




Commissariat
à la protection de
la vie privée du Canada

Rapport spécial au Parlement

**Mesures de vérification et de contrôle :
Renforcer la protection de la vie privée et la
supervision des activités du secteur canadien du
renseignement à l'ère de la cybersurveillance**

Le 28 janvier 2014



Commissariat à la protection de la privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

© Ministre des Travaux publics et des Services gouvernementaux Canada 2014

IP54-55/2014F-PDF
978-0-660-21730-7

Suivez nous sur Twitter : [@PriveePrivacy](https://twitter.com/PriveePrivacy)

Table des matières

Introduction : Mandat du Commissariat et objet du présent rapport	1
Évolution du contexte de la sécurité nationale	3
Incidence sur la protection de la vie privée	4
Défis particuliers liés à la reddition de comptes dans le contexte du renseignement	5
Secret et imputabilité	5
Collaboration parmi les agences de renseignement sans collaboration parmi les organismes de contrôle	6
Survol des modèles de supervision et d'examen pour les organismes de renseignement	7
Royaume-Uni	7
États-Unis	7
Canada	8
Améliorations recommandées	9
Renforcer les mécanismes d'examen et de présentation de rapports	9
Moderniser le régime de protection de la vie privée	11
Renforcer le cadre actuel de reddition de comptes	12
Conclusion : La protection de la vie privée dans le cadre de la supervision des activités de renseignement	14
Remerciements	15
Annexe A : Bref historique des recommandations successives formulées par le Commissariat au sujet de la supervision, des contrôles et des mécanismes de protection de la vie privée dans le cadre des activités de renseignement	16
Sources	20

Introduction : Mandat du Commissariat et objet du présent rapport

Au cours des derniers mois, les préoccupations au sujet de la protection de la vie privée dans le contexte des activités liées à la sécurité nationale se sont intensifiées. Afin de contribuer à un débat informé et constructif au sujet de ces préoccupations, le Commissariat à la protection de la vie privée du Canada a préparé ce rapport, soumis à la réflexion du Parlement en espérant qu'il lui sera utile afin de déterminer si le Canada dispose toujours de mesures de protection de la vie privée adéquates dans le contexte de la sécurité nationale.

Le Commissariat surveille la conformité à la *Loi sur la protection des renseignements personnels*, qui régit le secteur public fédéral, et à la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui régit le secteur privé. Les organismes et les activités de renseignement sont régis par la *Loi sur la protection des*

renseignements personnels, qui s'applique aux pratiques des institutions fédérales dans le domaine pour protéger la vie privée des individus¹.

Le commissaire à la protection de la vie privée du Canada est un agent indépendant du Parlement. Le Commissariat reçoit des plaintes, effectue des vérifications et formule des avis sur des enjeux touchant la protection de la vie privée à l'intention des organisations commerciales, des institutions fédérales et du Parlement. Le présent rapport spécial est présenté aux deux chambres conformément à l'article 39(1) de la *Loi sur la protection des renseignements personnels*.

Alors que le Commissariat surveille la conformité à la *Loi sur la protection des renseignements personnels* pour l'ensemble de la fonction publique, des organismes spécialisés ont été créés afin de surveiller la conformité aux lois dans le domaine des activités de renseignement au Canada et de procéder à l'examen de celles-ci, entre autres sous l'angle de la protection de la vie privée. Il s'agit entre autres du Comité de surveillance des activités de renseignement de sécurité (CSARS), du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) et de la Commission des plaintes du public contre la GRC.

¹ *Loi sur la protection des renseignements personnels*, L.R.C., 1985, ch. P-21, art. 2.

Le droit à la vie privée est un droit fondamental au Canada. Il est garant de l'intégrité des personnes et essentiel à une société libre et démocratique. Or, les événements récents ont mis en lumière de nouveaux risques en matière de vie privée dans le cadre politique et technologique actuel des activités de renseignement. L'évolution des menaces pesant sur la sécurité des États libres et démocratiques – associée à la vitesse et à la puissance des moyens de surveillance techniques et à la volonté de prévenir les attentats ou de s'y préparer – crée un problème urgent auquel doivent s'attaquer les États démocratiques. Dans un contexte où les préoccupations du public concernant la protection de la vie privée vont en augmentant, le présent rapport a pour but de formuler des recommandations concrètes et de faire progresser un débat public raisonnable et constructif.

Évolution du contexte de la sécurité nationale

Il importe de souligner l'incidence des changements politiques et sociétaux sur les activités liées au renseignement et la protection de la vie privée². De manière générale, les spécialistes canadiens de la sécurité résument ces changements comme suit :

- Le clivage traditionnel entre les menaces intérieures et étrangères s'est estompé en raison des tendances mondiales en matière de migration internationale et de l'utilisation accrue des outils Internet. Par exemple, des citoyens canadiens ont pris part à des attaques terroristes à l'étranger.
- La capacité technique en matière de surveillance a augmenté en flèche, renforcée par la création et la communication comme jamais auparavant de renseignements personnels de sources ouvertes en ligne. Par exemple, des organismes chargés de veiller à la sécurité publique se servent de renseignements personnels recueillis sur des sites de réseautage social.

- L'échange de renseignements personnels, en soi, génère encore plus de renseignements personnels en raison des profils et des métadonnées. En particulier, les communications en ligne peuvent brosser un portrait détaillé d'individus.
- Les menaces à la sécurité nationale, traditionnellement associées à certains États ennemis comme l'Union soviétique au cours de la guerre froide, se sont multipliées et dispersées. Par exemple, certains individus faisant partie de la population générale sont devenus radicalisés et pourraient représenter une menace à la sécurité nationale.
- La surveillance de la population générale s'intensifiant au rythme des percées technologiques et de l'apparition de nouveaux outils, il est désormais possible d'effectuer des collectes de données à des échelles beaucoup plus grandes. Par exemple, les systèmes de télévision en circuit fermé sont maintenant omniprésents.
- Entre temps, les individus qui représentent une menace exploitent eux aussi les renseignements personnels pour leurs propres fins. On pense notamment à l'usurpation d'identité et à la communication par l'entremise d'Internet.

² Angela Gendron et Martin Rudner, *Évaluation des cybermenaces pesant contre les infrastructures du Canada*, mars 2012 – http://publications.gc.ca/collections/collection_2013/scrs-SCRS/PS74-1-2012-fra.pdf, p. 25-42. Voir aussi Martin Rudner, *Canada's Communication Security Establishment: From Cold War to Globalization*, Centre for Security and Defence Studies, document hors série n° 22, 2000 – http://circ.jmellon.com/docs/pdf/canadas_communications_security_establishment_from_cold_war_to_globalization.pdf, p. 23-34; Comité sénatorial spécial sur l'antiterrorisme, *Liberté, sécurité et la menace complexe du terrorisme*, 2011 – <http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-f.pdf>, p. 9-24.

Incidence sur la protection de la vie privée

L'incidence déterminante de ces changements sur la protection de la vie privée découle de l'importance et de la disponibilité sans précédent des renseignements personnels. Les activités de renseignement sont maintenant orientées vers des individus dispersés au sein de la population générale³. Conséquemment, la manière dont ses activités sont menées peuvent ouvrir la voie à une collecte à grande échelle. L'information de sources ouvertes comme celle que l'on retrouve sur les sites de réseautage sociale est balayée électroniquement et a le potentiel de devenir la principale source de renseignement. Toutefois, l'information est souvent affichée en ligne avec une certaine attente en matière de vie privée — que cette attente soit raisonnable ou non — et de plus, cette information pourrait être erronée. Comme d'autres l'ont souligné, Internet a effacé les distinctions territoriales, les frontières sectorielles et les attributions juridictionnelles nettes en ce qui concerne la collecte de données, la communication d'information et l'analyse du renseignement, tout en multipliant par plusieurs ordres de grandeur la capacité de collecte de renseignements⁴. En outre, le secteur privé, en l'occurrence, le secteur des télécommunications, est de plus en plus chargé directement de la cueillette de

renseignements ou utilisé à cette fin. Les organismes canadiens de renseignement sont de plus en plus entraînés dans des domaines nationaux (p. ex. la lutte contre la radicalisation à l'échelle locale ou contre le financement de mouvements violents).

