

Examen parlementaire de la *Loi antiterroriste*

Comité spécial sénatorial

Présentation du chef du CST – 11 avril 2005

Discours

INTRODUCTION

Madame la Présidente, Honorables sénateurs, je vous remercie de m'avoir invité à paraître devant vous aujourd'hui à titre de chef du Centre de la sécurité des télécommunications. J'apprécie cette occasion qui m'est donnée de discuter avec vous de l'impact qu'a eu la *Loi antiterroriste* sur le CST.

Avant de commencer, j'aimerais vous présenter trois membres de mon équipe de gestion supérieure qui sont là pour m'appuyer.

À ma droite se trouve Barb Gibbons, chef adjoint des Services centraux du CST. À côté de moi, à gauche, se trouve John Ossowski, directeur général des Politiques et des communications, et à côté de lui, David Akman, directeur des Services juridiques du CST.

RÔLE ET MANDAT DU CST

De toute évidence, les violents attentats terroristes du 11 septembre 2001 ont bouleversé à jamais notre façon de traiter les questions de sécurité en Amérique du Nord.

Ces événements ont été un réveil brutal pour le Canada et un point tournant pour le CST. La *Loi antiterroriste* qui a été proclamée en décembre 2001 a eu deux impacts importants sur le CST : elle a conféré au CST un mandat législatif et elle a comblé une lacune en matière de pouvoirs qui a permis au CST de s'engager dans la guerre contre le terrorisme.

En vertu de son mandat conféré par la loi, le CST assume trois grands rôles : la collecte de renseignements étrangers, la protection de l'information électronique et la prestation d'assistance aux organismes fédéraux chargés de l'application de la loi et de la sécurité.

J'aimerais maintenant m'attarder sur ces trois éléments du mandat du CST pour mieux les expliquer.

Premièrement, le CST utilise des méthodes à la fine pointe de la technologie pour acquérir des communications étrangères afin de fournir du renseignement étranger au gouvernement du Canada. Le travail du CST est de repérer précisément les communications qui contiennent du renseignement étranger utile, de les acquérir, de les traiter pour comprendre l'information qu'elles contiennent et de diffuser cette dernière aux personnes qui en ont besoin.

Conformément aux priorités approuvées par le cabinet, le CST fournit du renseignement à des centaines de clients au gouvernement fédéral. Ce renseignement les aide à mieux comprendre les enjeux mondiaux. Il étaye leurs décisions. Il contribue à l'élaboration des politiques étrangères et des

politiques de défense du Canada. Et plus important encore, il aide à protéger la sécurité du pays et de ses citoyens et citoyennes.

À l'appui des engagements soulignés dans la *Politique de sécurité nationale*, le CST se concentre maintenant beaucoup plus sur les enjeux de sécurité. En effet, l'organisme consacre la majorité de ses ressources en matière de renseignement étranger à la collecte de renseignements et à la production de rapports sur des sujets tels le terrorisme, la prolifération et les cybermenaces. Le CST appuie également les activités des Forces canadiennes déployées à l'étranger.

Deuxièmement, dans le cadre de son programme de sécurité des TI, le CST fournit des avis, des conseils et des services pour aider à protéger l'information électronique.

Ce programme est mené dans un contexte où l'on reconnaît de plus en plus que la sécurité et la prospérité de notre pays dépendent de la sécurité de son information la plus importante, et où l'on est de plus en plus conscient que les cyberattaques posent des menaces permanentes et réelles.

Ainsi, le CST analyse les menaces et les vulnérabilités pour déterminer là où la protection doit être accrue.

Nous collaborons aussi avec d'autres organismes du gouvernement pour prédire et prévenir les cyberattaques, et nous aidons à développer et à approuver les systèmes et dispositifs de communication sécurisés qui protègent l'information la plus sensible du gouvernement.

S'alignant sur les objectifs de la *Politique de sécurité nationale*, le CST cherche de plus en plus à aider le gouvernement à protéger ses renseignements et ses réseaux essentiels.

