurs grosses saisies aux frontières et rapports publiés par des organismes de réglementation des stupéfiants, lesquels sont venus souligner la taille immense du marché des drogues synthétiques au Canada, ont mis ce marché à l'avant-plan des récents programmes d'application de la loi et accru son attention médiatique. Les drogues synthétiques sont des drogues produites par la synthèse chimique, par exemple l'ecstasy (MDMA), la marijuana synthétique et les sels de bain. Peu d'études ont examiné les éléments structuraux des marchés des drogues synthétiques, surtout au Canada. On ne s'entend pas quant à savoir si ce marché est contrôlé par une poignée de grandes entreprises illicites hautement organisées, ou en majeure partie par de petits groupes criminels concurrentiels et transitoires. Ce manque de connaissance découle principalement des difficultés méthodologiques inhérentes à l'étude des marchés cachés et secrets, en particulier le problème de l'accès à des participants fiables. C'est pourquoi les chercheurs ont élaboré des méthodes novatrices pour étudier le marché des drogues synthétiques et en analyser la structure.

Prenons cet article en exemple : les auteurs ont réalisé une analyse de la composition des drogues et une analyse économique à partir des drogues saisies et des données sur les prix au Québec. L'analyse de la composition des drogues peut renseigner les chercheurs sur le marché d'après la constitution chimique de la drogue (p. ex. composition de la substance) et ses propriétés physiques (p. ex. couleur et logo). Il existe un vaste éventail de méthodes de synthèse et une quantité infinie de couleurs et de logos possibles pour produire des drogues synthétiques. En associant les drogues selon des caractéristiques semblables, il est possible de déterminer le nombre et la taille des fabricants de drogues dans une région donnée. Quant à elle, l'analyse économique fondée sur les données sur les prix peut révéler les facteurs économiques en jeu dans le marché.

La première étape de l'étude consistait à faire un survol descriptif du marché d'après les données sur la composition des drogues. 365 drogues synthétiques ont été obtenues des saisies effectuées par les organismes

d'application de la loi dans neuf régions différentes du Québec entre juin 2007 et 2008. Ces drogues ont été analysées par Santé Canada et classifiées selon leur constitution chimique et leurs propriétés physiques. On a ainsi découvert que la constitution chimique et les propriétés physiques variaient grandement d'un comprimé à l'autre. Les saisies ont aussi fourni des données sur les prix. La majorité des drogues étaient vendues comme du « speed » (67 %), et les prix ressemblaient de près à ceux des autres pays occidentaux.

Au cours de la deuxième étape, on a effectué une analyse des réseaux à partir des mêmes données. Cette technique a permis aux chercheurs de mettre au jour les liens entre les drogues saisies au chapitre de la constitution chimique et des propriétés physiques. Les chercheurs ont constaté que le comprimé le plus populaire contenait de la méthamphétamine et de la caféine (27 % de toutes les drogues saisies). Seulement 43 % des drogues vendues comme de l'ecstasy et 66 % des drogues vendues comme du speed contenaient la substance active dont elles portaient le nom. Les chercheurs ont découvert que les caractéristiques chimiques et physiques variaient grandement entre les drogues saisies, 13 % d'entre elles seulement possédant des caractéristiques identiques à un comprimé ou plus.

Pour créer un modèle statistique de la relation observée dans l'analyse des réseaux, les chercheurs ont procédé à une analyse par grappes, regroupant les produits chimiques en fonction de leur pureté et les assimilant à de grandes catégories (qualité A, B et C) afin de garantir la fiabilité du test. Ils ont inclus les logos et les couleurs physiques comme variables lorsque le nombre était suffisant (n=3). Une fois les variables regroupées dans des grappes, les chercheurs ont procédé à des analyses de la variance afin de brosser un portrait des facteurs déterminant les prix à l'échelle provinciale, et de comparer les prix des drogues à Montréal par rapport aux autres emplacements géographiques.