Le potentiel d'atteinte à la vie privée dans ce nouveau contexte est tel qu'il exige une protection de la vie privée proportionnelle.

³ Martin Rudner, « Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism », *Intelligence and National Security*, vol. 22, n° 4, 2007, p. 473-490.

⁴ Andrea Wright, *Security Intelligence: New Challenges for Democratic Control*, 2007, allocution prononcée à la Conférence 2007 du Consortium européen pour la recherche politique.

Défis particuliers liés à la reddition de comptes dans le contexte du renseignement

SECRET ET IMPUTABILITÉ

Le secret fait partie intégrante de nombreuses activités de renseignement — il en va de même de la reddition de comptes. Les exigences en matière de présentation de rapports ainsi que les examens et les contrôles pertinents prévus par la loi obligent les décideurs et les institutions à rendre des comptes. Les arguments relatifs à la sécurité nationale ne réduisent en rien les obligations redditionnelles, et les organismes de sécurité doivent rendre compte aux Canadiens de l'usage qu'ils font des renseignements personnels⁵. Des mécanismes d'examen indépendants sont nécessaires pour assurer cette reddition de comptes par les organismes de sécurité, préserver la confiance du public et vérifier que le respect des droits individuels peut être démontré⁶.

⁵ Ronald Deibert, *Bounding Cyber Power: Escalation and Restraint in Global Cyberspace*, CIGI, Internet Governance Papers, octobre 2013 – http://www.cigionline.org/sites/default/files/no6_2.pdf, p. 15; voir aussi Ronald Deibert, *Black Code: Inside the Battle for Cyberspace*, 2013, p. 8-11 et 31-43.

⁶ Comité sénatorial permanent de la sécurité nationale et de la défense, « Manque de surveillance », *Manuel de sécurité du Canada*, décembre 2004 – <http://www.parl.gc.ca/Content/SEN/Committee/381/defe/rep/rep03nov04part2-f.htm>.

Dans son rapport annuel 2012-2013 – le dernier de son mandat – l'ancien commissaire du Centre de la sécurité des télécommunications, l'honorable Robert Décary, affirme : « Il reste beaucoup à faire, encore, mais je crois que la glace est brisée et que les autorités concernées comprennent mieux aujourd'hui qu'il est possible, sans trahir des secrets d'État et sans mettre en péril la sécurité nationale, d'expliquer avec beaucoup plus d'ouverture le travail qu'elles font. Plus la transparence sera grande, plus le scepticisme et le cynisme de la population iront s'atténuant ». La transparence est la clé de l'imputabilité.

Quoi qu'il en soit, on doit dans de nombreux cas protéger les détails personnels concernant les employés, les informateurs rémunérés, les cibles ou les personnes d'intérêt. Il y a des limites raisonnables à la communication intégrale et proactive de l'information sur toutes les opérations gouvernementales, en particulier celles associées à une fonction de sécurité et de renseignement. Pour que les sources et les techniques demeurent efficaces et fiables, il faut éviter de les divulguer. Les échanges opérationnels très sensibles avec d'autres gouvernements et des partenaires doivent se faire en préservant un certain niveau de confidentialité et ne peuvent être décrits en détail. Il est toutefois important de rappeler que des dispositions visant à protéger l'information dans ces cas sont déjà prévues dans la législation actuelle : la *Loi sur le Service canadien du renseignement de sécurité*, la *Loi sur la protection de l'information*, la *Loi sur la preuve au Canada*, la *Loi sur la protection des renseignements personnels* et la *Loi sur l'accès à l'information*⁷.

⁷ Stanley Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril*, Lexis Nexis, 2005, p. 289-314.

Les organismes de sécurité eux-mêmes bénéficieraient d'un élargissement de la portée du débat public dans le cadre duquel ils doivent être en mesure de participer à une discussion intelligente, à tout le moins sur les grandes questions associées à la protection de la vie privée. Traditionnellement, les organismes de renseignement ont évité le débat public concernant leur rôle au sein des sociétés démocratiques. Leurs témoignages dans le cadre des débats parlementaires publics ont été relativement peu nombreux. Le Canada ne fait pas figure d'exception; tous ses alliés entretiennent cette culture du secret depuis près de 60 ans. Toutefois, le Centre de la sécurité des télécommunications Canada (CSTC) et le BCCST ont tous deux affiché récemment sur leurs sites Web respectifs de l'information décrivant leur mandat et leurs activités, en réponse aux préoccupations du public et aux controverses médiatiques, et dans le but d'améliorer les connaissances au sujet de leurs travaux.

COLLABORATION PARMIL LES AGENCES DE RENSEIGNEMENT SANS COLLABORATION PARMIL LES ORGANISMES DE CONTRÔLE

Comme l'indique le plus récent rapport du CSARS, on observe un « fusionnement accru des mondes du renseignement d'origine humaine (HUMINT) et du renseignement d'origine électromagnétique (SIGINT), mondes autrefois bien distincts » et l'intégration accrue de ces domaines « pourrait conduire à la perte potentielle de contrôle sur l'information partagée ». L'honorable Robert Décary signale dans son dernier rapport : « Tandis que le Centre et le SCRS collaborent et mènent des actions conjointes, mon bureau et le CSARS n'ont pas la possibilité de mener une enquête conjointe. Il existe quand même une certaine possibilité de collaboration en vertu de la législation actuelle. »

Toutefois, la *Loi sur la protection des renseignements personnels* est demeurée essentiellement intacte depuis 1983. La loi ne contient aucune disposition qui ne permette de mener des enquêtes ou des vérifications conjointes avec d'autres organismes semblables, même à une époque où le partage de renseignements a augmenté de façon importante.

Survol des modèles de supervision et d'examen pour les organismes de renseignement

Comment pouvons-nous atteindre une norme élevée de protection de la vie privée dans ce nouveau contexte du renseignement?

Un aperçu des modèles en cours au Royaume-Uni, aux États-Unis et au Canada témoignant de l'éventail de mécanismes qu'il pourrait être utile d'envisager.

ROYAUME-UNI

- Au Royaume-Uni, un commissaire indépendant examine les demandes de mandat et les approbations des enquêteurs gouvernementaux selon des conditions précises définies par la loi.
- Des statistiques sur les interceptions de communications privées sont également compilées et publiées une fois l'an, et elles sont accompagnées de précisions sur toutes les demandes gouvernementales de soi-disant « renseignements sur les abonnés » permettant d'identifier des individus en particulier dans le cadre d'une enquête. Ce régime est en place depuis l'adoption de la *Regulation of Investigatory Powers Act* (RIPA) en 2001.
- Des commissaires spéciaux sont par ailleurs chargés de la protection des renseignements, de la surveillance, de l'utilisation de caméras en circuit fermé et des services de renseignement.
- En outre, le Royaume-Uni a créé un comité spécial doté d'une autorisation de sécurité, dont les membres sont issus des deux chambres du Parlement – le Comité du

renseignement et de la sécurité (Intelligence and Security Committee) – pour superviser les activités relatives à la sécurité nationale approuvées par le ministre (conformément aux dispositions révisées de la *Justice and Security Act* de 2013)⁸.

