BIBLIOTHÈQUE du PARLEMENT
LIBRARY of PARLIAMENT

Série des rapports de recherche, 2017-2018
ISSN 2203-5249

Surveillance des organismes de renseignement : comparaison des pays du « Groupe des cinq »

Cat Barker et Claire Petrie (Bibliothèque du Parlement, Australie)
Joanna Dawson et Samantha Godec (Bibliothèque de la Chambre des communes, Royaume-Uni)
Holly Porteous (Bibliothèque du Parlement, Canada)
Pleasance Purser (Bibliothèque du Parlement, Nouvelle-Zélande)

Le 13 décembre 2017

Le présent document est le fruit d'une collaboration entre des chercheurs parlementaires de quatre pays. Chacun est responsable du contenu et de l'exactitude de sa contribution. Nous remercions les auteurs du Canada, de la Nouvelle-Zélande et du Royaume-Uni de leur apport au document.

RÉSUMÉ

- L'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis assurent chacun une surveillance de leurs organismes de renseignement par des instances parlementaires (ou du Congrès), indépendantes ou judiciaires, ou par une combinaison de deux ou trois de ces instances, en plus de la reddition de comptes par le truchement du pouvoir exécutif. Toutefois, il existe des différences dans la nature de ces instances et dans la portée de leurs mandats.
- Les six organismes qui forment la communauté du renseignement **australienne** sont supervisés par un comité parlementaire qui examine leur administration et leurs dépenses, et par un inspecteur général des services de renseignement et de sécurité indépendant, qui examine la légalité et le bien-fondé de leurs activités. La plupart des activités et des pouvoirs des organismes sont autorisés par les ministres responsables. Un examen réalisé en juin 2017 a donné lieu aux recommandations suivantes : les mandats du comité et de l'inspecteur général devraient être élargis de manière à inclure quatre organismes supplémentaires, et les ressources de l'inspecteur général devraient être augmentées de façon importante.
- Le **Canada** a adopté une loi prévoyant la création d'un comité de parlementaires chargé d'examiner les politiques, l'administration, les finances et les activités de la communauté de la sécurité nationale et du renseignement du Canada. À l'heure actuelle, seuls deux organismes sont visés par un examen de la légalité, qui est mené par des experts indépendants. La force policière nationale du Canada, qui a la responsabilité de mener des enquêtes relatives à des infractions en matière de sécurité nationale, est soumise à un examen par un organisme indépendant. Toutefois, cet examen se limite au traitement des plaintes déposées par le public concernant la conduite des agents de police et, avec le consentement du ministre de la Sécurité publique, à la réalisation d'études d'intérêt public sur des activités particulières. On a présenté un projet de loi qui permettrait la création d'un seul comité d'experts chargés d'enquêter sur des plaintes liées aux activités de trois organismes et d'examiner la légalité, le caractère raisonnable et la nécessité de l'ensemble des activités de sécurité nationale et de renseignement du gouvernement fédéral. Le projet de loi propose aussi la création d'un poste de commissaire au renseignement, dont le rôle consisterait à approuver certaines activités entreprises par les organismes responsables du renseignement électromagnétique et du renseignement de sécurité au Canada.
- L'*Intelligence and Security Act 2017* de la **Nouvelle-Zélande** remplace les quatre lois qui s'appliquaient auparavant aux deux organismes de renseignement et de sécurité et à leurs organes de surveillance, et met en œuvre des recommandations issues du premier examen périodique des organismes. Ceux-ci sont supervisés par un comité parlementaire, qui décortique leurs politiques, leur administration et leurs dépenses. Par ailleurs, un inspecteur général des services de renseignement et de sécurité indépendant s'assure que les organismes agissent de manière appropriée et exercent leurs activités légalement et efficacement. Des mandats relatifs au renseignement peuvent être délivrés par un ministre responsable qui agit soit seul, soit conjointement avec un commissaire aux mandats relatifs au renseignement.
- Au **Royaume-Uni**, l'Intelligence and Security Committee (comité du renseignement et de la sécurité) s'attache surtout à surveiller les dépenses, l'administration, les politiques et (avec certaines limites) les activités des trois principaux organismes de renseignement, même si l'examen du travail d'autres organismes de renseignement, de sécurité et d'application de la loi s'inscrit dans son mandat. L'Investigatory Powers Commissioner (commissaire aux pouvoirs d'enquête) assure la surveillance indépendante de l'utilisation de pouvoirs intrusifs par les trois principaux organismes de renseignement. Ce dernier et plusieurs commissaires judiciaires devront examiner régulièrement l'exercice par des organismes publics de diverses fonctions prévues par la loi et pourraient devoir examiner, à la demande du premier ministre, toute autre fonction des trois principaux organismes de renseignement. On a adopté une loi en vertu de laquelle les mandats, actuellement délivrés par les ministres, n'entreront en vigueur qu'après avoir été examinés par un commissaire judiciaire. L'Investigatory Powers Tribunal (tribunal des pouvoirs d'enquête) fait enquête sur des plaintes au sujet de l'utilisation par des organismes publics de pouvoirs d'enquête.

- La communauté du renseignement des **États-Unis** est formée de 17 organismes relevant du pouvoir exécutif. La surveillance par le Congrès de la communauté du renseignement est répartie entre plusieurs comités, y compris des comités spécialisés sur le renseignement à la Chambre et au Sénat. Même si chaque comité a des pouvoirs limités en ce qui concerne ce qu'il peut examiner, collectivement, les comités ont la capacité d'enquêter sur l'ensemble des activités liées au renseignement du gouvernement américain. L'Executive Office of the President (bureau exécutif du président [EOP]) comprend plusieurs mécanismes clés qui permettent la surveillance de la communauté du renseignement, y compris le President's Intelligence Advisory Board (comité consultatif du président sur le renseignement) et le Privacy and Civil Liberties Oversight Board (conseil de surveillance en matière de vie privée et de libertés civiles). Ceux-ci sont renforcés par un réseau d'inspecteurs généraux et de conseillers juridiques. En plus des inspecteurs généraux affectés à des organismes et à des ministères particuliers, l'inspecteur général de la communauté du renseignement effectue des vérifications, des inspections et des enquêtes à l'égard d'activités et de programmes transversaux. La magistrature fédérale examine une vaste gamme d'activités liées au renseignement en vertu d'un certain nombre de lois, y compris la Constitution. Plus particulièrement, le Foreign Intelligence Surveillance Court (tribunal de surveillance des renseignements étrangers) examine les demandes de mandats liées à la collecte de renseignements étrangers par le gouvernement américain.
- Malgré les différences dans l'approche qu'ils adoptent, les cinq pays ont chacun élaboré un cadre qui comprend un système de freins et de contrepoids qui couvre les diverses directions du gouvernement et qui vise à garantir que les organismes sont responsables de leur administration et de leurs dépenses ainsi que de la légalité et du bien-fondé de leurs activités.
- Les communautés du renseignement ont évolué pour répondre aux nouveaux défis à mesure qu'ils surviennent, et elles vont continuer de le faire. Il sera important que les mécanismes de surveillance évoluent au même rythme que ces changements.

TABLE DES MATIÈRES

Page

COLLABORATEURS

Le présent document de recherche est le fruit d'une collaboration entre des chercheurs de l'Australie, du Canada, de la Nouvelle-Zélande et du Royaume-Uni, qui travaillent tous dans des organisations de recherche soutenant leur parlement national respectif.

Le projet a été dirigé par Cat Barker (Bibliothèque du Parlement, Australie). Les autres collaborateurs sont Claire Petrie (Bibliothèque du Parlement, Australie), Holly Porteous (Bibliothèque du Parlement, Canada), Pleasance Purser (Bibliothèque du Parlement, Nouvelle-Zélande), et Joanna Dawson et Samantha Godec (Bibliothèque de la Chambre des communes, Royaume-Uni).

