

Témoignage de
Garry W.G. Clement
Président et chef de la direction
Clement Advisory Group
Comité des Finances de la Chambre des communes (Canada)
Étude des coûts, de l'impact économique, de la fréquence et des pratiques exemplaires du
traitement de la question du financement du terrorisme au Canada et à l'étranger

Bonjour, monsieur le président Rajotte; bonjour, distingués membres du Comité. Merci de m'avoir invité à témoigner à cette audience. Le financement des activités terroristes est un sujet d'une extrême importance pour moi. Je suis très sensible au fait que vous preniez le temps de vous y plonger.

– *Le premier ministre Stephen Harper a déclaré ceci* : « Notre gouvernement tient sérieusement à prendre des mesures pour assurer la sécurité des Canadiens. Les récentes attaques perpétrées au Canada, qui ont entraîné la mort du Caporal Nathan Cirillo et de l'Adjudant Patrice Vincent, de même que les attaques perpétrées en France et en Australie, nous rappellent que le monde est rempli de dangers et que le Canada n'est pas à l'abri de la menace du terrorisme. Les récents actes terroristes survenus au Canada ne consistaient pas en une attaque contre notre pays seulement, mais aussi contre nos valeurs et notre société dans son ensemble. »

Peu d'événements dans une vie suscitent des émotions très profondes et restent vifs dans la mémoire. Les attentats perpétrés contre les États-Unis par Al-Qaïda le 11 septembre 2001 et les attaques lancées récemment à Ottawa sont à l'évidence parmi les moments historiques qui resteront gravés dans nos esprits. Au moment des attentats du 11 septembre, j'étais officier responsable adjoint des enquêtes criminelles dans la région de la capitale nationale et j'ai pu voir de mes yeux comment un acte terroriste majeur peut avoir un effet profond sur notre société et nos vies. L'expansion de notre action militaire en Syrie continuera de nous placer dans la mire des extrémistes, et il est donc indispensable d'utiliser toutes nos ressources dans un effort concerté pour couper les fonds aux groupes terroristes.

J'ai eu la grande chance de participer au Programme des produits de la criminalité, mis en place par la GRC, dès les tout premiers stades, en 1983. J'étais aussi l'un des rares négociateurs préparés à réagir à une situation de prise d'otage terroriste. J'ai au total plus de 35 ans d'expérience en matière de criminalité financière et je me suis surtout intéressé à la lutte contre le blanchiment d'argent et le financement des

activités terroristes. Depuis que j'ai quitté la GRC, j'ai offert des services consultatifs concernant la fraude, le blanchiment d'argent, la cybercriminalité et le financement des activités terroristes. Beaucoup de mes clients appartiennent au secteur des services financiers. La semaine dernière, j'étais à Mumbai, où je me suis adressé au Conseil international des associations de sécurité pour parler de la menace de la cybercriminalité, du point de vue pénal et du point de vue du risque de financement du terrorisme.

Mon expérience d'enquêteur au gouvernement et de consultant pour le secteur privé m'a donné l'occasion, fort rare, de comprendre deux perspectives très différentes. Pendant plus de 34 ans, ma perspective a été celle d'un agent d'application de la loi. À ce titre, mon point de vue était celui d'un fonctionnaire et d'un enquêteur. Au cours des sept dernières années, en ma capacité actuelle de consultant, j'ai vu les choses du point de vue du secteur privé et de la conformité aux normes. Cela me permet de comprendre les responsabilités, les susceptibilités, les difficultés et les frustrations à la fois du gouvernement et du secteur financier lorsqu'il est question de lutte contre le blanchiment d'argent et le financement des activités terroristes. La différence de perspective est notable. C'est l'une des nombreuses difficultés que soulèvent le financement des activités terroristes et d'autres enjeux d'ordre pénal.

Les établissements financiers dépensent des millions de dollars chaque année à dresser des obstacles au blanchiment d'argent et au financement des activités terroristes. Le blanchiment d'argent et le financement des activités terroristes sont des zones distinctes de la criminalité financière bien qu'ils partagent certains éléments communs. Ce n'est pas d'aujourd'hui que les financiers du terrorisme recourent aux techniques de blanchiment d'argent pour financer les activités des jeunes gens impressionnables et désespérés qui appuieront sur la gâchette ou allumeront la mèche. Il peut être très frustrant pour un établissement financier d'élaborer des moyens de défense contre le financement des activités terroristes, sans parler du repérage des opérations financières à l'origine du financement d'actes terroristes. Les terroristes estiment être en guerre et ne respectent aucune règle ni aucun uniforme. Ils se camouflent dans les populations civiles pour déchaîner leur fureur contre des cibles qui ne se doutent de rien ou contre des structures symboliques. S'ils peuvent échapper à la police et aux services de renseignement pour remplir leur mission, ils peuvent aussi échapper à la vigilance des établissements financiers.