ÉTATS-UNIS

- Aux États-Unis, un tribunal spécial constitué de juges ayant une autorisation de sécurité préside la Foreign Intelligence Surveillance Court (FISC), qui est chargée d'approuver les activités de surveillance du Federal Bureau of Investigation (FBI) et de la National Security Agency (NSA)⁹.
- Le Congrès dispose, pour chaque chambre, d'un comité permanent distinct doté d'une autorisation de sécurité et chargé de la surveillance du renseignement. On estime que ces deux comités remplissent une importante fonction d'analyse critique¹⁰.
- Le Congrès administre et dirige également le Government Accountability Office, qui est un organisme indépendant.

⁸ Parlement du Royaume-Uni. A Bill to provide for oversight of the Security Service, the Secret Intelligence Service, GCHQ and other activities relating to intelligence or security matters; to provide for closed material procedure in relation to certain civil proceedings; to prevent the making of certain court orders for the disclosure of sensitive information; and for connected purposes (Justice and Security Act 2013) – <http://services.parliament.uk/bills/2012-13/justiceandsecurity/stages.html>. Voir aussi Nicholas A. MacDonald, « Les parlementaires et la sécurité nationale au Canada », *Revue parlementaire canadienne*, hiver 2011 –

http://www.revparl.ca/34/4/34n4_11f_MacDonald.pdf.

⁹ Frederick Kaiser, « Congressional Oversight of Intelligence: Current Structure and Alternatives », dans *Intelligence Oversight and Disclosure Issues*, Nova, 2010, p. 1-27.

¹⁰ Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment, National Research Council of the National Academies, Washington DC, National Academies Press, 2008 – http://iis-db.stanford.edu/pubs/22285/Protecting_Individual_Privacy.pdf, p. 166-184.

- La Maison-Blanche a mis sur pied un comité de surveillance de la protection de la vie privée et des libertés civiles dont le mandat consiste à formuler des avis à l'intention du président et à faire rapport au Congrès sur la lutte contre le terrorisme, la protection de la vie privée et les libertés civiles.
- Des rapports annuels sur les écoutes électroniques, les enregistreurs de numéros de téléphone composés et les dispositifs d'interception et de localisation sont présentés au Congrès.

CANADA

- Au Canada, le Parlement a adopté, au début des années 1980, la *Loi sur le Service canadien du renseignement de sécurité*¹¹, qui définit clairement les menaces et établit les limites des enquêtes¹².
- La *Loi* établissait également le CSARS afin de protéger les droits et les libertés des Canadiennes et des Canadiens, et de veiller à ce que le Service canadien du renseignement de sécurité (SCRS) exerce ses activités en toute légalité et de façon appropriée en tout temps¹³.
- Le CSARS présente occasionnellement des rapports sur le nombre de mandats délivrés ou renouvelés.

- En vertu de la *Loi*, des rapports détaillés sur la surveillance électronique exercée par les organismes fédéraux chargés de l'application de la loi sont aussi soumis annuellement à l'examen du Parlement (comme l'exige l'article 195 du *Code criminel*).
- Des rapports annuels donnant des précisions sur d'autres pouvoirs extraordinaires comme l'arrestation préventive et la tenue d'audiences dans le cadre des enquêtes sont également exigés¹⁴.
- Depuis 1997, le BCCST présente chaque année au ministre de la Défense nationale un rapport qui est ensuite déposé au Parlement. Le rôle du commissaire du CSTC est de s'assurer que le CSTC agit en conformité avec la loi et entreprend des mesures pour protéger la vie privée des Canadiennes et des Canadiens.
- Depuis 1988, la Commission des plaintes du public contre la GRC joue un rôle similaire en matière d'examen¹⁵.

¹¹ Comité spécial d'examen de la Loi sur le Service canadien du renseignement de sécurité et de la Loi sur les infractions en matière de sécurité, Chambre des communes, « Une période de transition mais non de crise : rapport à la Chambre des communes du Comité spécial d'examen de la Loi sur le Service canadien du renseignement de sécurité et de la Loi sur les infractions en matière de sécurité », Ottawa, Imprimeur de la Reine du Canada, 1990, p. 83-184.

¹² Timothy S. Hardy, « Intelligence Reform in the mid-1970s », *CIA Center for the Study of Intelligence Archive*, vol. 20, n° 2 – <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol20no2/pdf/v20i2a01p.pdf>, p. 10-13.

¹³ Comité de surveillance des activités de renseignement de sécurité, À propos du CSARS, octobre 2012 – <http://www.sirc-csars.gc.ca/abtprp/index-fra.html>.

¹⁴ Sécurité publique Canada, Rapport annuel sur la surveillance électronique, 2012 – <http://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/lctnrc-srvllnc-2012/index-fra.aspx>; Sécurité publique Canada, Rapport annuel concernant les engagements assortis de conditions : arrestations effectuées sans mandat – <http://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/rrsts-wtht-wrnt-2007-fra.aspx>; ministère de la Justice du Canada, Fiche d'information : La Loi sur la lutte contre le terrorisme – Dispositions sur les audiences d'investigation et les engagements assortis de conditions, avril 2010 – http://www.justice.gc.ca/fra/nouv-news/cp-nr/2010/doc_32499.html.

¹⁵ En raison des modifications apportées récemment à la Loi sur la GRC, la Commission des plaintes du public contre la GRC jouera bientôt un rôle accru en matière d'examen et sera habilitée à mener de vastes enquêtes systémiques permettant d'analyser de façon plus approfondie le travail au chapitre de la sécurité nationale.

Améliorations recommandées

Le but de la revitalisation sur ce front devrait être de protéger la vie privée dans un climat de menaces complexes; de surveiller la collecte pour s'assurer qu'elle est raisonnable, proportionnée et aussi peu envahissante que possible; de veiller à la mise en place de contrôles appropriés concernant la conservation et l'accès (par les intervenants des secteurs public et privé); de veiller à l'exactitude des analyses; et de limiter la portée des demandes et de la communication de renseignements au moyen de mesures de sécurité adéquates, d'ententes et de mises en garde¹⁶.

Pour formuler les recommandations qui suivent, nous nous sommes grandement inspirés de l'expérience historique du Canada, du Royaume-Uni et des États-Unis¹⁷. À notre avis, l'actuel système canadien de surveillance du renseignement fonctionnerait mieux si on l'adaptait aux nouvelles réalités opérationnelles¹⁸. Nous estimons que les mesures proposées ci-après permettraient d'améliorer raisonnablement le cadre actuel et de protéger les droits des individus.

¹⁶ Andrea Wright, « Casting Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight and Review », dans *The Human Rights of Anti-Terrorism*, Irwin, 2008, p. 327-370.

¹⁷ Jez Littlewood, « Accountability of the Canadian Security and Intelligence Community post 9/11: Still a Long and Winding Road? », dans *Democratic oversight of intelligence services*, Federation, 2010, p. 83-107.

¹⁸ Craig Forcese, « The Collateral Casualties of Collaboration: The Consequence for Civil and Human Rights of Transnational Intelligence Sharing », dans *International Intelligence Cooperation and Accountability*, Londres, Routledge, 2011, p. 72-97.