Les politiques en matière de publication du Congressional Research Service (service de recherche du Congrès, États-Unis) empêchent les États-Unis de participer au projet à l'heure actuelle[1]. On a inclus dans la section comparative, sur la base de recherches effectuées par Cat Barker et Samantha Godec, des renseignements sur les mécanismes de surveillance américains.

1. Le Congressional Research Service ne publie pas les rapports qu'il fournit aux parlementaires et aux comités; toutefois, les destinataires des rapports ont été, par le passé, libres de les publier sur leur propre site Web, et certaines tierces parties recueillent les rapports sur des sites Web accessibles au public. On a redéposé en mai 2017 un projet de loi selon lequel le Government Publishing Office devrait rendre accessibles en ligne les rapports du CRS : H.R.2335—Equal Access to Congressional Research Service Reports Act of 2017; J. Haggarty, *Congressmen reintroduce bill to make CRS reports public*, Congressional Data Coalition blog, 9 mai 2017.

LISTE DES ACRONYMES

AAT	Administrative Appeals Tribunal (Australie)
ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
AGO	Australian Geospatial-Intelligence Organisation
AIC	Australian Intelligence Community
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
BCCST	Bureau du commissaire du Centre de la sécurité des télécommunications (Canada)
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada (Canada)
CCETP	Commission civile d'examen et de traitement des plaintes relatives à la GRC (Canada)
COMRENSFC	Commandement du renseignement des Forces canadiennes
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement (Canada)
CSARS	Comité de surveillance des activités de renseignement de sécurité (Canada)
CSNRPM	Conseiller à la sécurité nationale et au renseignement auprès du premier ministre (Canada)
CST	Centre de la sécurité des télécommunications (Canada)
DIBP	Department of Immigration and Border Protection (Australie)
DIO	Defence Intelligence Organisation (Australie)
DSD	Defence Signals Directorate (Australie)
EOP	Executive Office of the President (États-Unis)
ETHI	Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (Canada)
GCHQ	Government Communications Headquarters (Royaume-Uni)
GCSB	Government Communications Security Bureau (Nouvelle-Zélande)
GRC	Gendarmerie royale du Canada
HPSCI	House Permanent Select Committee on Intelligence (États-Unis)
IG	Inspecteur général (États-Unis)
IGIS	Inspector-General of Intelligence and Security (Australie, Nouvelle-Zélande)
INSLM	Independent National Security Legislation Monitor (Australie)
IPA	*Investigatory Powers Act 2016* (Royaume-Uni)
IPC	Investigatory Powers Commissioner (Royaume-Uni)
IPT	Investigatory Powers Tribunal (Royaume-Uni)
ISA 1994	*Intelligence Services Act 1994* (Royaume-Uni)
ISA 2001	*Intelligence Services Act 2001* (Australie)
ISA 2017	*Intelligence and Security Act 2017* (Nouvelle-Zélande)
ISC	Intelligence and Security Committee (Nouvelle-Zélande, Royaume-Uni)
JIC	Joint Intelligence Committee (Royaume-Uni)
JSA	*Justice and Security Act 2013* (Royaume-Uni)
JTAC	Joint Terrorism Analysis Centre (Royaume-Uni)
LCPSNR	*Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (Canada)
MDN	Ministère de la Défense nationale (Canada)
MI5	Security Service (Royaume-Uni)

MI6	Secret Intelligence Service (Royaume-Uni)
NSC	National Security Council (Royaume-Uni)
NZSIS	New Zealand Security Intelligence Service
ONA	Office of National Assessments (Australie)
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement (Canada)
PCLOB	Privacy and Civil Liberties Oversight Board (États-Unis)
PIAB	President's Intelligence Advisory Board (États-Unis)
PJCIS	Parliamentary Joint Committee on Intelligence and Security (Australie)
RIPA	*Regulation of Investigatory Powers Act 2000* (Royaume-Uni)
SCRS	Service canadien du renseignement de sécurité
SECD	Comité sénatorial permanent de la sécurité nationale et de la défense (Canada)
SECU	Comité permanent de la sécurité publique et nationale de la Chambre des communes (Canada)
SIS	Secret Intelligence Service (Royaume-Uni)
SPC	Sécurité publique Canada
SSCI	Senate Select Committee on Intelligence (États-Unis)
USIC	US Intelligence Community

INTRODUCTION

La taille et les pouvoirs des organismes nationaux de sécurité et de renseignement de l'Occident ont augmenté de façon importante depuis les attaques terroristes du 11 septembre. À cause des renseignements révélés par Edward Snowden en 2013 et d'autres réformes apportées aux pouvoirs des organismes de renseignement, y compris celles qui devaient permettre de mieux faire face aux menaces associées au groupe État islamique et aux « combattants étrangers », le cadre de responsabilisation qui s'applique à ces organismes présente un intérêt continu.

Les communautés du renseignement et les cadres de surveillance connexes en Australie, au Canada, en Nouvelle-Zélande, au Royaume-Uni et aux États-Unis ont évolué pour répondre aux besoins particuliers de ces pays et des contextes précis dans lesquels ils exercent leurs activités. Toutefois, en tant que pays démocratiques occidentaux qui font face à des défis semblables pour ce qui est d'équilibrer l'impératif de la reddition de comptes avec le besoin qu'ont les organismes de renseignement de fonctionner avec un degré de confidentialité, et qui collaborent étroitement et ont une relation étroite en matière de partage de renseignements en vertu des arrangements du Groupe des cinq, ces pays sont des exemples pertinents et utiles pour faire une comparaison[2]. En septembre 2016, les organismes de surveillance indépendants des cinq pays ont convenu d'établir le Five Eyes Intelligence Oversight and Review Council (conseil de surveillance et d'examen des activités de renseignement du Groupe des cinq) pour faciliter la mise en commun d'expériences et de pratiques exemplaires au chapitre de la surveillance et de l'examen. Les membres du conseil vont se réunir en personne chaque année et au moyen d'une communication électronique sécurisée tous les trimestres[3].

A. Aperçu et objectif

Le présent document de recherche fournit d'abord des renseignements sur les communautés du renseignement, les mécanismes clés pour la surveillance de la communauté du renseignement, et tout changement récent apporté aux cadres de surveillance en Australie, au Canada, en Nouvelle-Zélande et au Royaume-Uni, ou tout examen de ces cadres, par pays. S'ensuit une analyse comparative qui fait ressortir certaines des similitudes et des différences entre ces pays (incluant les États-Unis) quant aux mécanismes qui existent en matière de surveillance du renseignement.

Dans chaque pays, il y a en place, une surveillance des organismes de renseignement par des instances parlementaires (ou du Congrès), indépendantes ou judiciaires, ou par une combinaison de deux ou trois de ces instances, en plus de la reddition de comptes par le truchement du pouvoir exécutif. Toutefois, il y a des différences dans la nature de ces instances et dans la portée de leurs mandats. En voici des exemples : la mesure dans laquelle les comités du Parlement ou du Congrès peuvent accéder à des documents classifiés, la mesure dans laquelle ils peuvent examiner les activités (par opposition à

2. La coopération entre le Royaume-Uni et les États-Unis à l'égard de renseignements électromagnétiques étrangers a été officialisée au moyen de la signature de l'accord BRUSA (maintenant connu sous le nom de traité UKUSA) en 1946. En 1955, l'accord a été révisé afin d'englober explicitement l'Australie, le Canada et la Nouvelle-Zélande. Cela a constitué le fondement de ce qu'on appelle de façon officieuse l'alliance des « Five Eyes » (Groupe des cinq), qui a été récemment qualifiée d'accord d'échange de renseignements et de coopération le plus complet et étroit du monde dans M. Cullen et P. Reddy, *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*, 29 février 2016, p. 46; National Security Agency Central Security Service, *UKUSA Agreement Release 1940–1956*, site Web de la National Security Agency. En avril 2017, le Canada a publié une version caviardée de l'accord CANUSA de 1949. Voir B. Robinson, *CANUSA Agreement declassified*, blogue Lux Ex Umbra, 23 avril 2017.