Voici les principales constatations de cette étude : D'abord, l'échantillon contenait un grand nombre de drogues différentes. Les auteurs y voient la preuve de nombreux fabricants de drogues synthétiques évoluant sur un marché concurrentiel au Québec. Ensuite, le prix de la drogue dépendait de la constitution de celle-ci et de si elle était vendue comme de l'ecstasy ou du

speed, selon la région. À Montréal, les prix dépendaient uniquement de l'étiquetage de la drogue (speed ou ecstasy), tandis qu'à l'extérieur de Montréal, les prix reposaient uniquement sur sa qualité. Selon les auteurs, ces différences sont probablement attribuables à la structure des marchés et aux coûts de production. À l'extérieur de Montréal, les trafiquants sont susceptibles de vendre des produits de qualité afin d'accroître la confiance et les futures ventes. En revanche, dans le milieu urbain de Montréal, le grand nombre de clients potentiels diminue la nécessité pour les trafiquants de se bâtir une clientèle solide en cultivant des liens de confiance.

Plusieurs limites de cette étude doivent être notées. Il est possible de contrefaire le logo de manière à associer la drogue à une marque de grande qualité. Les chercheurs pourraient avoir mal classifié les drogues en associant celles portant le même logo au même fabricant. En outre, les chercheurs n'ont pu acquérir d'information sur la concentration de chaque substance. Ils ont supposé que les drogues ayant la même constitution chimique provenaient du même lot de production, et que les drogues renfermant des quantités différentes de la substance provenaient de fabricants différents. Enfin, l'étude repose sur la supposition que les fabricants emploient invariablement la même méthode et la même recette. Or, cette supposition n'a pas été confirmée par la littérature. Les auteurs font remarquer qu'ils pourraient donc être passés à côté d'un seul fabricant modifiant son processus de fabrication.

Ouellet, M. et Morselli, C. (2014). Precursors and Prices: Structuring the Quebec Synthetic Drug Market. *Journal of Drug Issues*, 44(1), 37-55.

COMPRENDRE LE DÉVELOPPEMENT DES ENTREPRISES ILLÉGALES

Les exigences logistiques d'une opération illégale dictent la taille et la structure de l'entreprise.

Cet article examine la relation entre, d'une part, l'envergure et le *modus operandi* des opérations illégales et, d'autre part, la taille des entreprises criminelles. Il contribue au débat continu quant aux limites que l'illégalité impose au développement et à la croissance des organisations participant à la vente de biens et de services illégaux. D'après la littérature, il existe une contrepartie entre la sécurité et l'efficacité, ce qui signifie que plus une entreprise illégale est

grande, plus elle peut réaliser de profits, mais au prix d'un risque accru de détection et de perturbation. On soutient également dans la littérature que les grandes entreprises illégales sont mieux placées pour gérer ces risques parce qu'elles peuvent regrouper leurs ressources, recruter des personnes remplaçables pour les tâches dangereuses, ou recruter des gens pour les tâches spécialisées comme la sécurité. On avance également que les entreprises illégales progressent graduellement le long d'une trajectoire où elles passent de petits groupes individuels à de grandes organisations, changeant avec la nature des crimes qu'elles commettent.

Cet article contribue au dialogue sur la relation entre l'envergure de l'opération, la taille de l'organisation et la minimisation des risques, grâce à une analyse des entreprises illégales évoluant sur le marché noir de la cigarette en Allemagne de 1990 à 1999. L'étude se concentre sur la région de Berlin, qui affichait la plus haute concentration géographique de cigarettes de contrebande. Durant cette période, le marché illégal de la cigarette procédait de différentes façons. Il pouvait par exemple détourner de véritables cigarettes de marque des canaux de distribution légaux dans d'autres pays, pour ensuite les introduire illégalement sur le marché noir allemand.