Il est extrêmement difficile de repérer les activités suspectes dans les établissements financiers, surtout s'il s'agit de financement d'activités terroristes. C'est là qu'il est absolument important de comprendre la perspective des intéressés. Quand on veut circonscrire et dénoncer une activité suspecte, il faut tenir compte de « qui, quoi, où, quand, pourquoi et comment ». En général, la police s'intéresse surtout au « pourquoi », tandis que les établissements financiers s'interrogent plutôt sur le « comment ». C'est là,

entre autres, que la collaboration entre les organismes d'application de la loi et les établissements financiers est indispensable, car la prévention des actes terroristes suppose des échanges d'information en temps réel. Nous devons veiller à ce qu'il existe un mécanisme permettant à la fois au SCRS et à la GRC de partager proactivement de l'information sur des alertes potentielles, par des voies confidentielles, notamment en matière de révocation de passeport et de voyage à destination de pays jugés à très haut risque. Les banques sont bien placées pour fournir des renseignements utiles si leurs actions bien définies sont approuvées et protégées par la réglementation officielle. C'est quelque chose qui, je crois, pourrait se faire par la nomination d'une personne-ressource dans chaque grand établissement après vérification et désignation en bonne et due forme.

Comme on le sait, les personnes radicalisées réagissent à brève échéance. Pour réussir, les terroristes isolés, comme les loups solitaires, aussi bien que les groupes terroristes ont besoin d'argent. Ils ont besoin de fonds pour agir et réussir. Invariablement, leurs sources de financement passeront par les établissements financiers. Pour fonctionner, les terroristes doivent avoir accès à de l'argent en tout temps. Qu'il soit nominal ou important, l'afflux de fonds est d'une importance critique sur le plan opérationnel. Les terroristes, comme les criminels, recueillent des fonds, les déplacent, les déposent et les dépensent au profit de leurs activités illicites. C'est pourquoi les exigences redditionnelles énoncées dans la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes sont essentielles pour notre sécurité nationale. On s'en convainc d'autant plus aujourd'hui où les finances sont l'une des deux points faibles les plus importants visés par les organisations terroristes et les organisations criminelles.

On ne saisit pas l'ensemble de la situation du financement des activités terroristes, et, compte tenu de l'importance des sommes en cause, il peut être très difficile de le circonscrire. C'est là que le gouvernement, par le biais des relations entre les organismes de lutte contre le financement des activités terroristes, doit collaborer plus efficacement avec le secteur des services financiers pour circonscrire les sources de financement en question. Les établissements financiers pourraient effectivement circonscrire les sources de financement d'activités terroristes, mais c'est tout à fait improbable dans les circonstances actuelles. Il faut systématiquement prendre des mesures pour accroître le facteur de probabilité et, de ce fait, la possibilité de circonscrire les sources de financement. Le défi pour le gouvernement et pour les banques est d'améliorer l'efficacité du processus. C'est là que le gouvernement doit se faire plus efficace et plus efficient dans les moyens d'aider les établissements financiers à repérer les activités suspectes. À mon avis, les organismes d'application de la loi et le CANAFE devraient élaborer de meilleurs mécanismes de rétroaction en temps réel à l'intention des établissements financiers concernant la façon dont les terroristes se servent d'eux et leur fournir des typologies susceptibles d'être utilisées pour la surveillance des opérations financières.