3. Inspector-General of Intelligence and Security (IGIS, Australie), *Annual report 2016–17*, 2017, p. v.

l’administration, aux dépenses et aux politiques) des organismes de renseignement, et le fait que la surveillance indépendante est principalement centralisée ou distribuée. Dans tous les pays sauf aux États-Unis, des examens ou des réformes importants des mécanismes de surveillance du renseignement ont été entrepris au cours des cinq dernières années, et d’autres réformes particulières sont actuellement à l’étude en Australie et au Canada. On a bon espoir qu’en mettant en évidence certaines des similitudes et des différences qui existent entre ces systèmes le présent document pourra soutenir les parlementaires dans chacun des pays visés dans le cadre de leur examen des mécanismes actuels et de toute réforme éventuelle.

B. Portée

L’information sur le cadre de surveillance du renseignement de chaque pays porte essentiellement sur les principaux mécanismes en place dans les sphères indépendantes, judiciaires et parlementaires (ou du Congrès). On fournit moins de détails sur les systèmes plus généraux de surveillance par le pouvoir exécutif et d’autres mécanismes redditionnels, comme les vérificateurs généraux, dont la compétence pourrait comprendre les organismes de renseignement, sans y être limitée.

Les organismes présentés pour chaque pays sont ceux qui sont définis ou perçus par le pays comme faisant partie de sa communauté du renseignement au moment de la publication du présent document. Les mécanismes de surveillance décrits sont, sauf indication contraire, ceux qui sont en place au moment de la publication de ce document. Les réformes qui sont envisagées au moment de la publication de ce document sont abordées dans les sections sur les faits nouveaux et les réformes proposées dans chaque pays.

AUSTRALIE

A. Aperçu des organismes de renseignement

L'Australian Intelligence Community (communauté du renseignement de l'Australie [AIC]) comprend les six organismes décrits plus bas. L'AIC fait partie de la communauté de sécurité nationale élargie qui comprend des organismes chargés de l'application de la loi, de la protection frontalière et des politiques[4].

L'Australian Security Intelligence Organisation (organisation du renseignement de sécurité de l'Australie [ASIO]) est l'agence nationale du renseignement de sécurité de l'Australie. Son rôle est de cerner les menaces à la sécurité, d'enquêter sur celles-ci et de fournir des conseils à cet égard, et elle relève du procureur général[5].

L'Australian Secret Intelligence Service (service du renseignement secret de l'Australie [ASIS]) est l'agence de collecte de renseignements secrets étrangers de l'Australie. Ses fonctions principales sont de recueillir et de distribuer dans l'ensemble du gouvernement australien des renseignements étrangers qui pourraient influer sur les intérêts de l'Australie, de réaliser des activités de contre-espionnage et d'assurer la liaison auprès d'organismes de renseignement et de sécurité étrangers. L'ASIS relève du ministre des Affaires étrangères[6].

L'Office of National Assessments (bureau des évaluations nationales [ONA]) est responsable d'analyser l'information (y compris celle provenant de sources ouvertes) liée à des affaires internationales d'intérêt politique, stratégique ou économique pour l'Australie et de fournir des conseils sur celle-ci. Il joue aussi un rôle dans la coordination et l'évaluation des activités de l'Australie liées au renseignement étranger. L'ONA relève du premier ministre[7].

Il y a trois organismes de renseignement au ministère de la Défense, dont deux qui ont des responsabilités qui s'étendent au-delà de ce portefeuille. L'Australian Signals Directorate (direction des renseignements électromagnétiques de l'Australie [ASD], anciennement connue sous le nom de Defence Signals Directorate [DSD]) recueille et analyse des renseignements électromagnétiques étrangers et fournit au gouvernement australien des conseils et des services liés à la sécurité de l'information et des communications[8]. L'Australian Geospatial-Intelligence Organisation (organisation du renseignement géospatial de l'Australie [AGO]) a pour rôle principal de recueillir et d'analyser des renseignements géospatiaux et des renseignements par imagerie dans le but d'informer le gouvernement au sujet des capacités, des intentions ou des activités d'organisations ou de personnes situées à l'extérieur de l'Australie, d'appuyer les activités de l'Australian Defence Force (force de

4. Selon un examen récemment achevé, dans l'avenir, un cadre de référence plus réaliste pour la communauté du renseignement comprendrait également l'Australian Criminal Intelligence Commission, l'Australian Transaction Reports and Analysis Centre et des parties de la police fédérale australienne (AFP) et du ministère de l'Immigration et de la Protection des frontières. Ministère du premier ministre et du Cabinet (PM&C), *2017 Independent Intelligence Review*, Canberra, Commonwealth d'Australie, juin 2017, p. 46 à 48.

5. *Australian Security Intelligence Organisation Act 1979* (*Asio Act*). Voir plus particulièrement les articles 17 (fonctions) et 4 (définition de « sécurité »). Australian Security Intelligence Organisation (ASIO), *About ASIO*, site Web de l'ASIO.

6. *Intelligence Services Act 2001* (ISA 2001), partie 3 (établissement) et articles 6 et 11 (fonctions). Australian Secret Intelligence Service (ASIS), *About us* et *Governance*, site Web de l'ASIS.

7. *Office of National Assessments Act 1977*, particulièrement l'article 5 (fonctions). Office of National Assessments (ONA), *Overview* et *Legislation*, site Web de l'ONA.

8. ISA 2001, articles 7 et 11. Australian Signals Directorate (ASD), *About ASD* et *Accountability*, site Web de l'ASD.

défense de l'Australie) et de soutenir les fonctions de sécurité nationale d'autorités du Commonwealth et des états[9]. La Defence Intelligence Organisation (organisation du renseignement de défense [DIO]) évalue et analyse le renseignement sur des pays et des organisations étrangères afin de soutenir les activités, la capacité et l'élaboration de politiques de l'Australian Defence Force, ainsi que la prise de décisions relativement à des questions de défense et de sécurité nationale[10].

B. Surveillance

1. Surveillance : résumé

Deux commissions royales dirigées par le juge Robert Marsden Hope dans les années 1970 et 1980 et d'autres examens majeurs effectués dans les années 1990 et au début des années 2000 ont joué un rôle important pour définir le cadre de surveillance des organismes de renseignement de l'Australie[11]. Même si l'AIC a grandi depuis et a évolué de façon importante, les principaux mécanismes de surveillance sont pour la plupart demeurés inchangés.

Le Parliamentary Joint Committee on Intelligence and Security (comité mixte du Parlement sur le renseignement et la sécurité [PJCIS]) et l'Inspector-General of Intelligence and Security (inspecteur général du renseignement et de la sécurité [IGIS]) jouent des rôles complémentaires. Le comité surveille l'administration et les dépenses des organismes de renseignement, tandis que l'inspecteur général examine leurs activités opérationnelles. Ces mécanismes permanents sont complétés par des examens externes des organismes de renseignement, le plus récent ayant été effectué en juin 2017[12]. Les changements à apporter aux mécanismes de surveillance recommandés lors du plus récent examen sont décrits plus bas, dans la section intitulée « Faits nouveaux et réformes proposées ».

La surveillance judiciaire des activités liées au renseignement est limitée, les tribunaux participant peu à la délivrance ou à la surveillance de mandats. Le seul tribunal spécialisé est la Security Division of the Administrative Appeals Tribunal (division de la sécurité du tribunal des appels administratifs), qui examine le bien-fondé de la plupart des catégories d'évaluations négatives sur la sécurité émises par l'ASIO[13].

---

9. ISA 2001, articles 6B et 11. Australian Geospatial-Intelligence Organisation (AGO), *About AGO*, *GEOINT support to Government and Defence*, *GEOINT support to national security* et *GEOINT support to military operations*, site Web de l'AGO.

10. Defence Intelligence Organisation (DIO), *About us*, *What we do*, *General intelligence*, « Scientific intelligence analysts » et *Technical intelligence*, site Web de la DIO. Les fonctions de la DIO ne sont pas définies dans la législation.