Troisièmement, le CST fournit un soutien aux organismes fédéraux chargés de l'application de la loi et de la sécurité. C'est là un prolongement naturel de l'expertise technique du CST dans des domaines tels la cryptologie et la sécurité des TI.

Il faut absolument comprendre que, dans le cadre de ce troisième élément de son mandat, le CST peut fournir de l'aide technique et opérationnelle à ses partenaires fédéraux uniquement dans le cadre de leurs propres pouvoirs et limites.

Si, par exemple, le CST fournit une assistance opérationnelle au SCRS en vertu de cette partie de son mandat, il le fait dans le cadre des pouvoirs du SCRS, sous sa supervision directe conformément à ses règles et procédures.

DÉCLIN DE L'EFFICACITÉ

Permettez-moi maintenant de passer aux graves lacunes juridiques que comportait la structure des pouvoirs du CST auxquels la *Loi antiterroriste* a remédié.

Pendant les années 1990, alors que le CST se délestait des charges engendrées par la guerre froide, le monde des télécommunications prenait

son essor à un rythme révolutionnaire. Les nouvelles technologies ont connu une expansion sans égal. Le volume, la variété et la rapidité des communications se sont accrus à une vitesse exponentielle. Le routage des messages est devenu imprévisible. On pouvait trouver « de tout n'importe où » dans le paysage des communications.

Or, le CST devait continuer de travailler dans le contexte d'un cadre juridique élaboré pour protéger la vie privée des Canadiens dans un environnement de communications très différent, et bien moins complexe, que celui d'aujourd'hui.

Dans ce nouvel environnement, l'interdiction absolue d'intercepter des « communications privées », énoncée dans la partie six du *Code criminel*, contribuait de plus en plus à empêcher le CST d'accomplir sa mission de base, celle de recueillir des communications étrangères.

Pour apprécier cet impact à sa juste valeur, il est important de comprendre que la définition d'une communication privée, tel que l'entend le *Code criminel*, comprend toute communication, dont on peut raisonnablement s'attendre à ce qu'elle reste privée, qui débute ou prend fin au Canada.

Cette disposition du *Code criminel* touchait le CST de deux façons.

Premièrement, elle empêchait le CST d'intercepter une communication envoyée du Canada ou reçue au Canada par une cible de renseignement étranger. Par exemple, le CST ne pouvait pas fournir de renseignement sur un groupe terroriste connu à

l'étranger si celui-ci communiquait avec un de ses membres ou avec un complice au Canada.

Deuxièmement, cette disposition empêchait le CST d'intercepter toute communication qui pouvait contenir des informations privées. Il y avait là un obstacle supplémentaire, car dans ce nouvel environnement technologique où « tout se trouve n'importe où », – cette jungle pratiquement infinie de communications et d'autoroutes électroniques – il était impossible pour le CST de démontrer, avant qu'il n'ait intercepté la communication que sa provenance et sa destination étaient toutes les deux étrangères.

Le résultat était qu'à mesure que les technologies évoluaient, le CST était de plus en plus incapable d'accéder à des sources de renseignement utiles.

Au moment où les attentats du 11 septembre ont eu lieu, tous les principaux partenaires internationaux du CST, les États-Unis, la Grande-Bretagne, l'Australie et la Nouvelle-Zélande, avaient déjà trouvé des solutions à cette question. Le CST se faisait devancer.

À l'égard de son mandat de protection, la capacité du CST à protéger l'information et les systèmes électroniques s'érodait également.

Dans le nouveau cyberenvironnement, le CST devait surveiller les activités des réseaux du gouvernement du Canada et obtenir des échantillons de messages ayant des caractéristiques de virus ou d'autres codes malveillants.

Or, en interdisant d'intercepter des communications privées, le *Code criminel* empêchait le CST d'entreprendre ces activités de protection essentielles.

Par conséquent, le CST perdait rapidement son emprise sur les outils essentiels de protection de l'information.