Nous sommes tous devenus beaucoup trop conscients de la façon dont des groupes terroristes comme l'EIL et l'EI tirent parti des sites Web des réseaux sociaux non seulement pour répandre leur propagande ou recruter des jeunes, mais aussi pour recueillir des fonds. La mondialisation conjuguée à l'aptitude des organisations terroristes à utiliser Internet et les médias sociaux pour attirer, séduire et radicaliser des gens qu'ils gagnent à leur « cause » et au djihad ou pour faciliter d'autres actes extrémistes accroît exponentiellement la menace et les effets du terrorisme. En termes simples, les combattants étrangers qui sont recrutés par les organisations terroristes élargissent la portée internationale des insurrections transnationales aussi bien que les conflits religieux et idéologiques. C'est ce qui a permis à l'EIL et à d'autres d'obtenir un appui international et de le transformer en financement. En février 2015, le Groupe d'action financière a publié un article sur les modes de financement employés par l'EIL, et l'une des méthodes soulignées était les cartes internationales de télécommunications prépayées. Les donateurs achètent des cartes prépayées et envoient le numéro de la carte au collecteur de fonds par Skype. Le collecteur envoie le numéro à l'un de ses partisans dans un pays comme la Syrie et le vend à un moindre prix. Et l'argent comptant est remis plus tard à l'EIL. Les cartes prépayées peuvent sembler de peu de conséquence, mais, quand on se rend compte que des centaines de sympathisants peuvent en acheter, elles peuvent collectivement représenter un financement important. À cet égard, les nouveaux pouvoirs prévus aux termes du projet de loi C-51 en matière de saisie par ordonnance judiciaire de contenus à teneur de propagande terroriste sur Internet et la nouvelle disposition sanctionnant le fait de préconiser et de fomenter sciemment la perpétration d'infractions de terrorisme, comme le financement d'une entité terroriste désignée, peuvent être très utiles.

Dans un rapport publié récemment par l'Institut McKenzie (*Foreign fighters : A Threat to National Security*, décembre 2014), le Colonel Bernd Horn explique ceci : « *Pour les gouvernements occidentaux, les combattants étrangers représentent également une menace dissimulée. Lorsqu'ils rentrent chez eux ou que leurs organisations respectives leur ordonnent de rentrer chez eux pour y continuer le combat, ces combattants constituent une cohorte plus expérimentée, plus mortelle et plus dangereuse et perfectionnée que beaucoup de leurs homologues internes. Ils représentent désormais une menace importante, qu'ils agissent en groupe ou à titre de « loups solitaires ». Le Canada n'y échappe pas. Les sources gouvernementales concèdent que plus de 130 Canadiens ont quitté le pays pour participer à des entraînements ou des opérations effectives auprès d'organisations terroristes. Par ailleurs, on connaît 80 ex-combattants étrangers canadiens qui sont rentrés et résident actuellement au Canada. La crainte du gouvernement est que ces combattants étrangers exacerbent le potentiel et l'efficacité du terrorisme d'origine intérieure. La situation est d'autant plus alarmante qu'il n'est pas toujours facile d'identifier et de retracer les personnes qui quittent le pays à des fins malveillantes parce que les individus radicalisés et prêts à agir ne correspondent pas à un seul et même profil identifiable.*

Comme ils voyagent avec des passeports canadiens ou des passeports de grands pays occidentaux, ils peuvent facilement franchir les frontières internationales sans être assujettis aux restrictions et aux visas imposés à beaucoup de citoyens non occidentaux. En fin de compte, les combattants étrangers représentent une menace croissante dont les répercussions touchent la stabilité globale et la sécurité intérieure. Les solutions sont loin d'être simples, et elles supposent une perspective nationale et internationale exhaustive. Compte tenu de la barbarie et la sauvagerie dont fait preuve l'organisation terroriste État islamique, on ne saurait impunément ignorer le cancer que représentent les combattants étrangers et les organisations qu'ils soutiennent. Ces combattants, bien qu'ils ne soient pas tous ralliés au djihad ou à des organisations islamiques, représentent tout de même un danger caché qui alimente les insurrections transnationales et une menace secrète pour la sécurité nationale. On ne peut les ignorer. »

Le financement des activités terroristes est une question tout aussi complexe aujourd'hui qu'elle l'était au lendemain des attentats du 11 septembre. Les organismes d'application de la loi, de réglementation et de renseignement ont, ici au Canada, comme à l'étranger, obtenu des résultats valables et significatifs. De nouvelles méthodes, proactives et modernes, ont été élaborées et mises en œuvre à l'appui de ces efforts. Lorsque le gouvernement réussit à mettre en œuvre des méthodes proactives, il entrave l'aptitude des terroristes à mener leurs opérations. Cela dit, certaines préoccupations persistantes et la faculté d'adaptation des terroristes, ajoutées à la facilité d'exploitation des faiblesses systémiques du secteur financier, perpétueront la difficulté à régler les enjeux associés au financement des activités terroristes.