RENFORCER LES MÉCANISMES D'EXAMEN ET DE PRÉSENTATION DE RAPPORTS

- 1. Exiger du CSTC qu'il présente, de façon proactive, des statistiques annuelles sur les affaires dans le cadre desquelles il a reçu une demande d'aide de la part d'un organisme fédéral en vue de l'interception de communications**
 - En vertu de la *Loi sur la défense nationale*, le CSTC peut offrir un soutien à des organismes fédéraux de sécurité et d'application de la loi, notamment dans le cas d'enquêtes sur des Canadiennes et Canadiens. La publication de rapports annuels réguliers, comme le *Rapport annuel* du CSARS et le *Rapport annuel sur la surveillance électronique* de Sécurité publique Canada, représenterait une amélioration à cet égard¹⁹.
 - Dans la mesure du possible, le CSTC pourrait publier des renseignements à jour plus détaillés sur le mandat et le protocole de fonctionnement, ainsi que d'autres renseignements statistiques, conformément aux principes de transparence du gouvernement.
- 2. Demander au CSTC de présenter annuellement au ministre un rapport à déposer au Parlement**
 - Modifier la *Loi sur la défense nationale* pour exiger du CSTC la production d'un rapport public non classifié à déposer au Parlement, comme le fait le SCRS. Ce rapport décrirait ses activités en cours et résumerait ses évaluations du risque (extrémisme violent, crime

¹⁹ Centre de la sécurité des télécommunications Canada, *Le CST vu de l'intérieur – Soutien aux organismes fédéraux chargés de l'application de la loi et de la sécurité*, décembre 2013 – <http://www.cse-cst.gc.ca/home-accueil/inside-interieur/assist-assistance-fra>.

organisé, corruption à l'étranger, etc.) et ses priorités politiques générales²⁰.

3. Élargir la portée des exigences en matière de présentation de rapports sur l'utilisation de la surveillance

- Inclure les autres formes de surveillance électronique pour lesquelles la sécurité nationale constitue le critère d'obtention d'une autorisation dans le *Rapport annuel sur la surveillance électronique* de Sécurité publique Canada. Mentionnons notamment l'utilisation d'ordonnances de communication ainsi que le pistage de l'emplacement et l'installation d'enregistreurs de données, qui sont des mesures auxquelles les enquêteurs peuvent avoir recours en vertu du *Code criminel*.
- Pour les besoins de la production de rapports, séparer les activités menées à la demande du gouvernement canadien et les activités menées à la demande d'un gouvernement étranger, ainsi que les activités nécessitant une approbation sous forme de mandat et les activités d'aide à des enquêtes pour lesquelles l'obtention d'un mandat n'est pas nécessaire.

4. Mettre à jour le document présentant un survol du secteur du renseignement canadien

- Mettre à jour le document intitulé *La collectivité canadienne de la sécurité et du renseignement* et en publier une nouvelle édition aux fins de sensibilisation du public et comme document de référence pour les médias. La dernière édition a été publiée en 2001 par le Secrétariat de la sécurité et du renseignement du Bureau du Conseil privé²¹.

- Décrire le processus qui sous-tend la collecte de renseignements en expliquant le mode d'établissement des priorités et des exigences en matière de renseignement et indiquer les contrôles internes en place dans l'appareil de sécurité et de renseignement au Canada²².
- Demander au gouvernement de produire un livre blanc afin de préciser le mandat des divers organismes de renseignement canadiens et les modalités de leur coopération avec les partenaires étrangers. Faire ressortir dans les attributions l'importance de la protection de la vie privée et des droits garantis par la *Charte canadienne des droits et libertés* ainsi que les enseignements tirés de diverses commissions d'enquête (O'Connor, Iacobucci et Major)²³. Une fois publié, ce livre blanc pourrait faciliter la discussion et favoriser l'apport d'améliorations à long terme.

²⁰ Nombre de ces détails figurent dans d'autres publications du CSTC couramment rendues publiques ou communiquées en vertu du processus d'accès à l'information.

²¹ Bureau du Conseil privé, *La collectivité canadienne de la sécurité et du renseignement*, 2001 – <http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/csis-scrs/pdf/si-fra.pdf>.

²² Par exemple, il faut justifier le mode d'établissement actuel des priorités en matière de collecte de renseignements d'origine électromagnétique étant donné que la collecte au CSTC est soumise à des contrôles internes minimes (contrairement aux processus de ciblage interne en place au SCRS) et qu'aucun examen judiciaire n'est effectué (contrairement aux pratiques en vigueur au sein de la Gendarmerie royale du Canada et de l'Agence des services frontaliers du Canada). Un meilleur accès à l'information concernant le fonctionnement de l'appareil de sécurité nationale et aux renseignements personnels recueillis et analysés par les organismes est essentiel pour assurer un contrôle et un débat démocratique efficaces. Voir Cour fédérale du Canada, *Affaire intéressant une demande présentée par [] visant la délivrance d'un mandat en vertu des articles 12 et 21 de la Loi sur le service canadien du renseignement de sécurité*, LRC 1985, c C-23, 2013 CF 1275 – <http://reports.fja.gc.ca/fra/2015/2013cf1275.html>.

²³ Bureau du Conseil privé, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, 2004 – <http://publications.gc.ca/site/fra/259269/publication.html>, p. 21-22.

5. Produire un rapport sur les recommandations de la Commission d'enquête Major

- Produire un rapport d'étape public (comme l'a demandé le juge Major à la fin de son mandat à la tête de la Commission d'enquête) sur l'examen, le rejet et la mise en œuvre de ses recommandations ainsi que de celles de la Commission O'Connor sur l'examen de la politique²⁴.

MODERNISER LE RÉGIME DE PROTECTION DE LA VIE PRIVÉE

6. Réformer les lois sur la protection de la vie privée pour restreindre la collecte excessive et baliser la communication de renseignements personnels

- Modifier les deux lois fédérales sur la protection de la vie privée, soit la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)²⁵.

²⁴ Il faudrait également veiller en priorité à expliquer de manière plus claire aux citoyens et aux parlementaires la façon dont les examens opérationnels ont été effectués par le passé et les enseignements qui en ont été tirés (p. ex. examen interne de la GRC après le rapport O'Connor). Les exigences du Bureau du Conseil privé devraient également imposer une certaine forme de participation et de consultation du public pour assurer la transparence concernant l'établissement des priorités en matière de renseignements. Dans ce contexte particulier, ces recommandations découlent du rapport Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India, volume 4, intitulé *Particularités des poursuites pour terrorisme : Vers une meilleure conciliation du renseignement de sécurité et de la preuve*, 2010 – http://publications.gc.ca/collections/collection_2010/bcp-pco/CP32-89-5-2010-4-fra.pdf, p. 204-311.

²⁵ Comme nous l'avons mentionné plus haut, les capacités de collecte et d'analyse des renseignements transcendent les secteurs et les frontières plus que jamais auparavant, tandis que le rôle des organismes d'examen et la mission des parlementaires sont demeurés pratiquement inchangés.

- Dans ce contexte particulier, sous le régime de la *Loi sur la protection des renseignements personnels*, demander aux ministères de faire la preuve que la collecte de renseignements personnels est nécessaire.
- Exiger une évaluation des facteurs relatifs à la vie privée avant la mise en œuvre de nouveaux programmes.
- Renforcer les dispositions régissant l'échange de renseignements personnels avec des autorités étrangères pour favoriser la protection de la vie privée. Notamment :
 - Les organismes canadiens devraient traiter avec le plus grand soin les renseignements personnels qu'ils transfèrent aux organismes étrangers.
 - Il leur incombe également de s'assurer que la communication des renseignements est justifiée par une enquête.
 - Des mises en garde s'imposent aussi quant à l'utilisation de renseignements sensibles par les organismes canadiens et étrangers et à leur communication à d'autres intervenants.
 - Les règles régissant la coopération entre organismes nationaux et internationaux doivent être définies aussi clairement que possible au préalable et, dans la mesure du possible, consignées par écrit.
 - Les organismes canadiens doivent faire preuve de circonspection lorsqu'il s'agit d'étiqueter des personnes.
 - Les organismes canadiens ne peuvent recycler le renseignement provenant de l'étranger sans en avoir évalué l'exactitude.