11. Royal Commission on Intelligence and Security, *Report*, Canberra, Australian Government Printing Service, 1977 (à noter qu'il y a plusieurs volumes); Royal Commission on Australia's Security and Intelligence Agencies, *General report*, Canberra, Australian Government Printing Service, décembre 1984 (cette commission royale a aussi présenté plusieurs rapports sur des organismes et des enjeux particuliers); Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service: public edition* (Samuels Inquiry), Commonwealth d'Australie, 1995; P. Flood, *Report of the Inquiry into Australian intelligence Agencies* (Flood Review), Commonwealth d'Australie, 2004.

12. Selon le Flood Review de 2004, en plus des mécanismes d'examen permanents, on devrait faire tous les cinq à sept ans un examen externe périodique de l'AIC. Flood Review, p. 63; R. Cornall et R. Black, *2011 Independent Review of the Intelligence Community report*, Commonwealth d'Australie, 2011; PM&C, *2017 Independent Intelligence Review*.

13. *ASIO Act*, section 4 de la partie 4; ASIO, *ASIO's security assessment function*, note d'information, site Web de l'ASIO.

Les budgets de l'ASIO, de l'ASIS et de l'ONA sont publiés annuellement dans des états budgétaires des portefeuilles, et les organismes peuvent devoir rendre des comptes dans le cadre d'audiences connexes de comités sénatoriaux (voir plus bas sous la section « Comités sénatoriaux permanents »; l'ASIO est le seul organisme qui témoigne régulièrement lors de ces audiences)[14]. Toutefois, les fonds supplémentaires consentis à l'ASIO et à l'ASIS dans le budget de 2017-2018 ne figurent pas dans les totaux inscrits dans les états budgétaires des portefeuilles, et il n'est pas clair si d'autres montants ont également été exclus[15].

L'ASIO est le seul organisme qui produit un rapport annuel accessible publiquement, qui est ensuite aussi déposé au Parlement. Une version classifiée du rapport annuel de l'ASIO est fournie au procureur général, qui doit la communiquer au chef de l'opposition[16]. Tous les organismes de l'AIC font l'objet de vérifications financières et administratives effectuées par l'Australian National Audit Office (bureau national de vérification de l'Australie)[17].

L'Independent National Security Legislation Monitor (contrôleur indépendant de la législation sur la sécurité nationale [INSLM]) ne supervise pas les organismes eux-mêmes, mais a une fonction connexe qui consiste à examiner l'application, l'efficacité et les conséquences de la législation relative au contre-terrorisme et à la sécurité nationale, y compris les pouvoirs spéciaux en matière de terrorisme de l'ASIO[18].

2. Surveillance parlementaire

a. Parliamentary Joint Committee on Intelligence and Security

Le PJCIS a été établi en 1988 et s'appelait alors Parliamentary Joint Committee on the Australian Security Intelligence Organisation[19]. L'ASIS a été amené sous la direction du comité en 2002, mettant en œuvre une recommandation de la Commission of Inquiry into the Australian Secret Intelligence Service (commission d'enquête sur l'Australian Secret Intelligence Service [Samuels Inquiry]) qui a publié un rapport en 1995[20]. L'ASD a été ajoutée en même temps[21]. Le PJCIS supervise l'ensemble des

14. Les états budgétaires des portefeuilles sont déposés au Parlement le soir où le budget fédéral est transmis. Voir Gouvernement d'Australie, *Portfolio Budget Statements*, site Web du budget de 2016-2017.

15. C. Barker, « National security overview », *Budget review 2017–18*, Research Paper Series, 2016–17, Parlement d'Australie, Bibliothèque du Parlement, mai 2017; P. Maley, « Budget 2017: ISIS threat sparks funding boost », *The Australian*, 10 mai 2017, p. 11.

16. *ASIO Act*, article 94.

17. *Auditor-General Act 1997*, article 56; *Crimes Act 1914*, article 85ZL, site Web de l'Australian National Audit Office.

18. *Independent National Security Legislation Monitor Act 2010* (*INSLM Act*), articles 3, 4 et 6; site Web de l'Independent National Security Legislation Monitor.

19. Parliamentary Joint Committee on Intelligence and Security (PJCIS), « History of the Intelligence and Security Committee », site Web du Parlement d'Australie. L'*Australian Security Intelligence Organization Amendment Act 1986* a inséré la partie VA dans l'*Australian Security Intelligence Organisation Act 1979* (elle a depuis été abrogée et remplacée par des dispositions figurant dans l'ISA 2001).

20. PJCIS, « History of the Intelligence and Security Committee »; Samuels Inquiry, chap. 5 (p. 40 à 63). Le comité mixte du Parlement sur l'ASIO, l'ASIS et la DSD a été établi par la partie 4 de l'ISA 2001.

21. La version initiale du projet de loi d'origine aurait permis l'établissement d'un comité de surveillance de l'ASIO et de l'ASIS. Le projet de loi a été modifié de manière à inclure la DSD dans le mandat du comité pour respecter une recommandation formulée par le Joint Select Committee on Intelligence and Security (comité mixte spécial de l'intelligence et de la sécurité) dans son rapport sur le projet de loi et deux autres. Parlement d'Australie, *page d'accueil de l'Intelligence Services Bill 2001,* site Web du Parlement d'Australie; Joint Select Committee on Intelligence and Security, *An advisory report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and certain parts of the Cybercrime Bill 2001*, Parlement d'Australie, août 2001.

six organismes de l'AIC depuis 2005, année où son mandat a été élargi pour inclure l'ONA, la DIO et l'AGO en réponse à une recommandation formulée dans le *Report of the Inquiry into Australian Intelligence Agencies* (rapport de l'enquête sur les organismes de renseignement de l'Australie [Flood Review]) publié en 2004[22].

b. Fonctions

Le PJCIS est établi en vertu de la partie 4 de l'*Intelligence Services Act 2001* (loi sur les services du renseignement [ISA 2001]), et des détails supplémentaires sont exposés dans l'annexe 1 de la *Loi*. L'article 29 définit ce que sont les fonctions du PJCIS, et, de façon tout aussi importante, ce qu'elles ne sont pas. En ce qui concerne la surveillance de l'AIC, les fonctions du PJCIS sont (sous réserve des restrictions énoncées plus bas) les suivantes[23] :

- examiner l'administration et les dépenses des organismes de l'AIC, y compris leurs états financiers annuels;
- examiner toute affaire liée à un organisme de l'AIC que lui renvoie un ministre responsable ou une Chambre du Parlement;
- examiner toute affaire concernant les activités de l'ASIO liées au programme de rétention des données de télécommunications qui sont exposées par l'ASIO dans un rapport annuel au sujet du programme;
- communiquer ses commentaires et ses recommandations à chaque Chambre du Parlement et au ministre responsable[24].

On empêche tout particulièrement le PJCIS d'examiner :

- les priorités liées à la collecte et à l'évaluation de renseignements des organismes de l'AIC;
- les sources d'information, toute autre forme d'aide opérationnelle ou méthode opérationnelle offerte aux organismes de l'AIC;
- les opérations particulières que l'ASIO, l'ASIS, l'AGO, la DIO ou l'ASD[25] a déjà menées, mène actuellement ou envisage de mener;
- l'information fournie par un gouvernement étranger (ou un de ses organismes) si ce dernier n'a pas consenti à sa divulgation;
- un volet des activités d'un organisme de l'AIC qui ne touche pas un Australien;

---

22. PJCIS, « History of the Intelligence and Security Committee »; Flood Review, p. 57 à 59. L'*Intelligence Services Legislation Amendment Act 2005* a modifié la partie 4 et l'annexe 1 de l'ISA 2001.

23. Le PJCIS a aussi un rôle à jouer pour ce qui est de surveiller des fonctions particulières de la police fédérale australienne, particulièrement ses fonctions de lutte contre le terrorisme (ajoutées en 2014 : *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*) et des activités liées au programme de conservation des données de télécommunications de l'Australie (depuis 2015 : *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*). ISA 2001, alinéas 29(1)baa), bab), bac) et be) et paragraphe 29(5). Ce rôle et d'autres fonctions du PJCIS prévus dans l'ISA 2001 et d'autres lois dépassent la portée du présent document. Pour obtenir un bref résumé, voir PJCIS, « Role of the Committee », site Web du Parlement d'Australie.