De nos jours, nous affrontons trois difficultés importantes. Les crimes les plus importants auxquels nous devons faire face dans le secteur des services financiers sont la fraude, le blanchiment d'argent et la cybercriminalité. La fraude a été au centre de la crise financière américaine et elle continue de représenter une menace importante pour notre économie. La Commission Charbonneau a récemment révélé ce qui se passe lorsque la fraude est généralisée. Le blanchiment d'argent recouvre toutes les activités criminelles lorsque les produits de la criminalité sont blanchis par le biais des établissements financiers. Les principaux instruments qui facilitent la fraude et le blanchiment d'argent sont les virements bancaires, les services de banque correspondante, les services de remises de fonds illicites, les sociétés fictives et les mécanismes électroniques. La cybercriminalité est, d'après moi, la menace la plus grave, et elle sert aussi bien des gouvernements voyous, des terroristes ou des organisations criminelles. C'est le crime sans frontière par excellence.

Les services de remises de fonds illicites sont un problème important au Canada. Lorsque des sanctions ont été prises contre l'Iran, beaucoup de banques canadiennes ont fermé toutes les entreprises de

services monétaires faisant affaire avec l’Iran et elles ont-elles-mêmes fermé beaucoup de comptes de Canadiens d’origine iranienne. Il s’en est suivi que les services de remises de fonds illicites en ont profité et ont très bien réussi à transférer des fonds depuis. Nous devons reconnaître que nous accueillons de nombreux étudiants iraniens tous les ans et que la très nombreuse collectivité irano-canadienne a légitimement besoin transférer des fonds entre l’Iran et le Canada. Malheureusement, ces transferts se font désormais dans le cadre d’une économie clandestine qui pave la voie à la fois au financement des activités terroristes et au blanchiment d’argent par des organisations criminelles. Au cours des dernières années, j’ai déposé plusieurs rapports de renseignement grâce aux informations fournies par des sources iraniennes proches et qui démontrent clairement que des services de remises de fonds illicites iraniens fonctionnent librement dans la plupart des grandes villes du Canada. J’estime que ces services représentent un risque grave du point de vue du financement des activités terroristes.

C’est un défi constant. Beaucoup de banques ne peuvent pas identifier les clients qui exploitent des services de remises de fonds, et les organismes d’application de la loi de tous les niveaux n’ont pas suffisamment d’enquêteurs financiers pour surveiller efficacement ces services. Ces services ont toutes les apparences de la légalité, mais, comme une certaine bijouterie de Toronto, ils fonctionnent comme des services de transfert de fonds illicite vers des pays à très haut risque. Des groupes terroristes et des organisations criminelles se servent donc des services de remises de fonds illicites pour faciliter leurs activités.

Par ailleurs, les sanctions imposées à des pays comme l’Iran ont incité certaines entités à utiliser régulièrement des sociétés fictives pour dissimuler leurs propriétaires véritables et à déplacer illégalement des fonds par le biais de services de banque correspondante ou de virements bancaires. Le scandale de la banque Lloyds est un exemple flagrant de la façon dont l’Iran se servait des services de banque correspondante. Dans cette affaire, la Lloyds avait supprimé des renseignements sur les services de messagerie financière SWIFT pour dissimuler l’identité de banques iraniennes et ainsi échapper au système de surveillance bancaire des États-Unis. L’affaire de la Fondation Alavi est un exemple de la façon dont l’Iran s’est servi de sociétés fictives pour dissimuler ses propriétaires véritables dans un immeuble à bureaux de New York. Dans les deux cas, il y a eu usage de virements bancaires.

Les mécanismes de paiement électronique sont un souci croissant compte tenu de la façon dont les terroristes transfèrent de l’argent et du caractère anonyme et instantané du processus. Ils se multiplient rapidement et peuvent être facilement détournés par les criminels et les terroristes. L’Afrique est une région préoccupante à cet égard.

Je rappelle depuis plusieurs années que le secteur des guichets automatiques privés doit être assujéti à la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes. Les entreprises de ce secteur font valoir qu'elles fournissent une surveillance suffisante, mais, d'après mon expérience, ce n'est pas le cas. Les guichets automatiques privés sont un instrument de blanchiment d'argent qui serait facile à contrôler grâce à une modification de la réglementation faisant obligation de rendre compte au CANAFE des fonds placés dans les machines privées.