- Élargir les motifs de recours à la Cour fédérale en vertu de la *Loi sur la protection des renseignements personnels*. Présentement, le Commissariat à la protection de la vie privée du Canada peut uniquement saisir la Cour fédérale de questions relatives à l'accès aux renseignements personnels par les individus concernés. Alors que le CSARS et le commissaire du CSTC peuvent recevoir des plaintes du public, le Commissariat à la protection de la vie privée pourrait recevoir des plaintes portant sur des enjeux de sécurité nationale qui ne sont pas de leur ressort. Si ces plaintes visaient la collecte, l'utilisation ou la communication, nous n'aurions aucun recours en Cour fédérale sauf en ce qui a trait à l'accès aux renseignements personnels. Nous recommandons par conséquent d'élargir les motifs justifiant un examen par la Cour fédérale de manière à couvrir la collecte, l'utilisation et la communication des renseignements personnels.
- De même, exiger la présentation de rapports publics sur le recours à diverses dispositions de la LPRPDE dans les cas où des entités du secteur privé telles des télécommunicateurs remettent des renseignements personnels à des organismes de sécurité nationale sans la supervision du tribunal.
- Alors que la supervision de la protection de la vie privée dans le contexte de la sécurité nationale est divisée entre plusieurs organismes de supervision, la *Loi sur la protection des renseignements personnels* ne permet pas au Commissariat de coopérer avec d'autres organismes. La loi devrait être modifiée pour permettre cette collaboration.

7. Réglementer l'accès aux analyses et aux enquêtes réalisées au moyen de sources de renseignements personnels ouvertes accessibles au public

- Élaborer des lignes directrices régissant expressément la collecte, l'utilisation et la diffusion des produits du renseignement reposant sur l'utilisation de sources en ligne et de sites de réseaux sociaux. La prise de position du Commissariat est que le fait que des renseignements personnels soient accessibles sur Internet ne leur enlève pas leur caractère personnel. Nous sommes d'avis que les ministères ne devraient pas accéder aux renseignements personnels sur des sites de médias sociaux à moins qu'ils puissent démontrer un lien direct avec une activité gouvernementale légitime.

RENFORCER LE CADRE ACTUEL DE REDDITION DE COMPTES

8. Accroître les pouvoirs des organismes fédéraux chargés de l'examen des activités liées à la sécurité nationale

- Donner suite concrètement aux préoccupations antérieures du BCCST, de la Commission des plaintes du public contre la GRC et du CSARS concernant la tenue d'examen conjoints et prévoir une consultation préalable auprès de chaque organisme sur les mesures nécessaires²⁶.

²⁶ Par exemple, Bureau du commissaire du Centre de la sécurité des télécommunications, *Sujets d'actualité : Questions et réponses*, 13 janvier 2014 – http://www.ocsec-bccst.gc.ca/new-neuf/faq_f.php.

9. Clarifier et mettre à jour les autres autorisations législatives s'appliquant aux activités de renseignement

- Clarifier les dispositions de la *Loi sur la défense nationale* régissant les autorisations ministérielles afin d'encadrer adéquatement les activités du CSTC sur le plan législatif. Pour reprendre une recommandation antérieure, il serait utile de définir légalement les termes « activité », « catégorie d'activité », « intercepter » et « interception »²⁷.
- Examiner le mandat du CSTC, tel qu'il est défini dans la législation, et présenter explicitement dans la *Loi sur la défense nationale* les modalités générales, les références et les définitions se rapportant à ses opérations²⁸.

²⁷ BCCST, *Rapport annuel 2007-2008*, 2008 - http://www.ocsec-bccst.gc.ca/ann-rpt/2007-2008/ann-rpt_f.pdf, *Rapport annuel 2009-2010*, 2010 - http://www.ocsec-bccst.gc.ca/ann-rpt/2009-2010/ann-rpt_f.pdf, *Rapport annuel 2012-2013*, 2013 - http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_f.pdf.

²⁸ Hubbard, Brauti, Fenton. "Electronic Surveillance under the National Defence Act" du *Wiretapping and Other Electronic Surveillance: law and Procedure* (Mars 2008), 17-1 – 17-10; Penney, Steven, « National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits », *Osgoode Hall Law Journal*, vol. 48, n° 2, 2010, p. 247 – <http://digitalcommons.osgoode.yorku.ca/ohlj/vol48/iss2/2>.

10. Renforcer la coordination et l'investissement à l'appui du rôle de supervision exercé par le Parlement

Les recommandations formulées ci-dessus n'empêchent pas d'élargir le rôle des Parlementaires. De façon générale, ce rôle demeure celui d'exiger une reddition de comptes au nom des Canadiennes et des Canadiens²⁹. À cette fin, nous recommandons ce qui suit aux parlementaires :

- Étudier globalement l'état des mécanismes de supervision et d'examen en place au Canada. Les instances parlementaires actuelles peuvent se pencher sur la reddition de comptes par les ministres et autres dirigeants politiques, tout en effectuant des études utiles et en soulevant des questions stratégiques.³⁰
- Appeler régulièrement les représentants de la communauté canadienne du renseignement à témoigner devant des comités.
- Entendre les points de vue de la société civile, des défenseurs des droits et des universitaires œuvrant dans le domaine.
- Coordonner les sujets d'étude et les témoins pour mieux couvrir le secteur canadien du renseignement. Par exemple, il pourrait y avoir grand intérêt à se pencher sur les questions de protection de la vie privée à la lumière de l'interface émergente entre les organismes de sécurité, les intervenants du secteur privé et la nécessité de préserver une infrastructure essentielle.

²⁹ Comité sénatorial spécial sur l'antiterrorisme, *Liberté, sécurité et la menace complexe du terrorisme : Rapport intérimaire du Comité sénatorial spécial sur l'antiterrorisme*, mars 2011 – <http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-f.pdf>, p. 46-50.

³⁰ Canada. Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada, *Deuxième rapport : La liberté et la sécurité devant la loi*, 1981 – <http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-fra/mcdonald1979-81-rapport2-fra/mcdonald1979-81-rapport2-volume2-fra/mcdonald1979-81rapport2-volume2-partie2-fra.pdf>, p. 939-954.

Conclusion :

La protection de la vie privée dans le cadre de la supervision des activités de renseignement

Comme nous le rappelait le Bureau du vérificateur général dans son rapport de mars 2009, « [l]a population canadienne fera confiance aux organismes de sécurité et de renseignement si elle sait que les ministères et organismes gouvernementaux maintiennent un équilibre entre la protection de la vie privée des citoyens et la sécurité nationale³¹ ».

Nous espérons que le présent rapport contribuera à cet effort.

³¹ Bureau du vérificateur général du Canada, *Rapport de mars 2009 de la vérificatrice générale du Canada — Chapitre 1 — La sécurité nationale : l'échange de renseignements et d'information*, p. 2.