24. ISA 2001, paragraphe 29(1).

25. Sauf dans la très faible mesure prévue en vertu des paragraphes 29(4) et (5), c'est-à-dire « aux seules fins d'évaluer l'efficacité globale de la partie 5–1A de la *Telecommunications (Interception and Access) Act 1979* (conservation de données de télécommunications) et de formuler des recommandations sur celle-ci » [TRADUCTION].

- les règles prises au sujet de la protection des renseignements personnels des Australiens;
- le contenu ou les conclusions des évaluations ou des rapports produits par la DIO ou l'ONA, ou l'examen des sources d'information ayant servi de fondement à ces évaluations et à ces rapports;
- les activités de coordination et d'évaluation menées par l'ONA[26].

c. Pouvoirs et exécution des fonctions

Le PJCIS effectue des examens annuels de l'administration et des dépenses des organismes de l'AIC. Ces examens sont fondés sur des renseignements fournis par les organismes de l'AIC, l'IGIS et le vérificateur général dans des mémoires (dont la plupart sont classifiés) et dans le cadre d'audiences à huis clos[27]. Les rapports produits sur ces examens sont déposés devant chaque Chambre du Parlement et publiés sur le site Web du PJCIS. Ils renferment des commentaires formulés par le PJCIS sur des affaires pertinentes et, parfois, des recommandations précises à l'intention du gouvernement. Par exemple, dans son rapport 2011-2013, le PJCIS a recommandé que le gouvernement examine l'application continue du dividende de l'efficience et d'autres mesures d'économies pour les organismes de l'AIC et qu'il se penche sur les réformes nécessaires pour équiper l'AIC afin qu'elle puisse relever les défis que présentent les changements technologiques[28].

Le PJCIS n'a pas le pouvoir de lancer ses propres enquêtes sur des affaires liées aux activités d'un organisme de l'AIC. Toutefois, il peut, par résolution, demander que le ministre responsable lui renvoie une telle affaire (bien que les ministres puissent rejeter de telles demandes)[29]. Comme on l'a déjà souligné, les affaires peuvent aussi être renvoyées par une Chambre du Parlement. En pratique, la plupart des enquêtes effectuées par le PJCIS ou ses prédécesseurs relativement à des affaires liées aux activités d'un organisme de l'AIC ont été lancées à la suite d'un renvoi du ministre, et presque toutes ont porté sur des réformes possibles ou proposées de la législation[30]. Dans les deux cas, une exception notable a été le renvoi au comité mixte du Parlement sur l'ASIO, l'ASIS et la DSD d'une enquête sur le renseignement concernant les armes de destruction massive de l'Iraq. Cette enquête, renvoyée par le Sénat en juin 2003, est une d'à peine trois enquêtes ayant été renvoyées par une Chambre du Parlement au PJCIS ou à un comité qui l'a précédé[31]. Il semble n'y avoir que deux cas où

---

26. ISA 2001, paragraphe 29(3). Les fonctions du PJCIS ne comprennent pas non plus le traitement de plaintes individuelles au sujet des organismes de l'AIC [alinéa 29(3)g)].

27. De façon générale, le mémoire de l'IGIS n'est pas classifié, et l'ASIO et l'ONA fournissent des mémoires non classifiés ou des résumés non classifiés de mémoires classifiés. Les rapports du PJCIS comprennent des annexes où sont énumérés les mémoires et leur classification. On peut accéder aux mémoires et aux résumés non classifiés à partir des pages d'accueil des diverses enquêtes. PJCIS, « Completed inquiries and reports », site Web du Parlement d'Australie.

28. PJCIS, *Review of administration and expenditure: no. 11 and no. 12–Australian intelligence agencies*, Parlement d'Australie, septembre 2014, p. 10 et 61. Le dividende de l'efficience est une réduction annuelle du financement qui s'applique au budget opérationnel des ministères et organismes du gouvernement australien. Certains organismes en sont exemptés. N. Horne, *The Commonwealth efficiency dividend: an overview*, Background Note, Parlement d'Australie, Bibliothèque du Parlement , 13 décembre 2012.

29. ISA 2001, alinéa 29(1)b) et paragraphe 29(2).

30. Des détails des enquêtes effectuées par le PJCIS et les comités qui l'ont précédé sont accessibles à partir de PJCIS, « Completed inquiries and reports », site Web du Parlement d'Australie.

31. Australie, Sénat, « ASIO, ASIS and DSD—Joint Statutory Committee—Reference », *Journals*, 80, 18 juin 2003. Les deux autres étaient des renvois à des fins d'examen de projets de loi introduits par des motions proposées par des ministres : Australie, Chambre des représentants, « Bill—Reference to committee », *Votes and Proceedings*, 14, 21 mars 2002 (Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill); Australie, Chambre des représentants, « Bill—Reference to committee », *Votes and Proceedings*, 128, 15 octobre 2003 (Intelligence Services Amendment Bill 2003).

un ministre a renvoyé une affaire à la demande du PJCIS ou d'un comité précédent : le premier, en février 2000, sur la nature, la portée et le caractère approprié des rapports publics de l'ASIO, et le second, en mars 2015, sur l'autorisation de l'accès aux données de télécommunications afin d'identifier la source d'un journaliste[32].

L'ISA 2001 octroie des pouvoirs au PJCIS à l'appui de ses fonctions. Le PJCIS peut demander une séance d'information au responsable d'un organisme de l'AIC ou à l'IGIS[33]. Il peut aussi exiger d'une personne qu'elle se présente devant lui et fournisse un témoignage ou produise des documents s'il a des motifs raisonnables de croire que la personne est capable de fournir les renseignements ou les documents recherchés, même si ce pouvoir est soumis à certaines contraintes[34]. Le PJCIS ne peut pas utiliser ce pouvoir à l'égard de l'IGIS ou de n'importe quel employé de l'IGIS[35]. En ce qui concerne les organismes de l'AIC, le pouvoir ne peut être utilisé qu'à l'égard des responsables des organismes (même si le responsable d'un organisme peut nommer un membre du personnel[36]). Conformément aux limites de ses fonctions, le PJCIS ne peut obliger qui que ce soit à lui transmettre des renseignements opérationnels de nature délicate ou qui pourraient porter préjudice à la sécurité nationale de l'Australie ou à la conduite de ses relations étrangères[37]. Un ministre responsable d'un organisme de l'AIC peut délivrer un certificat au PJCIS pour empêcher qu'une personne divulgue des renseignements opérationnels de nature délicate lorsqu'elle est sur le point de produire un document ou qu'elle fournit, ou est sur le point de fournir, un témoignage[38].

Le PJCIS a le pouvoir de recevoir des témoignages sous serment ou une affirmation solennelle et, sous réserve des restrictions concernant les renseignements de nature délicate, de divulguer ou de publier des témoignages et le contenu de documents qu'il reçoit[39]. Il ne peut mener un examen en public qu'avec l'approbation des ministres responsables des organismes de l'AIC[40].

---

32. Parliamentary Joint Committee on ASIO (PJC on ASIO), *A watching brief: the nature, scope and appropriateness of ASIO's public reporting activities*, Parlement d'Australie, septembre 2000; PJCIS, *Inquiry into the authorisation of access to telecommunications data to identify a journalist's source*, Parlement d'Australie, 8 avril 2015. Les deux renvois ont été faits en réponse aux recommandations du comité pertinent dans les rapports précédents : PJC on ASIO, *An advisory report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999*, Parlement d'Australie, mai 1999, p. 44; PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, Parlement d'Australien, 27 février 2015, p. 258. Il est possible que d'autres références ministérielles aient découlé de suggestions ou de demandes du comité; de telles affaires peuvent ne pas toujours être explicitement mentionnées dans les rapports d'enquête.

