Résumé de recherche sur le crime organisé n° 19

Évaluation de l’ampleur de la cyberfraude

BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**

Les données sur la cyberfraude sont recueillies par plusieurs organisations, comme les banques, les organismes de réglementation et divers services de police. Souvent, ces données ne sont pas consignées. Une étude des structures de réseaux de cybercriminalité pourrait servir aux méthodes appliquées pour cibler des populations clandestines de cyberfraudeurs.

La cyberfraude, sous toutes ses formes, représente-t-elle un problème grave au Canada? Par rapport à la fréquence et aux coûts d’autres types de crimes, comment se profile-t-elle? Bien que les médias électroniques et imprimés fassent état de plusieurs cas de cyberfraude, la fréquence à laquelle ces fraudes sont commises et les pertes qui en découlent sont extrêmement difficiles à évaluer avec précision. Le Canada n’a pas de méthode uniforme pour la collecte de données sur la cyberfraude.

L’étude avait pour principaux objectifs d’évaluer la possibilité d’utiliser des méthodes novatrices pour estimer la portée de la cyberfraude, de déterminer les sources de données et les lacunes, et de proposer de nouvelles sources de données qui pourraient aider à établir un portrait précis et complet de la nature et de la prévalence de la cyberfraude au Canada. À cette fin, des chercheurs ont procédé à une analyse de la littérature et ont réalisé des entrevues avec des policiers et des personnes travaillant dans le domaine des technologies de l’information.

Des entrevues avec des délinquants pourraient permettre de dessiner la structure des réseaux de populations clandestines et aider les responsables de l’application de la loi à identifier les têtes dirigeantes de ces groupes. Parmi les options disponibles pour mettre au jour cette communauté clandestine, un modèle tronqué de Poisson semble le plus efficace. Idéalement, la présente recherche pourrait ouvrir la voie à une collecte et à une analyse de données qui éclaireraient les responsables de l’application de la loi ou de l’élaboration des politiques ainsi que les enquêteurs sur l’ampleur de la cyberfraude et de la communauté des cybercriminels au Canada. Cette recherche peut faire progresser les stratégies de prévention et de suppression de la cyberfraude, mais aussi le développement de moyens empiriques pour évaluer l’efficacité de certaines initiatives, notamment d’éléments de la Stratégie de cybersécurité du Canada.

La création d’une banque de données nationales pour consigner et évaluer les données qui se rapportent à la cyberfraude a été proposée. Cet outil pourrait également permettre de réaliser des sondages en ligne auprès des Canadiens afin de recueillir des renseignements sur la cyberfraude. Un nouvel outil national pourrait être utilisé pour recueillir les données et efficacement assurer le suivi des signalements de cyberfraudes. Des renseignements confirmés sont utiles pour les policiers, mais également pour les responsables des politiques. Une banque de données centrales répertoriant les cyberfraudeurs connus et les cas de cyberfraude survenus au pays pourrait permettre de suivre la piste de suspects dans des affaires de cyberfraude et faciliter leur identification. Cette banque de données pourrait également permettre de mieux comprendre les méthodes employées par un individu ou un groupe d’individus pour commettre une fraude au pays. Des données sur les incidents de cyberfraude pourraient également aider les agents d’application de la loi à mieux comprendre le type de cyberfraudes commises au Canada.

En plus des moyens potentiels d’évaluer la cyberfraude, les répondants ont également fourni d’autres commentaires. La cybercriminalité peut franchir les frontières nationales. Les activités d’un délinquant donnent souvent lieu à la perpétration d’un crime dans plusieurs pays à la fois. Pour pallier

la complexité du problème, plusieurs solutions sont proposées : l'harmonisation des infractions substantielles commises à l'aide d'un ordinateur dans les lois nationales; l'harmonisation des dispositions en matière de procédure liées aux enquêtes sur les crimes informatiques et la poursuite en justice de leurs auteurs; la mise en place de mesures de collaboration qui faciliteront la communication d'éléments de preuve et d'information ainsi que l'extradition de suspects; la mise en place de ressources afin de veiller à ce que les tribunaux soient prêts à faire face des cas complexes de fraudes internationales.

Les répondants ont proposé de créer une base de données en ligne répertoriant les pratiques exemplaires que pourraient alimenter et consulter les professionnels du milieu de la sécurité des TI. Cette base de données pourrait offrir un forum en ligne à la communauté de professionnels, qui pourraient échanger des conseils et des astuces. Les répondants ont également soulevé la possibilité d'offrir des séances d'information ou des conférences dans certains secteurs industriels pour agir de façon proactive à l'égard des menaces de cyberfraudes et des vulnérabilités. Ces initiatives pourraient améliorer l'efficacité de l'industrie de la sécurité des TI et de la police, et renforcer les relations entre ces deux communautés.

Enfin, une autre suggestion suppose qu'il faudrait mettre l'accent sur l'éducation des Canadiens, qui doivent savoir comment reconnaître les canulars. L'éducation pourrait limiter les pertes monétaires et les autres préjudices subis par les personnes, les entreprises et les compagnies d'assurance en raison d'une cyberfraude.

Smyth, Sara et Rebecca Carleton. *Évaluation de l'ampleur de la cyberfraude − Document de travail sur les méthodes potentielles et les sources de données*, Ottawa, Sécurité publique Canada, 2011.

Pour obtenir de plus amples renseignements sur la recherche en matière de crime organisé au sein de Sécurité publique Canada, veuillez communiquer avec l'Unité de recherche sur le crime organisé à l'adresse ocr-rco@ps-sp.gc.ca.

Les résumés de recherche sur le crime organisé sont rédigés pour Sécurité publique Canada et le Comité national de coordination sur le crime organisé (CNC). Le CNC et ses comités régionaux et provinciaux de coordination travaillent à différents niveaux en misant sur un but commun : établir des liens entre les organismes d'application de la loi et les décideurs du secteur public afin de lutter contre le crime organisé. Les résumés de recherche sur le crime organisé appuient les objectifs de recherche du CNC en faisant ressortir des renseignements fondés sur la recherche qui sont pertinents pour l'élaboration de politiques ou d'opérations. Les opinions exprimées dans le présent résumé sont celles des auteurs et ne reflètent pas nécessairement les opinions de Sécurité publique Canada ou du Comité national de coordination sur le crime organisé.