Remerciements

Le Commissariat remercie tout particulièrement les deux conseillers principaux qui ont participé au volet recherche et examen du projet, soit Martin Rudner (professeur-chercheur émérite à l'école Norman Paterson des affaires internationales de l'Université Carleton) et Ray Boisvert (président-directeur général d'I-Sec Integrated Strategies [ISECIS] et directeur adjoint du renseignement au SCRS à la retraite). Leurs idées et leur compréhension des choses nous ont été extrêmement utiles tout au long du processus.

Nous tenons également à exprimer notre reconnaissance au groupe de professionnels dévoués qui nous ont fait bénéficier de leur perspicacité – Robert Marleau (ancien greffier de la Chambre des communes, commissaire à l'information et commissaire à la protection de la vie privée du Canada par intérim), Horst Intscher (ancien directeur du Centre d'analyse des opérations et déclarations financières du Canada), Angela Gendron (attachée supérieure de recherche au Canadian Centre of Intelligence and Security Studies de l'Université Carleton) et Dave McMahon (chef des opérations, Sec Dev Group). Chacun d'entre eux a consacré du temps et des efforts à l'examen des idées et des propositions présentées dans ce rapport.

Enfin, nous avons demandé à des organismes exerçant leurs activités dans la sphère des libertés civiles et de l'examen de la sécurité de formuler des commentaires sur le rapport, soit la Commission des plaintes du public contre la GRC, l'Association canadienne des libertés civiles (ACLC) et la Coalition pour la surveillance internationale des libertés civiles (CSILC). Les opinions qu'ils ont exprimées diffèrent grandement, mais nous tenons à remercier chacun de ces organismes pour leurs précisions, leurs commentaires et leurs critiques.

Annexe A : Bref historique des recommandations successives formulées par le Commissariat au sujet de la supervision, des contrôles et des mécanismes de protection de la vie privée dans le cadre des activités de renseignement

En 2005, dans le contexte de l'examen de la *Loi antiterroriste* par la Chambre des communes, le Commissariat a déposé une série de recommandations visant à renforcer la surveillance et la protection de la vie privée dans le cas du Centre de la sécurité des télécommunications Canada. En 2008, à la suite de la publication des rapports des commissions d'enquête O'Connor et Iacobucci, nous avons exhorté le Parlement à réformer la *Loi sur la protection des renseignements personnels* compte tenu de l'intensification de la communication du renseignement et des activités de surveillance des organismes de sécurité nationale. En 2009, à l'invitation du Comité permanent de la sécurité publique et nationale de la Chambre des communes, nous avons recommandé différents mécanismes pour remédier aux lacunes que nous avons observées dans la supervision du renseignement. En 2011, dans un mémoire présenté dans le cadre des consultations gouvernementales sur la sécurité du périmètre et la compétitivité économique avec les États-Unis, nous avons formulé une série de recommandations sur la surveillance et la supervision. Plus récemment, en 2013, nous avons réclamé une amélioration de la transparence et de la reddition de comptes lorsque des entreprises du secteur privé communiquent des renseignements personnels au gouvernement pour les besoins de l'application de la loi. Toutes ces recommandations ont été consignées dans des mémoires :

Présentation du Commissariat à la protection de la vie du Canada au Comité spécial du Sénat sur la Loi antiterroriste, le 9 mai 2005 (http://www.priv.gc.ca/parl/2005/ata_050509_f.asp#section4.2)

- Les changements que la *Loi antiterroriste* apportent à la *Loi sur la Défense nationale* afin de permettre au Centre de la sécurité des télécommunications d'intercepter les conversations privées auxquelles pourraient participer des personnes au Canada devraient être amendés de façon à ce qu'une autorisation judiciaire préalable soit exigée.

- L'article 273.65(2)d) de la *Loi sur la Défense nationale*, qui est censé assurer la protection de la vie privée des Canadiennes et des Canadiens contre les activités de surveillance des communications effectuées par le CST, devrait être modifié. La condition de « mesures satisfaisantes pour protéger la vie privée des Canadiennes et des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité » devrait être modifiée de façon à exiger « toutes les mesures raisonnables » ou de préciser clairement en quoi des mesures sont « satisfaisantes ».
- L'article 273.65(4)d) de la *Loi sur la Défense nationale* visant à permettre au CST de faire la collecte de renseignements essentiels à la protection des systèmes informatiques du gouvernement limite ce qui peut être « utilisé » ou « conservé ». Il y a lieu d'apporter des modifications pour limiter la *collecte* de renseignements par le CST.
- L'article 273.65(8) de la *Loi sur la Défense nationale* devrait être modifié de façon à exiger que le commissaire du CSTC voie à ce que l'interception de communications privées ait été autorisée par une instruction ministérielle et que l'instruction elle-même soit autorisée par la loi et conforme à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*.

Responsabilité du gouvernement en matière de renseignements personnels : Réforme de la Loi sur la protection des renseignements personnels, avril 2008

(http://www.priv.gc.ca/information/pub/pa_ref_add_080417_f.asp)

- Ajouter l'obligation pour les ministères de prouver la nécessité de recueillir des renseignements personnels.
- Étendre l'examen de la Cour fédérale à tous les aspects touchant la *Loi sur la protection des renseignements personnels*, au lieu de le limiter au refus d'accès, comme c'est le cas actuellement.
- Inscrire dans la loi l'obligation, pour les sous-ministres, d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) avant de mettre en œuvre des programmes et des politiques. Cette obligation devrait comprendre la soumission de l'EFVP à l'examen du Commissariat et la publication des résultats de l'EFVP, sous réserve de contraintes liées à la sécurité nationale.
- Énoncer un mandat clair en matière de sensibilisation du grand public.
- Accorder plus de souplesse au Commissariat quant à la publication des pratiques du gouvernement en matière de gestion des renseignements personnels, au lieu de limiter cet exercice à la publication de rapports annuels et de rapports spéciaux, comme c'est le cas actuellement.
- Accorder au Commissariat le pouvoir discrétionnaire de traiter plus efficacement et promptement les plaintes qui ne revêtent pas une grande importance sur le plan systémique ou sociétal, de façon à lui permettre d'affecter plus de ressources aux plaintes ayant une grande incidence sur l'amélioration de la gestion des renseignements personnels dans l'ensemble du gouvernement fédéral.
- Harmoniser la *Loi sur la protection des renseignements personnels* et la LPRPDE en supprimant la restriction voulant que la première s'applique uniquement aux renseignements consignés.
- Renforcer l'obligation relative au rapport annuel de l'article 72 de la *Loi sur la protection des renseignements personnels*, en exigeant que les institutions fédérales présentent au Parlement un rapport de portée plus générale sur les responsabilités de gestion associées aux renseignements personnels, y compris les responsabilités établies par les politiques du Conseil du Trésor concernant l'évaluation des facteurs relatifs à la vie privée et le couplage de données.