J'invite instamment le comité à envisager des modifications à la réglementation qui permettraient l'usage de la technologie pour identifier des clients dans le cadre d'une intégration indirecte. La réglementation actuelle s'appuie énormément sur des attestations qui se sont révélées dangereuses compte tenu des possibilités criminelles qu'elles offrent et des progrès accomplis par les cybercriminels. Compte tenu de l'évolution de la technologie, je soutiens respectueusement qu'on peut efficacement améliorer l'identification.

Les extraits suivants d'un rapport du commissaire à la protection de la vie privée du Canada étayent cette idée et, je crois, militent en faveur d'une identification efficace des intéressés :

« La reconnaissance faciale automatisée consiste à identifier un individu à partir de la géométrie de son visage. Pour que la technologie soit efficace, il faut disposer d'une image numérique de qualité du visage de l'individu en question, d'une base de données d'images numériques d'individus identifiés et d'un logiciel de reconnaissance faciale capable d'établir une correspondance exacte entre l'image d'un individu et une image d'un individu identifié qui est enregistrée dans la base de données. Parmi toutes les technologies biométriques, la reconnaissance faciale est celle qui imite le plus la façon dont les gens s'y prennent pour identifier les autres, c'est-à-dire en examinant leur visage. Il est extrêmement difficile et coûteux de doter une machine de cette aptitude qui ne nécessite aucun effort de la part des humains. Cela dit, grâce à une convergence de facteurs au cours des dernières années, la reconnaissance faciale est devenue une technologie viable et de plus en plus exacte. Les images numériques sont désormais omniprésentes en raison de la prolifération des caméras de surveillance, des téléphones intelligents équipés d'un appareil photo et des appareils photos numériques de qualité bon marché. Les dispositifs de stockage à prix modique ont donné lieu à la création de vastes bases de données en ligne renfermant des images d'individus identifiés, par exemple les titulaires de permis de conduire ou de passeport, les personnes possédant une carte d'identité d'employé et celles ayant un casier judiciaire. Les individus ont adopté l'affichage et l'étiquetage des photos en ligne sur des plateformes comme Facebook, Instagram, Picasa et Flickr. En outre, la technologie de reconnaissance faciale a fait l'objet de perfectionnements considérables, notamment au chapitre de l'analyse des images et de l'extraction des données. Les visages ont été transformés en données électroniques qu'il est désormais possible de regrouper, d'analyser et de classer de

façons inédites. Les données d'images du visage sont d'autant plus précieuses et sensibles qu'il s'agit d'une caractéristique de notre corps mesurable de façon unique et d'un élément clé de notre identité. »

En se servant de la technologie, une personne qui souhaite être accueillie par un établissement financier et/ou une entreprise de services monétaires serait tenue d'être interviewée par un moyen qui d'emblée permettrait à l'établissement ou l'entreprise de procéder à une entrevue en face à face et de comparer les documents d'identification à l'aide du système visuel. De plus, en utilisant un système comme Skype, l'intervieweur pourrait parler directement au client proposé, prendre connaissance visuellement de ses documents d'identification, de prendre une photo du client et, s'il y a lieu, de demander des précisions sur l'origine des fonds, les antécédents de l'intéressé et/ou de son entreprise, etc. Je pense que cela éliminerait une partie du risque de fraude et de vol d'identité auquel nos établissements financiers sont exposés de nos jours.

J'ai récemment collaboré avec une entreprise de services monétaires et l'une de nos cinq grandes banques, où une somme importante avait été détournée au moyen d'un programme d'hameçonnage visant un client des deux établissements dont l'identité avait été volée. Si l'on avait eu accès à une procédure externe aux exigences actuelles permettant l'usage de la technologie pour parler directement au client, je suis convaincu que ce crime n'aurait pas été aussi facile à commettre.

Je pense aussi que nous avons besoin de la même aptitude technologique et notamment de la biométrie de reconnaissance faciale aux bureaux des frontières pour aider les autorités à intercepter les Canadiens de retour au pays qui ont jugé bon de rallier la cause des terroristes et risquent de revenir plus radicalisés.