On a recueilli les données dans la base de données du service des douanes de l'Allemagne (appelée INZOLL) et obtenu accès aux dossiers criminels par l'intermédiaire du bureau du procureur de Berlin. C'est dans la base de données INZOLL que sont stockées les données sur les enquêtes relatives à la cigarette; les renseignements collectés aux fins de cette étude portaient notamment sur le nombre de cigarettes saisies et le nombre de suspects dans les affaires liées à la cigarette. On a également utilisé les dossiers de l'INZOLL pour mener des études de cas des personnes dont les structures de délinquance étaient les plus complexes et avaient fait l'objet des enquêtes les plus poussées, afin de se faire une idée des activités de certains des acteurs clés du marché noir de la cigarette à Berlin. Les dossiers criminels sont exhaustifs, renfermant toutes les preuves collectées et examinées au cours d'une enquête, de même que les procédures judiciaires subséquentes.

Au chapitre de l'envergure de l'opération, les données de l'INZOLL ont été classées dans trois catégories : les opérations de petite envergure (moins de

50 000 cigarettes saisies), les opérations de moyenne envergure (de 50 000 à 250 000 cigarettes saisies) et les opérations de grande envergure (plus de 250 000 cigarettes saisies). La grande majorité des opérations (97,9 %) tombaient dans la première catégorie, mais il était évident que l'envergure des opérations variait considérablement. La plupart des opérations (91,6 %) impliquaient un seul suspect enregistré, 17 étant le plus grand nombre de suspects impliqués dans une seule affaire.

Si l'on examine les dossiers criminels de 69 opérations illégales où au moins deux personnes se sont livrées à des activités criminelles, on constate que la plupart des dossiers concernaient des opérations de petite envergure. L'auteur a classé ses constatations dans trois catégories. Premièrement, les « entreprises illégales autosuffisantes » étaient les plus courantes. Il s'agit principalement d'opérations de petite envergure qui n'avaient pas besoin d'appuis extérieurs à leurs réseaux sociaux. Deuxièmement, les « entreprises illégales semi-intégrées » obtenaient des soutiens externes (p. ex., location de véhicules) en tant que citoyens privés ou en se faisant passer pour de petites entreprises non commerciales. Troisièmement, les « entreprises illégales intégrées » étaient des organisations aussi imbriquées dans des processus commerciaux légitimes. Leur principale source de sécurité résidait dans leur capacité à se fondre dans l'économie légale, souvent par l'exploitation de sociétés de façade.

L'auteur a découvert que le marché illégal examiné comportait généralement des opérations de petite envergure; cependant, un nombre relativement petit d'opérations de grande envergure représentait une partie substantielle des activités illégales. L'auteur a également constaté que les opérations qui manipulaient de grandes quantités de cigarettes de contrebande étaient généralement de plus grande taille, et que ces grandes entreprises affichaient une plus grande différenciation horizontale et verticale que celles évoluant à plus petite échelle. Enfin, l'auteur a observé que les trafiquants exercent souvent leurs activités jusque dans les sphères légales.

von Lampe, K. (2015). Big business: Scale of operation, organizational size, and the level of integration into the legal economy as key parameters for understanding the development of illegal enterprises. *Trends in Organized Crime*, 18, 289-310.

Pour obtenir davantage de renseignements sur la recherche effectuée au Secteur de la sécurité communautaire et de la réduction du crime de Sécurité publique Canada, pour obtenir une copie du rapport de recherche complet, ou pour être inscrit à notre liste de distribution, veuillez communiquer avec :

Division de la recherche
Sécurité publique Canada
340, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
PS.CSCCBResearch-RechercheSSCRC.SP@canada.ca

Les résumés de recherche sont produits pour le Secteur de la sécurité communautaire et de la réduction du crime, Sécurité publique Canada. Les opinions exprimées dans le présent résumé sont celles des auteurs et ne reflètent pas nécessairement celles de Sécurité publique Canada.

ISSN : 2369-8152

© Sa Majesté la Reine du chef du Canada, 2017

Le présent document peut être reproduit à des fins non commerciales, sans autorisation, à condition que la source soit citée.