Droits et réalité : augmenter la surveillance des programmes en matière de sécurité nationale du Canada, mai 2009 (http://www.priv.gc.ca/parl/2009/parl_sub_090507_f.asp)

- Souligner à nouveau l'importance d'adopter la méthode employée par les organismes d'examen actuels, afin de permettre une plus grande coordination et une plus grande coopération entre tous les membres du réseau en ce qui a trait aux vérifications et aux rapports. Comme l'a constaté le Commissariat, il est très avantageux de mener conjointement des enquêtes avec les organismes provinciaux et d'élaborer des rapports en collaboration avec les organismes fédéraux de vérification, et toutes les activités du gouvernement bénéficieraient d'une telle approche.
- Aborder la question de la gestion des données et des renseignements personnels par les organismes. Les enquêtes Iacobucci et O'Connor se sont toutes les deux penchées sur la manière dont des renseignements ont été communiqués et sur la qualité de ces renseignements. Une formation améliorée sur la théorie et la pratique en matière de protection de la vie privée, le traitement équitable de l'information et la protection des données pourrait entraîner de grands changements.
- Insister sur la nomination de chefs de la protection des renseignements personnels au sein du gouvernement, en particulier dans les organismes où la collecte de renseignements personnels de nature délicate est généralisée.
- Offrir à la Commission des plaintes du public contre la GRC les ressources et les autorisations légales nécessaires pour lui permettre de réaliser des examens plus importants.
- Insister sur l'urgence, pour le Secrétariat du Conseil du Trésor du Canada et les ministres, d'émettre de nouvelles exigences de la politique obligeant les organismes à utiliser des ententes sur l'échange de renseignements, à réaliser des évaluations des facteurs relatifs à la vie privée, ainsi qu'à formuler des conseils et à émettre des directives sur la protection de la vie privée.
- Insister auprès du gouvernement pour qu'il procède à la réforme de la *Loi sur la protection des renseignements personnels*.
- Accroître le rôle du Parlement dans la supervision des activités liées à la sécurité nationale. Vu l'extrême importance du dossier, il est nécessaire d'accroître les ressources et les fonctions du présent Comité de la Chambre et de son homologue au Sénat quant à la supervision des organismes de sécurité nationale. La mise en commun des compétences spécialisées, la coordination des examens et la communication de l'information pertinente permettrait d'améliorer les mécanismes existants.

Le droit fondamental à la vie privée dans le contexte d'une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre, juin 2011

(http://www.priv.gc.ca/information/research-recherche/sub/sub_bs_201106_f.asp)

- Mettre en place des mesures de contrôle et des limites claires en ce qui a trait à l'échange de renseignements. Bien que le rapport final de l'enquête O'Connor présente de nombreuses recommandations traitant de problèmes au sein de la GRC, l'importance vitale des contraintes, des mesures de contrôle et des mises en garde concernant l'échange de renseignements demeure.
- Étendre la portée des mécanismes de supervision et remettre en question les fonctions liées à l'analyse transfrontalière des renseignements. Le Commissariat insiste sur le fait qu'il faut éviter de conclure des arrangements ne faisant pas état de responsabilités claires en ce qui a trait à la conservation et au contrôle des renseignements personnels, ou prévoyant des mécanismes de responsabilisation insuffisants en ce qui concerne l'utilisation des renseignements à l'extérieur du Canada.
- Appliquer le processus d'évaluation des facteurs relatifs à la vie privée (EFVP).

- Accroître les mesures de protection de la vie privée pour l'échange transfrontalier de données. Les dispositions de la *Loi sur la protection des renseignements personnels* qui régissent la communication de renseignements personnels par le gouvernement du Canada à des États étrangers doivent être renforcées.
- Renforcer les protections de base et le respect des droits et libertés en ligne. La collaboration et la collecte de renseignements par le gouvernement dans un contexte de cybersécurité ne devraient pas prendre de l'ampleur au détriment de la protection de la vie privée des personnes, des libertés civiles et des garanties constitutionnelles. Le Canada et les États-Unis devraient entamer des pourparlers sur la collaboration en matière de cybersécurité en ayant conscience de ce risque.
- Éviter les solutions et les stratégies purement techniques. Tout effort commun doit comprendre des directives juridiques claires. Il doit également s'accompagner d'une éducation et d'une sensibilisation du public à la sécurité des données et aux pratiques de protection des renseignements personnels à grande échelle, d'un renforcement des efforts visant à soutenir la recherche indépendante et multidisciplinaire sur les enjeux liés au cyberespace, d'un engagement binational pour la mise en œuvre de normes de sécurité offrant une meilleure protection de la vie privée et de l'assurance que les organismes de réglementation ont la capacité et l'autorité requises pour garantir de meilleures pratiques au sein de l'industrie.
- Élargir la consultation publique, le dialogue, la sensibilisation et l'engagement. À l'ère du numérique, où les citoyens veulent de l'engagement et de l'interaction, cette absence de dialogue ouvert est clairement inacceptable et nuira aux efforts à long terme. Les responsables canadiens et américains doivent créer des mécanismes pour communiquer régulièrement des rapports publics, permettre l'engagement des citoyens et mettre en place un processus ouvert pour prendre connaissance de leurs préoccupations et de leurs plaintes dès le début des efforts de collaboration en matière de cybersécurité.
- Accroître la recherche publique et le dialogue au sujet des défis internationaux liés à la cybersécurité. Une participation beaucoup plus importante du milieu universitaire, de la société civile, des médias et des citoyens est nécessaire. Il faudrait inciter les universités du Canada et des États-Unis à accroître leur intérêt et leur expertise sur le sujet, à mettre en place des réseaux et à organiser des activités conjointes pour faire état des résultats de leurs travaux de recherche. L'approvisionnement libre, les discussions transparentes et le débat ouvert sur la cybersécurité et sur les questions de protection de l'infrastructure devraient être la norme, et non l'exception.

Arguments en faveur de la réforme de la Loi sur la protection des renseignements personnels et les documents électroniques, mai 2013 (http://www.priv.gc.ca/parl/2013/pipeda_r_201305_f.asp)

- Lever le voile sur les communications autorisées. Exiger des organisations qu'elles rendent public le nombre de communications aux fins d'application de la loi effectuées en vertu de l'alinéa 7(3)c.1), à l'insu de l'intéressé et sans son consentement, et sans mandat, afin de faire la lumière sur la fréquence à laquelle on invoque cette exception et sur l'utilisation qui en est faite.

Sources

- Baldino, Daniel (sous la dir. de). *Democratic Oversight of Intelligence Services*, Sydney, The Federation Press, 2010.
- Ball, Kirstie, Kevin D. Haggerty et David Lyon (sous la dir. de). *Routledge Handbook of Surveillance Studies*, New York, NY, Routledge, 2012.
- Born, Hans et Marina Caparini. *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Burlington, VT, Ashgate Publishing Co., 2007.
- Born, Hans, Ian Leigh et Aidan Wills (sous la dir. de). *International Intelligence Cooperation and Accountability*, Londres, Routledge, 2011.
- Canada. Bureau du Commissaire du Centre de la sécurité des télécommunications. *Rapport annuel 2012-2013*, juin 2013. http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_f.pdf
- Canada. Bureau du Conseil privé. *La collectivité canadienne de la sécurité et du renseignement*, 2001. <http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/csis-scrs/pdf/si-fra.pdf>
- Canada. Bureau du Conseil privé. *Protéger une société ouverte : la politique canadienne de sécurité nationale*, Ottawa (Ont.), 2004. <http://publications.gc.ca/collections/Collection/CP22-77-2004F.pdf>
- Canada. Bureau du Conseil privé. *Rapport du Comité intérimaire de parlementaires sur la sécurité nationale*, 2004. [http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/cpsn-cpsn-cpsn-fra.pdf](http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/cpsn-cpsn/cpsn-cpsn-fra.pdf)
- Canada. Bureau du vérificateur général du Canada, *Rapport de mars 2009 de la vérificatrice générale du Canada — Chapitre 1 — La sécurité nationale : l'échange de renseignements et d'information*.
- Canada. Comité de surveillance des activités de renseignement de sécurité. « Le pourquoi de la surveillance du renseignement de sécurité au Canada », dans *Réflexions. Vingt années de surveillance externe indépendante du renseignement de sécurité au Canada*, Ottawa, Comité de surveillance des activités de renseignement de sécurité, 2005. <http://www.sirc-csars.gc.ca/opbapb/rfcrfx/sc02a-fra.html>
- Canada. Comité sénatorial permanent de la sécurité nationale et de la défense. *Manuel de sécurité du Canada*, décembre 2004. <http://www.parl.gc.ca/Content/SEN/Committee/381/defe/rep/rep03nov04-f.htm>
- Canada. Comité sénatorial spécial sur l'antiterrorisme. *Liberté, sécurité et la menace complexe du terrorisme : des défis pour l'avenir*, mars 2011. <http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-f.pdf>
- Canada. Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada. *Troisième rapport : Certaines activités de la GRC et la connaissance qu'en avait le gouvernement*, Ottawa, c1981. <http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-fra/mcdonald1979-81-fra.htm>
- Canada. Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada. *Deuxième rapport : la liberté et la sécurité devant la loi* (rapport McDonald), Ottawa, c1981. <http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-fra/mcdonald1979-81-fra.htm>
- Canada. Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada. *Premier rapport : Sécurité et information*, Ottawa, 1979, c1980. <http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-fra/mcdonald1979-81-fra.htm>
- Canada. Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar. *Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale — Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar*, Ottawa, Travaux publics et Services gouvernementaux Canada, 2006. http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-fra.pdf