33. ISA 2001, article 30. Cet article s'applique aussi au commissaire de la police fédérale australienne et au secrétaire du ministère de l'Immigration et de la Protection des frontières.

34. *Ibid.*, articles 2 et 3 de l'annexe 1.

35. *Ibid.*, article 2 de l'annexe 1.

36. *Ibid.*, article 3 de l'annexe 1.

37. *Ibid.*, article 1 de l'annexe 1. Les « renseignements opérationnels de nature délicate » (operationally sensitive information) sont définis dans l'article 1A de l'annexe 1.

38. *Ibid.*, article 4 de l'annexe 1. Le paragraphe 4(4) indique que la décision de délivrer un certificat empêchant ou limitant la fourniture de tels témoignages ne doit pas être remise en question par les cours ou les tribunaux.

39. *Ibid.*, articles 5, 6 et 7 de l'annexe 1.

40. *Ibid.*, article 20 de l'annexe 1.

Les rapports du PJCIS sur ses examens et ses enquêtes sont déposés au Parlement et sont accessibles au public en ligne, comme le sont les rapports annuels sur ses propres activités qu'il est tenu de produire en vertu de l'ISA 2001[41].

d. Composition et nomination

Le PJCIS doit être formé de cinq sénateurs et six membres de la Chambre des représentants. Il doit aussi être composé d'une majorité de membres du gouvernement et être présidé par un membre du gouvernement. Les membres du PJCIS sont nommés par une résolution de chaque Chambre du Parlement, après la nomination par le premier ministre (pour la Chambre des représentants) et par le leader du gouvernement au Sénat (pour le Sénat). Les mises en candidature doivent se faire après des consultations avec chaque parti non gouvernemental reconnu représenté dans chaque Chambre du Parlement relativement à l'intérêt de s'assurer que la composition du comité reflète la représentation des partis politiques reconnus au Parlement. Les ministres, le Président du Sénat et le Président de la Chambre des représentants ne peuvent pas être nommés au PJCIS. Le PJCIS est rétabli après le début de chaque nouvelle législature, et les nominations s'appliquent généralement pour la durée de la législature[42].

De façon générale, le PJCIS et ses prédécesseurs étaient composés de six membres du gouvernement et de cinq membres de l'opposition, mais ils ne comprenaient pas de membres d'autre allégeance[43]. Cela a attiré la critique des parlementaires d'autre allégeance[44].

e. Ressources

Le PJCIS est appuyé par un secrétariat fourni par le ministère de la Chambre des représentants, lequel emploie deux personnes qui se consacrent à la recherche. Le personnel de recherche est responsable d'un secrétaire du comité et est soutenu par un membre du personnel administratif; tous deux œuvrent dans le PJCIS et un autre comité. Des membres supplémentaires du personnel de recherche sont affectés dans l'ensemble des comités soutenus par le ministère de la Chambre des représentants, selon les besoins de ces comités à tout moment donné. En vertu d'une entente permanente conclue avec le gouvernement en 2015, le PJCIS soutient aussi les conseillers techniques de son secrétariat envoyés par le ministère du Procureur général et d'autres organismes, y compris l'ASIO. En vertu de l'ISA 2001, tous les employés qui soutiennent le PJCIS doivent faire l'objet d'une enquête de sécurité de même niveau (le plus élevé) et selon la même fréquence que le personnel de l'ASIS[45].

---

41. PJCIS, « Completed inquiries and reports ». Les rapports annuels des activités du PJCIS sont exigés en vertu de l'article 31 de l'ISA 2001. Il y a des restrictions quant à la divulgation de certains renseignements au Parlement : ISA 2001, article 7 de l'annexe 1.

42. ISA 2001, article 28 et articles 14 à 16A de l'annexe 1.

43. Le député indépendant Andrew Wilkie est une exception notable. Parlement d'Australie, « Mr. Andrew Wilkie MP », site Web du Parlement d'Australie. Il a fait partie du PJCIS au cours de la 43e législature (2010-2013), période durant laquelle le Parti travailliste a pu compter sur le soutien des députés indépendants Andrew Wilkie, Tony Windsor et Rob Oakeshott, et sur celui du Parti vert d'Australie, pour former un gouvernement minoritaire.

44. Voir, par exemple, N. McKim, « Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 », Sénat, *Debates*, 13 octobre 2016, p. 1722 à 1726; N. Xenophon, « Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 », Sénat, *Debates*, 13 octobre 2016, p. 1729 à 1732.

45. Secrétariat du PJCIS, communication personnelle, 8 mars 2017; I. C. Harris (dir.), *House of Representatives practice*, 5e édition, Canberra, Department of the House of Representatives, 2005, p. 642 et 643; ISA 2001, article 21.

f. Comités sénatoriaux permanents : prévisions budgétaires du Sénat

Le comité législatif de chaque comité sénatorial permanent examine les prévisions budgétaires des dépenses proposées et des dépenses supplémentaires pour les ministères de la fonction publique et d'autres organismes du Commonwealth, généralement trois fois par an. Les comités tiennent des audiences publiques lors desquelles ils ont l'occasion d'interroger les ministres (ou leurs représentants au Sénat) et les représentants gouvernementaux au sujet de l'administration du gouvernement[46].

Ces audiences procurent un moyen supplémentaire d'imposer la responsabilité financière, même si, en pratique, la mesure dans laquelle les organismes de l'AIC sont soumis à un examen minutieux dans le cadre du processus des prévisions budgétaires du Sénat est variable. L'ASIO est le seul organisme de l'AIC qui témoigne de façon régulière, et à part entière, lors des audiences sur les prévisions budgétaires du Sénat[47]. Les questions liées aux autres organismes de l'AIC ont tendance à être adressées aux ministères qui dirigent le portefeuille[48]. L'IGIS témoigne aussi durant les prévisions budgétaires du Sénat[49].

3. Inspector-General of Intelligence and Security

Le bureau de l'IGIS a été recommandé par la Royal Commission on Australia's Security and Intelligence Agencies (commission royale sur les organismes de sécurité et de renseignement de l'Australie) en 1984[50]. Le commissaire a jugé qu'il serait intéressant d'avoir un organe de surveillance indépendant, pour procurer au public une meilleure assurance que les activités des organismes de l'ACI sont appropriées et pour disculper les organismes ou les obliger à rendre des comptes, selon le cas, si des allégations de conduite inappropriée sont faites[51]. L'IGIS a été établi par l'*Inspector-General of Intelligence and Security Act 1986* (la loi sur l'inspecteur général du renseignement et de la sécurité [*IGIS Act*]) et a commencé ses activités en février 1987[52].

L'IGIS est un titulaire de charge publique indépendant nommé par le gouverneur général. De façon générale, le rôle de l'IGIS est « de s'assurer que les organismes agissent de façon légale et appropriée, se conforment aux lignes directrices et directives ministérielles et respectent les droits de la personne[53] ».

---

46. Australie, Sénat, *Consideration of estimates by the Senate's Legislation Committees*, Senate Brief, 5, Parlement d'Australie, s.d.; Australie, Sénat, *Standing orders*, Chapter 5: Standing and select committees (voir en particulier les règlements 25 et 26), Parlement d'Australie, s.d.

47. L'ASIO comparaît devant le Senate Legal and Constitutional Affairs Legislation Committee, qui englobe les portefeuilles du procureur général et de l'Immigration et de la Protection des frontières.

48. Les comités pertinents sont le Senate Foreign Affairs, Defence and Trade Legislation Committee et le Senate Finance and Public Administration Legislation Committee.

49. L'IGIS comparaît devant le Senate Finance and Public Administration Legislation Committee.

50. Royal Commission on Australia's Security and Intelligence Agencies, *General report*, p. 23 à 25.

51. *Ibid.*

52. *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*); IGIS, *Annual report 1986–87*, 1987.