Le gouvernement a fait des progrès systématiques et continus dans la lutte contre le financement des activités terroristes. Les organismes et entités responsables de la lutte contre ce financement ont mûri et ils évoluent eux aussi. Ils ont développé, individuellement et collectivement, des méthodes d'enquête permettant de relever des défis à la fois constants et nouveaux. Le SCRS et la GRC peuvent s'enorgueillir de capacités améliorées, mais, comme l'a rappelé le commissaire Paulson, les actes terroristes récents ont détourné des fonds vers ces menaces, de sorte que les activités des organisations criminelles sont passées à l'arrière-plan. J'invite instamment le comité à se rendre compte que, pour faire enquête sur les crimes financiers et notamment sur le blanchiment d'argent et le financement des activités terroristes, il faut énormément d'expertise. Cela fait des années que je dis et redis qu'il faut à un enquêteur très qualifié au moins cinq ans d'expérience dans le domaine du blanchiment d'argent pour acquérir l'expertise et les connaissances nécessaires pour mener à bien ces enquêtes complexes. Au cours de mon mandat, je peux

dire que le système promotionnel de la GRC a été un obstacle majeur à la garantie que des enquêteurs restent dans des secteurs spécialisés. Je suis sûr que vous conviendrez avec moi que, si vous devez subir une chirurgie du cerveau, vous ne voudrez pas qu'un généraliste s'en charge. Il en va de même pour les enquêtes financières. Pour se faire une idée de la complexité de ces cas, la récente condamnation de deux responsables de blanchiment d'argent au Québec, Chun et Lech, qui ont offert leurs services à des organisations criminelles, témoigne du dévouement et de la persévérance des enquêteurs de la Couronne et de la police pendant dix longues années.

Quels que soient les progrès accomplis en général, je crois que deux rapports montrent clairement que le Canada a obtenu d'excellents résultats en matière d'application de la loi. D'abord, le rapport final de l'Évaluation de l'Initiative intégrée de contrôle des produits de la criminalité (IICPC) - 2010-2011, où sont énoncées les conclusions suivantes :

Malgré l'incidence de l'Initiative, les constatations de l'équipe d'évaluation semblent indiquer que l'Initiative n'est pas aussi efficace ou efficiente qu'elle pourrait l'être. Au cours de la présente évaluation, on a pu cibler les difficultés suivantes : financement, roulement du personnel, formation, gouvernance, surveillance, communication, difficultés juridiques et relationnelles.

Pour atteindre ses objectifs de manière efficiente, l'Initiative demande une communication et une collaboration étroites entre ses partenaires. En effet, la principale caractéristique du concept d'origine de l'Initiative était l'intégration. Les données obtenues au cours de l'évaluation semblent indiquer que cette principale caractéristique de l'Initiative s'est estompée au fil du temps, au détriment des opérations qui sont menées dans le cadre de cette initiative.

Plusieurs facteurs relatifs aux effectifs ont eu des conséquences néfastes sur les opérations de l'Initiative, notamment : certains partenaires ont quitté les unités (les organismes ne sont plus co-implantés), le roulement des effectifs, les postes vacants, les difficultés de recrutement, le manque de personnel expérimenté et l'absence de formation. Ces facteurs humains doivent être résolus pour faire de l'Initiative une initiative à nouveau entièrement opérationnelle.

On peut dire que la cohérence et l'uniformité des données de rendement sont des caractéristiques nécessaires pour toute opération intégrée. Cependant, au moment de l'évaluation, aucun système intégré de surveillance n'était en place. De plus, tous les partenaires de l'Initiative ont chacun leurs propres systèmes et outils d'établissement de rapports, et il n'existe aucune norme commune. Les partenaires de l'Initiative doivent prendre des mesures pour améliorer la surveillance du rendement de l'Initiative au moyen de mesures cohérentes du rendement.

En résumé, l'absence d'une stratégie globale et d'un plan d'activités, de communication et de relations entre les partenaires, d'effectifs, d'intégration, d'indicateurs de rendement et d'un système de surveillance commun, contribue à un rendement inférieur.