- Canada. Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar. *Rapport sur les événements concernant Maher Arar*, Ottawa, Travaux publics et Services gouvernementaux Canada, 2006. http://www.pch.gc.ca/cs-kc/arar/index_f.htm
- Canada. Commission royale d'enquête sur la sécurité. *Report of the Royal Commission on Security*, Ottawa, Canada, Approvisionnement et Services Canada, 1969. <http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mackenzie1969-eng/mackenzie1969-eng.pdf>
- Cappe, Mel. « Consolider la démocratie par une surveillance efficace », allocation prononcée à la Conférence internationale des organismes de surveillance du renseignement, Ottawa, Canada, le 29 mai 2012.
- Cohen, Stanley A. *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril*, Markham, LexisNexis Butterworths, 2005.
- Cox, James. *Canada and the Five Eyes Intelligence Community*, CDFAI, Strategic Studies Papers, 2012. <http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf>
- Daniels, J., Patrick Macklem et Kent Roach (sous la dir. de). *Security of Freedom: Essays on Canada's Anti-Terrorism Act*, Toronto, University of Toronto Press, 2001.
- Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*, 2013.
- Deibert, Ronald. *Bounding Cyber Power: Escalation and Restraint in Global Cyberspace*, CIGI, Internet Governance Papers, octobre 2013. http://www.cigionline.org/sites/default/files/no6_2.pdf
- Diffie, Whitfield et Susan Eva Landau. *Privacy on the Line: the Politics of Wiretapping and Encryption*, Cambridge, Mass., MIT Press, 2007.
- Forcese, Craig. « Canada's National Security Complex: Assessing the Secrecy Rules », *IRPP Choices*, vol. 15, n° 5, juin 2009. <http://www.irpp.org/assets/research/security-and-democracy/canadas-national-security-complex/vol15no5.pdf>
- Gendron, Angela. « Just War, Just Intelligence: An Ethical Framework for Foreign Espionage », *International Journal of Intelligence and CounterIntelligence*, vol. 18, n° 3, automne 2005.
- Gendron, Angela et Martin Rudner. *Évaluation des cybermenaces pesant contre les infrastructures du Canada – Rapport préparé pour le Service canadien du renseignement de sécurité*, mars 2012. http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-fra.pdf
- Goold, Benjamin J. et Daniel Neyland. *New Directions in Surveillance and Privacy*, Cullompton, Royaume-Uni, Willian, 2009.
- Haas, Philipp R. *Intelligence Oversight and Disclosure Issues*, New York, NY, Nova Science Publishers, 2009.
- Haggerty, Kevin D. (sous la dir. de). *Surveillance and Democracy*, Abingdon, Routledge, 2010.
- Hanks, Peter et John D. McCamus (sous la dir. de). *National Security: Surveillance and Accountability in a Democratic Society*, Cowansville (QC), Yvon Blais, c1989.
- Harris, Shane. *The Watchers: the Rise of America's Surveillance State*, New York, Penguin Press, 2010.
- Harris, Victor H. *Does Intelligence Oversight Support or Hinder Counterinsurgency (COIN) and Homeland Defense Operations?*, Ann Arbor, MI, ProQuest LLC, 2010.
- Lefebvre, Stéphane. « Canada's Intelligence Culture: An Assessment », dans *Democratization of Intelligence: Melding Strategic Intelligence and National Discourse*, Washington DC, National Defense Intelligence College, 2009, p. 79-98. http://www.ni-u.edu/ni_press/pdf/Democratization_of_Intelligence.pdf
- Lefebvre, Stéphane. « Canada's Legal Framework for Intelligence », *International Journal of Intelligence and Counterintelligence*, vol. 23, n° 2, 2010, p. 247-295.
- Leigh, Ian et Ian Lustgarten. *In from the Cold: National Security and Parliamentary Democracy*, Oxford, 1994.
- MacDonald, Nicholas A. « Les parlementaires et la sécurité nationale au Canada », *Revue parlementaire canadienne*, hiver 2011. http://www.revparl.ca/34/4/34n4_11f_MacDonald.pdf
- Mattelard, Armand. *The Globalization of Surveillance*, Malden, MA, Polity, 2010.

- National Research Council of the National Academies. *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, Washington DC, National Academies Press, 2008. http://iis-db.stanford.edu/pubs/22285/Protecting_Individual_Privacy.pdf
- Obar, Jonathan A. et Clement Andrew. *Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty*, 1^{er} juillet 2013. <http://ssrn.com/abstract=2311792>
- Penney, Steven. « National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits », *Osgoode Hall Law Journal*, 247, 2010. <http://digitalcommons.osgoode.yorku.ca/ohlj/vol48/iss2/2>
- Petersen, Julie K. *Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications*, Boca Raton, Auerback Publications, 2007.
- Priest, Dana et William M. Arkin. *Top Secret America: The Rise of the New American Security State*, New York, NY, Little, Brown and Company, 2011.
- Rudner, Martin. *Canada's Communication Security Establishment: From Cold War to Globalization*, Centre for Security and Defence Studies, document hors série n° 22, 2000. http://circ.jmellon.com/docs/pdf/canadas_communications_security_establishment_from_cold_war_to_globalization.pdf
- Rudner, Martin, « Canada's Communications Security Establishment, Signals Intelligence and counter-terrorism », *Intelligence and National Security*, vol. 22, n° 4, p. 473-490.
- Select Committee on the Constitution, Chambre des Lords, Parlement, Grande-Bretagne. *Surveillance: Citizens and the State, Volume II: Evidence*, Londres, Stationery Office Limited, 2007. <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18ii.pdf>
- Solove, Daniel J. *Nothing to Hide: The False Trade-off between Privacy and Security*, New Haven, CT, Yale University Press, 2011.
- Walters, Gregory J. *Human Rights in an Information Age: a Philosophical Analysis*, Toronto (Ont.), University of Toronto Press, 2001.
- Whitaker, Reg, Gregory S. Kealey et Andrew Parnaby. *Secret Service: Political Policing in Canada from the Fenians to Fortress America*, Toronto (Ont.), University of Toronto Press, 2012.
- Wright, Andrea. *Security Intelligence: New Challenges for Democratic Control*, allocution prononcée à la Conférence 2007 du Consortium européen pour la recherche politique, septembre 2007.
- Wright, Andrea. « Casting Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight and Review », dans *The Human Rights of Anti-Terrorism*, Irwin, 2008, p. 327-370.