53. IGIS, « About IGIS », site Web de l'IGIS [TRADUCTION]. La description résume les objets de l'*IGIS Act* (article 4) et des aspects des fonctions d'enquête de l'IGIS en vertu de l'article 8.

a. Fonctions

L'IGIS a plusieurs fonctions principales : des fonctions d'enquête sur les organismes de l'AIC, des fonctions d'enquête sur les affaires liées au renseignement et à la sécurité, des fonctions d'inspection des organismes de l'AIC et des fonctions de divulgation dans l'intérêt du public[54].

Les fonctions d'enquête sur les six organismes de l'AIC de l'IGIS varient quelque peu selon les organismes de l'AIC et sont les plus vastes par rapport à l'ASIO[55]. L'IGIS peut faire enquête sur le respect, par les organismes de l'AIC, des lois australiennes et de toute ligne directrice ou directive donnée par le ministre responsable; le bien-fondé des activités des organismes; tout acte ou toute pratique d'un organisme qui peut être incompatible avec le droit en matière des droits de la personne ou contraire à ce droit; et les procédures des organismes liées à la réparation de griefs de leurs employés[56]. Le fait qu'une enquête puisse ou non être lancée à la demande du ministre responsable, de la propre initiative de l'IGIS et/ou en réaction à une plainte diffère quelque peu selon les affaires et les organismes. Dans la plupart des cas, l'IGIS peut entreprendre une enquête au moins à la demande du ministre responsable ou de la propre initiative de l'IGIS[57]. L'IGIS a besoin de l'approbation ministérielle pour enquêter sur une affaire liée à un organisme du Commonwealth qui s'est produite à l'extérieur de l'Australie ou avant l'entrée en vigueur de l'*IGIS Act*[58].

Le premier ministre peut demander que l'IGIS fasse enquête sur une affaire liée à un organisme de l'AIC ou sur une affaire liée au renseignement ou à la sécurité concernant n'importe quel organisme du Commonwealth, et l'IGIS doit généralement répondre à une telle demande[59]. L'IGIS ne peut pas, de sa propre initiative, faire enquête sur une affaire liée au renseignement ou à la sécurité concernant un organisme qui ne fait pas partie de l'AIC.

L'IGIS peut effectuer des inspections des dossiers des organismes de l'AIC qu'il estime indiquées, pour s'assurer que les organismes agissent légalement, de façon appropriée et conformément aux droits de la personne[60]. L'IGIS indique que ses inspections lui permettent de « cerner les questions ou les préoccupations avant qu'elles deviennent des problèmes systémiques qui pourraient nécessiter la prise

54. *IGIS Act*, article 8 et paragraphes 9(1) et (2) (enquêtes relatives aux organismes de renseignement), paragraphes 9(3) et (4) (enquêtes relatives aux questions liées au renseignement et à la sécurité), article 9A (inspections) et article 8A (divulgations dans l'intérêt du public).

55. Ces différences reflètent les différences au chapitre des fonctions dans l'ensemble de l'AIC, particulièrement entre la collecte et l'évaluation de renseignements, et l'aspect étranger ou national.

56. *IGIS Act*, article 8. Pour l'ASIO, l'IGIS a aussi, en vertu de cet article, des fonctions d'enquête liées à l'efficacité et au caractère approprié des procédures que l'ASIO a en place en ce qui concerne le bien-fondé de ses activités [sous-alinéa 8(1)a)(iv)], à certaines questions liées à la fonction d'évaluation de la sécurité de l'ASIO [alinéa 8(1)c)] et à la justification de la collecte et de la communication de certains renseignements [alinéa 8(1)d)]. Il est à noter que l'article 9AA impose des restrictions sur les fonctions de l'IGIS, y compris par rapport à des affaires qui se sont produites à l'extérieur de l'Australie.

57. *Ibid.* Une enquête menée en vertu de l'alinéa 8(1)c) (liée à une évaluation de sécurité) ne peut être entreprise qu'à la demande du ministre.

58. *Ibid.*, paragraphe 9AA(a). Les paragraphes 9AA(b) et (c) interdisent à l'IGIS de faire enquête sur des mesures prises par un ministre et sur des affaires qui font ou pourraient faire l'objet d'un examen par la Security Division of the Administrative Appeals Tribunal, sauf dans des circonstances très limitées.

59. *Ibid.*, article 9.

60. *Ibid.*, articles 4 (objets de la *Loi*) et 9A (inspections).

de mesures correctives majeures[61] ». Parmi les activités d'inspection de l'IGIS, on compte l'examen des dossiers liés à l'utilisation par l'ASIO de pouvoirs spéciaux, y compris de documents connexes accompagnant des demandes de mandat; l'examen d'autorisations ministérielles délivrées à l'ASIS, à l'AGO et à l'ASD; l'examen de dossiers opérationnels de l'ASIS et de son application des lignes directrices relatives aux armes; et la surveillance du respect de la législation pertinente par les organismes [62].

L'IGIS est aussi responsable de surveiller la gestion par les organismes de l'AIC des questions liées à la divulgation dans l'intérêt public et de faire enquête sur de telles questions lorsqu'elles touchent des organismes de l'AIC[63].

b. Pouvoirs et exécution des fonctions

L'IGIS a des pouvoirs importants, qui se comparent généralement à ceux d'une commission royale, pour soutenir l'exécution de ses fonctions d'enquête, y compris des pouvoirs pour obtenir des renseignements et des documents, recevoir des témoignages et pénétrer dans les locaux des organismes du Commonwealth[64]. Compte tenu de la nature délicate des affaires et des activités sur lesquelles l'IGIS peut enquêter, les enquêtes doivent être menées en privé[65].

L'IGIS doit produire des rapports sur ses enquêtes et les fournir aux responsables des organismes pertinents (à moins que l'affaire ne concerne un responsable d'organisme) et aux ministres responsables[66]. Des résumés des enquêtes sont généralement inclus dans les rapports annuels de l'IGIS, et des versions non classifiées des rapports d'enquête sont parfois publiées sur le site Web de l'IGIS[67]. L'actuel et les anciens titulaires de la charge d'IGIS ont reconnu l'importance de rendre publique la plus grande partie possible du travail de l'IGIS dans le respect des contraintes de sécurité[68].

Si un responsable d'organisme est intervenu ou propose d'intervenir en réaction à des conclusions ou à des recommandations présentées dans un rapport d'enquête de l'IGIS, il ou elle doit fournir des détails sur une telle intervention à l'IGIS. Si l'IGIS juge qu'une intervention adéquate et appropriée n'a pas eu lieu dans une période raisonnable, il peut préparer un rapport sur la question à l'intention du ministre responsable ou du secrétaire du ministère de la Défense[69].

---

61. IGIS, « Frequently asked questions » (voir « How does the IGIS ensure that Australian intelligence agencies act legally and with propriety? »), site Web de l'IGIS [TRADUCTION].

62. *Ibid.* Les rapports annuels de l'IGIS détaillent les inspections effectuées chaque année. Voir, par exemple, IGIS, *Annual report 2016–17*, p. 13 à 34.

63. *IGIS Act*, article 8A; *Public Interest Disclosure Act 2013*.

64. *IGIS Act*, section 3 de la partie II.

65. *Ibid.*, paragraphe 17(1).

66. *Ibid.*, articles 21 et 22.

67. IGIS, « Annual reports » et « Public reports », site Web de l'IGIS.

68. IGIS, *Corporate plan 2016–20*, 2016, p. 4; V. Thom, « Reflections of a former Inspector-General of Intelligence and Security », *AIAL Forum*, 83, avril 2016, p. 11 à 17.

69. *IGIS Act*, article 24. L'article 24A prévoit des dispositions équivalentes pour les rapports remis au ministre responsable ou au secrétaire du ministère de la Défense.