(<http://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/vltn-ntgrtd-prcds-crm-2010-11/index-fra.aspx>)

Ensuite le rapport intitulé « Suivre l'argent à la trace : Le Canada progresse-t-il dans la lutte contre le blanchiment d'argent et le financement des activités terroristes? Pas vraiment », déposé en 2013 par le Comité sénatorial permanent des banques et du commerce, où celui-ci concluait ce qui suit dans deux de ses recommandations :

- 1) *Le comité est d'avis que des changements sont nécessaires pour répondre à l'évolution du blanchiment d'argent et du financement des activités terroristes dans le monde, des avancées technologiques et du besoin de sensibilisation au régime. De ce point de vue, les cinq recommandations du comité mettent l'accent sur l'établissement de rapports fondés sur le risque, sur le respect des normes internationales et sur la sensibilisation de la population.*

- 2) *Que le gouvernement fédéral s'assure que le Centre d'analyse des opérations et déclarations financières du Canada et la Gendarmerie royale du Canada emploient des spécialistes du crime financier et qu'ils leur offrent une formation continue de sorte que leurs compétences évoluent au même rythme que les avancées technologiques.*

Le gouvernement doit sans arrêt circonscrire et évaluer les tendances émergentes et élaborer des typologies de cas qu'il puisse communiquer aux établissements financiers. Ce faisant, le secteur des services financiers pourra mettre en œuvre des stratégies de surveillance des opérations permettant de circonscrire des caractéristiques d'activité correspondant aux typologies applicables aux criminels et aux terroristes. Le gouvernement ne l'a pas fait aussi systématiquement qu'il l'aurait pu.

En général, les organismes d'application de la loi et le CANAFE n'ont pas particulièrement brillé dans un partenariat public-privé, certainement pas autant qu'ils le croient ni qu'ils l'auraient pu. Et je ne dis pas cela à la légère. Quand j'étais dans la GRC, j'ai passé mon temps à lutter pour maximiser les relations de liaison. Ce n'est qu'après ma retraite et le début de mon travail comme consultant auprès du secteur des services financiers que je me suis rendu compte que nous aurions pu faire plus et qu'il fallait en faire plus. Les organismes d'application de la Loi et le CANAFE devraient s'appliquer à écouter les représentants des établissements financiers et à leur fournir de la rétroaction pour ce qui concerne la façon dont les terroristes et les organisations criminelles utilisent le système financier pour faciliter leurs activités illicites.

Ce qui importe, surtout quand il s'agit de plus petites sommes d'argent, c'est de circonscrire des typologies et de les utiliser pour élaborer des stratégies ciblées de surveillance des opérations. Cela suppose une collaboration plus systématique entre les organismes d'application de la loi et le secteur des services financiers, notamment par le biais d'un recours accru à des spécialistes. Des organisations comme

l'Association of Certified Anti-Money Laundering Specialists, l'Association of Certified Financial Crime Specialists et l'Association of Certified Fraud Examiners sont des tribunes idéales pour les organismes de réglementation, le personnel chargé de surveiller la conformité des entreprises et les organismes d'application de la loi qui cherchent à collaborer et à échanger avec des collègues du monde entier. Le CANAFE a récemment offert à son personnel une formation le préparant à obtenir la certification de l'ACAMS, mais il y a vide au sein des organismes d'application de la loi, qui ne semblent pas accorder la même importance à ces réseaux et à ces possibilités d'apprentissage.

Ce genre d'initiative pourrait servir utilement à circonscrire les sources de financement des activités terroristes. On pourrait envisager un certain nombre de scénarios à circonscrire et viser de la même façon. Prenons l'exemple d'un loup solitaire qui quitte le Canada à destination de la Syrie pour y rejoindre un camp d'entraînement terroriste. Il y a peu de chances qu'il procède à des opérations bancaires pendant son entraînement. Il sort donc virtuellement de la grille financière. Le voyage en Syrie, la destination à haut risque et l'absence d'activité bancaire pourraient être des facteurs entrant en ligne de compte dans le système de surveillance ciblée d'un établissement financier.

Un de mes bons amis et ex-chef du programme de lutte contre le financement des activités terroristes au FBI, Dennis Lormel, a témoigné devant le Congrès, à qui il a expliqué les principaux éléments qui, selon lui, multiplient la probabilité de repérer une source de financement d'activités terroristes. J'ai repris ces éléments en les inscrivant dans le contexte canadien et j'en ai ajouté un, comme suit :