LOI ANTITERRORISTE – IMPACT SUR LE CST

Rien n'aurait pu souligner plus clairement les limites des pouvoirs du CST que les événements du 11 septembre 2001.

Suite à ces événements, les dispositions relatives au CST dans la *Loi antiterroriste* ont été conçues pour que les pouvoirs du CST reflètent à la fois les exigences du nouvel environnement de sécurité et les réalités des communications modernes, ainsi que l'obligation de protéger la vie privée des Canadiens.

Plus précisément, des mesures ont été prises pour exempter le CST de la partie six du *Code criminel*, lorsque le CST pouvait démontrer qu'il avait besoin de cette exemption pour remplir son mandat.

La *Loi* comprend donc un mécanisme, une autorisation du ministre de la Défense nationale, qui permet au CST d'intercepter des communications privées lorsqu'il dirige ses activités contre des entités étrangères situées dans d'autres pays.

LE TEXTE PRONONCÉ FAIT FOI

Je veux être très clair au sujet des activités que le ministre de la Défense nationale peut autoriser.

En vertu de la loi, le CST n'a pas le droit de diriger ses activités contre des personnes qui se trouvent dans le rayon de 12 milles délimitant le territoire canadien, que ces personnes soit canadiennes ou étrangères. Le CST n'a pas non plus le droit de diriger ses activités contre les Canadiens à l'étranger, que la *Loi* définit comme étant des Canadiens et des résidents permanents.

Toutefois, avec une autorisation ministérielle, lorsqu'il dirige ses activités contre des entités étrangères dans d'autres pays, le CST peut maintenant mener des activités même si en ce faisant il risque d'acquérir des « communications privées ». Lorsque cela se produit, la *Loi* permet au CST d'utiliser et de conserver ces communications, moyennant des mesures de protection très strictes. Autrement, dès qu'elles sont identifiées comme telles, les communications privées sont supprimées.

De même, le CST peut maintenant obtenir une autorisation ministérielle pour mener des activités de sécurité des TI essentielles dans le cadre desquelles des communications privées pourraient être interceptées.

En pratique, aussi bien pour le renseignement étranger que pour la sécurité des TI, le CST demande une autorisation ministérielle pour s'assurer une protection légale contre ce qui représenterait autrement une infraction au *Code criminel*, celle d'intercepter des communications privées qu'il pourrait acquérir incidemment dans le cadre d'activités précises de collecte ou de protection.

D'importance égale, ces « activités ou catégories d'activités », pour employer l'expression juridique, ne sont permises qu'une fois que le ministre est satisfait, après un examen approfondi du ministère de la Justice, que les conditions précises soulignées dans la *Loi* ont été respectées.

ÉVOLUTION DU CST DEPUIS LA *LOI ANTITERRORISTE*

Je voudrais maintenant expliquer de façon concrète comment le CST a profité de ses nouveaux pouvoirs.

Dans le cadre de son programme de renseignement étranger, les autorisations ministérielles ont permis au CST d'augmenter de façon importante sa capacité de cerner et de recueillir des communications qui donnent lieu à du renseignement étranger de grande valeur.

Évidemment, je ne peux pas entrer dans le détail des succès du CST en matière de renseignement étranger dans cette tribune publique. Par contre, je peux vous assurer que le renseignement fourni par le CST a directement contribué à la protection des troupes canadiennes en Afghanistan contre des attaques terroristes. Je peux aussi affirmer que le CST a fourni du renseignement sur des cibles terroristes étrangères pour protéger la sécurité et les intérêts de Canadiens et de nos alliés les plus proches. Le CST n'aurait pas été capable d'obtenir ce renseignement sans la *Loi antiterroriste*.

De même, dans le cadre de son programme de sécurité des TI, le CST a utilisé des autorisations ministérielles pour s'assurer que les systèmes et

réseaux informatiques du gouvernement du Canada sont mieux protégés contre les cyberattaques.

PROTECTION DE LA VIE PRIVÉE DES CANADIENS ET DES CANADIENNES

Permettez-moi maintenant de vous présenter les mesures qu'a mises en place le CST pour assurer la protection de la vie privée des Canadiens et des Canadiennes.

Avant de délivrer une autorisation, le ministre doit être convaincu, entre autres, que les activités ne seront pas dirigées contre des Canadiens ni contre toute personne au Canada et qu'il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens.

À cet égard, le CST a établi des procédures complètes pour faire en sorte que ses activités respectent l'esprit et la lettre du droit à la vie privée prévu dans la *Charte*. Tous les membres du personnel du CST prennent très au sérieux cette obligation, et tous ont reçu des directives précises et une formation complète dans ce domaine.

De plus, le CST a institué de nouvelles procédures pour les activités menées dans le cadre d'autorisations ministérielles. Elles permettent d'assurer que les activités du CST sont dirigées contre des entités étrangères dans d'autres pays et qu'elles ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.

Le CST travaille aussi en étroite collaboration avec une équipe juridique du ministère de la Justice, située sur place, pour veiller à ce que ses pratiques et ses procédures répondent à toutes les exigences prescrites par la loi.

Pour ce qui est des examens externes, le commissaire du CST, le très honorable Antonio Lamer – ancien juge en chef de la Cour suprême du Canada – qui travaille indépendamment du CST, a vu son rôle officialisé dans la *Loi antiterroriste*. Le commissaire a pour mandat de procéder à des examens concernant les activités du CST pour en contrôler la légalité. Il a libre accès à tout le personnel, toute l'information et tous les dossiers du CST.

De par la loi, le commissaire doit tous les ans faire rapport au ministre de la Défense nationale de son examen des activités du CST. Le ministre présente ensuite ce rapport au Parlement. En plus, le commissaire soumet régulièrement au ministre des rapports classifiés qui portent plus précisément sur certains programmes ou enjeux.

Je me permets d'indiquer que depuis que son bureau a été fondé en 1996, le commissaire a toujours confirmé que toutes les activités du CST examinées étaient conformes à la loi.

De plus, je note que, depuis que la *Loi antiterroriste* est en vigueur, le Bureau du commissaire à la protection de la vie privée a examiné les activités du CST menées en vertu de son nouveau mandat et n'a soulevé aucune inquiétude.

CONCLUSION

Bref, je suis d'avis que les pouvoirs accordés au CST en vertu de la *Loi antiterroriste* fournissent une bonne assise pour les activités de l'organisme tout en protégeant la vie privée des Canadiens.

La loi a répondu à l'urgent besoin de mettre à jour les pouvoirs du CST, permettant ainsi à l'organisme de contrer les nouvelles menaces et de suivre l'évolution rapide des communications.

Ces nouveaux pouvoirs sont maintenant absolument essentiels aux activités du CST, à sa capacité à surmonter des obstacles techniques incroyables et en fin de compte à sa capacité à contribuer à la sécurité du Canada et à ses autres intérêts nationaux.

En fait, dans le contexte stratégique et technologique actuel, le CST ne peut pas fonctionner de façon efficace sans ces pouvoirs.

Il y a trois ans, le ministre de la Défense nationale et moi-même avons expliqué au Parlement ce dont le CST avait besoin pour aider à protéger la sécurité des Canadiens et des Canadiennes. Le Parlement avait alors la tâche difficile de trouver le juste équilibre entre la protection des droits à la vie privée des Canadiens et la sécurité du pays.

En définitive, le Parlement a accordé au CST les pouvoirs essentiels dont il avait besoin pour être efficace dans le nouvel environnement stratégique et technique. J'espère qu'il continuera à soutenir le CST en lui offrant une

LE TEXTE PRONONCÉ FAIT FOI

structure de pouvoirs qui lui permettra de relever les défis très importants de la sécurité nationale auxquels est confronté notre pays.

Merci. Je serais heureux de répondre aux questions que vous pourriez avoir.