- 1) Le gouvernement et le secteur financier doivent comprendre l'importance d'une formation spécifique en matière de financement des activités terroristes. C'est une dimension qui manque des deux côtés, quoique plus particulièrement du côté des établissements financiers. Faute d'une formation spécifique, il est plus difficile de comprendre et d'entraver ce genre d'activités.
- 2) Le gouvernement doit se doter de moyens de fournir légalement des autorisations de sécurité permettant de sélectionner du personnel dans les établissements financiers à qui il pourra communiquer certains renseignements confidentiels susceptibles d'être comparés avec l'information contenue dans les systèmes de surveillance bancaire dans le but de repérer les comptes ou les opérations associés à des organisations terroristes.
- 3) Il faudrait élaborer un mécanisme de rétroaction complet et cohérent du côté des organismes d'application de la loi pour attester l'importance de la reddition des comptes en vertu de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes et notamment

de l'importance des déclarations d'opérations douteuses. L'examen de ces déclarations par le CANAFE est un bon système qui fournit des renseignements utiles. Par ailleurs, une rétroaction spécifique de la part des organismes d'application de la loi à l'intention des établissements financiers concernant la valeur et les avantages des données fournies en vertu de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, notamment des déclarations d'opérations douteuses, aurait un effet remarquable sur le moral des gens qui sont chargés de faire ces déclarations.

- 4) Le gouvernement doit évaluer toutes les déclarations d'opérations douteuses liées ou identifiables à des affaires de terrorisme. Ce genre d'examen permettrait de repérer des signaux d'alerte susceptibles de servir de mécanisme de formation, mais pourrait surtout entrer en ligne de compte dans l'élaboration des typologies aptes à renforcer la capacité de suivi ou de surveillance des établissements financiers. Par ailleurs, on pourrait s'intéresser aux raisons pour lesquelles l'établissement financier a fait une déclaration. Dans bien des cas, elle a été faite en raison de violations n'ayant rien à voir avec le financement des activités terroristes. Il convient donc de comprendre ce qui a déclenché la déclaration et utile, parallèlement, de vérifier en quoi la déclaration est liée à des intérêts terroristes.
- 5) Outre l'évaluation des déclarations d'opérations douteuses, le gouvernement et le secteur privé devraient, ensemble, circonscrire et évaluer autant d'enquêtes sur le financement des activités terroristes que possible dans ce qui est légalement accessible au public. On devrait comparer les études de cas pour déterminer les points communs et les caractéristiques communes des activités. On pourrait aussi facilement discerner des signaux d'alerte communs. Ce type d'évaluation, conjuguée à l'analyse des déclarations d'opérations douteuses, fournirait des renseignements plus utiles dans la recherche des caractéristiques du financement des activités terroristes, surtout dans les cas où les sommes sont plus nominales. Cela permettrait aux établissements financiers d'employer plus efficacement des techniques de surveillance et de suivi propres à circonscrire des données transactionnelles douteuses.
- 6) La combinaison des données fournies en vertu de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, notamment tirées des déclarations d'opérations douteuses, et de données empiriques et anecdotiques permettrait au gouvernement et au secteur financier, ensemble et unilatéralement, de procéder à une analyse des tendances. Ce serait un facteur important dans le repérage des tendances émergentes. À l'échelle du gouvernement, cela contribuerait à la mise en œuvre de stratégies d'enquête et d'application de

la loi. Du côté des établissements privés, cela permettrait au secteur financier de mettre en œuvre des stratégies d'atténuation des risques.

- 7) Les organismes d'application de la loi ont besoin des ressources qui leur permettraient de remplir leur mandat intégralement afin que la lutte contre financement des activités terroristes ne réduisent pas le nombre des enquêtes sur les activités financières des organisations criminelles, et faut reconnaître la nécessité d'une spécialisation qui devrait être assujettie à des objectifs précis.

Le paysage mondial a changé et les méthodes ont récemment évolué, mais le financement des activités terroristes ne change pas. Essentiellement, les terroristes ont besoin d'argent et doivent y avoir accès quand ils passent à l'action. Il incombe aux organismes gouvernementaux de collaborer, de coordonner leurs activités et de communiquer entre eux et avec le secteur privé pour empêcher les terroristes de déplacer de l'argent et d'y avoir accès et, ainsi, réduire leur aptitude à agir.

Comme l'a expliqué le président Obama, « les résolutions ne suffisent pas. Les promesses sur papier ne nous protègent pas... Les beaux discours et les bonnes intentions n'arrêteront aucune attaque terroriste. Les paroles prononcées ici aujourd'hui doivent être suivies et traduites par des actes. »

Je tiens une fois encore à remercier les distingués membres de comité de m'avoir donné la possibilité de participer à cette importante étude. Je suis à votre disposition pour répondre à vos questions ou fournir des éclaircissements sur ce que j'ai dit.