L'IGIS a un plein accès aux renseignements et aux dossiers détenus par les organismes de l'AIC aux fins de l'exécution de ses fonctions d'inspection[70]. Le ministre responsable doit fournir à l'IGIS des copies de toute ligne directrice ou directive délivrée à l'ASIO, à l'ASIS, à l'AGO et à l'ASD dès que possible[71]. Les organismes de l'AIC doivent fournir à l'IGIS des exemplaires de rapports fournis à un ministre responsable ou au secrétaire du ministère de la Défense, à la demande de l'IGIS[72]. Les organismes de l'AIC doivent aussi aviser l'IGIS de l'autorisation et de l'utilisation de pouvoirs particuliers. Par exemple, des copies des mandats d'urgence ou des autorisations accordées par des responsables d'organisme (en remplacement d'un ministre) doivent être fournies, et l'ASIO doit aviser l'IGIS de toute utilisation de la force contre une personne durant l'exécution d'un mandat, de l'autorisation d'une opération de renseignement spéciale et d'affaires liées à ses pouvoirs spéciaux relativement au terrorisme[73].

En 2006, l'IGIS a noté que de 60 à 70 % de ses ressources étaient consacrées à des activités d'inspection proactives, et de 30 à 40 %, à des travaux d'enquête[74]. Des données plus récentes sur la distribution proportionnelle des ressources ne semblent pas avoir été rendues publiques.

c. Nomination

L'IGIS est nommé par le gouverneur général, à temps plein ou à temps partiel[75]. Le premier ministre doit consulter le chef de l'opposition avant de recommander une nomination au gouverneur général[76]. L'IGIS peut être nommé pour une période pouvant aller jusqu'à cinq ans, et son mandat ne peut pas être reconduit plus de deux fois[77]. Si une personne a été nommée au poste d'IGIS en tant que juge et qu'elle cesse d'exercer ses fonctions de juge, le gouverneur général peut mettre fin à la nomination de cette personne[78]. Autrement, le gouverneur général peut mettre fin à la nomination de l'IGIS en raison d'une inconduite ou d'une incapacité physique ou mentale[79].

70. *Ibid.*, article 9A.
71. *Ibid.*, article 32B; *ASIO Act*, article 5A et paragraphes 8(6) et 8A(6).
72. *IGIS Act*, article 32A.
73. ISA 2001, article 9B et *ASIO Act*, article 29; *ASIO Act*, articles 31A (recours à la force), 35PA (opérations spéciales de renseignement. Voir aussi l'article 35Q), et 34ZI et 34ZJ (pouvoirs spéciaux liés à des infractions de terrorisme).
74. I. Carnell et N. Bryan, « Watching the watchers: how the Inspector-General of Intelligence and Security helps safeguard the rule of law », Administrative Review Council, 2006.
75. *IGIS Act*, articles 6 et 63. L'article 6A autorise le premier ministre à nommer une personne pour agir comme IGIS quand le poste est vacant ou en cas d'absence.
76. *IGIS Act*, article 6.
77. *Ibid.*, article 26.
78. La Constitution prévoit un mécanisme pour qu'un juge soit retiré « en raison d'une inconduite ou d'une incapacité prouvée ». *Australian Constitution*, article 72 [TRADUCTION].
79. *Ibid.*, article 30.

d. Ressources

En date du 30 juin 2017, l'IGIS était soutenu par 15 employés permanents de la fonction publique (y compris un IGIS adjoint), dont quatre travaillaient à temps partiel[80]. Les dépenses prévues au budget de l'IGIS pour 2017-2018 totalisent 3,32 millions de dollars australiens[81]. Malheureusement, il n'est pas possible de déterminer la dotation et les ressources de l'IGIS en tant que pourcentage de celles des organismes de l'AIC parce que ces renseignements ne sont pas rendus publics pour les trois organismes de renseignement de défense.

Bien que les fonctions principales de l'IGIS soient demeurées les mêmes au cours des dernières années, les pouvoirs des organismes de l'AIC, plus particulièrement de l'ASIO, ont été élargis durant cette période. Donc, même si la nature du rôle de surveillance de l'IGIS n'a pas changé, l'étendue des pouvoirs qu'il surveille maintenant (et, dans l'environnement de sécurité actuel, l'utilisation accrue possible de certains pouvoirs)[82] a exercé des pressions additionnelles en matière de ressources sur l'organisme. Toutefois, l'IGIS a indiqué dans son *Annual Report 2015-16* qu'il a reçu des fonds supplémentaires dans le cadre de la série de mesures du 2014-15 Mid-Year Economic and Fiscal Outlook (perspectives économiques et financières de mi-exercice de 2014-2015) et qu'il est exempté du dividende de l'efficience depuis 2015-2016[83]. Il a aussi affirmé que cela permettait le recrutement d'employés supplémentaires « afin que le bureau puisse continuer de fournir un programme de surveillance complet et efficace[84] ».

4. Surveillance judiciaire

a. Mandats

La surveillance judiciaire de l'autorisation des pouvoirs des organismes de l'AIC ou la participation à celle-ci sont limitées. L'autorisation ministérielle est requise pour certaines activités de l'ASIS, de l'AGO et de l'ASD et, sous réserve de l'exception signalée plus bas, les mandats visant l'exercice de pouvoirs par l'ASIO sont délivrés par le procureur général[85].

---

80. IGIS, *Annual report 2016–17*, p. 53.

81. Gouvernement d'Australie, *Portfolio budget statements 2017–18: budget related paper no. 1.14: Prime Minister and Cabinet Portfolio*, Canberra, Commonwealth d'Australie, 2017, p. 255.

82. L'ASIO est le seul parmi les organismes de renseignement opérationnels qui produit un rapport public annuel, et ce rapport doit uniquement contenir des détails sur le nombre de mandats/d'autorisations concernant des pouvoirs sélectionnés (*ASIO Act*, article 94).

83. IGIS, *Annual report 2015–16*, p. v. Pour obtenir des renseignements sur les changements apportés au budget, voir C. Barker, « Countering terrorism and violent extremism », *Budget review 2015–16*, Research Paper, 2014–15, Parlement d'Australie, Bibliothèque du Parlement, mai 2015.

84. IGIS, *Annual report 2015–16*, p. v [TRADUCTION]. Bien que des ressources supplémentaires aient été fournies, l'IGIS a connu des retards au chapitre du recrutement en raison de longs processus d'habilitation de sécurité, ce qui a mené à une sous-utilisation des fonds consacrés aux salaires en 2015-2016 et en 2016-2017. *Ibid.*, p. 10; IGIS, *Annual report 2016–17*, p. 60.

85. ISA 2001, articles 9 et 9A (les articles 9B et 9C autorisent les responsables d'organisme à donner des autorisations d'urgence qui demeurent en vigueur pour une période plus courte si les ministres ne sont pas disponibles); *ASIO Act*, articles 25, 25A, 26, 27, 27AA, 27A, 27C et 35C (l'article 29 permet au responsable de l'ASIO de délivrer un mandat d'urgence pour la plupart des types de mandats qui demeure en vigueur pour une période plus courte dans certaines circonstances); *Telecommunications (Interception and Access) Act 1979*, partie 2-2 (y compris les mandats d'urgence émis par le responsable de l'ASIO en vertu de l'article 10).

L'ASIO a accès à des pouvoirs spéciaux liés à des infractions de terrorisme, en vertu desquels elle peut obtenir un mandat pour interroger une personne sans détention, pour un maximum de 24 heures (mandats pour interrogatoire), ou pour détenir une personne à des fins d'interrogatoire, pour un maximum de sept jours consécutifs (mandats pour interrogatoire et détention)[86]. Pour faire une demande d'un tel mandat, le directeur général de l'ASIO doit obtenir le consentement du procureur général, puis demander à une « autorité de délivrance » la délivrance du mandat[87]. Une autorité de délivrance est un magistrat fédéral actuel ou un juge d'un tribunal fédéral, étatique ou territorial qui a été nommé par le procureur général, même si le procureur général a la capacité de déclarer des personnes faisant partie d'une classe précise comme des autorités de délivrance, peu importe leur position ou leur expertise[88]. Une fois le mandat délivré, la personne est amenée devant une « autorité désignée » – habituellement un ancien juge de la cour de district ou de la Cour suprême d'un État ou d'un territoire – qui surveille et supervise l'exercice du pouvoir en vertu du mandat[89].

Fait important, un juge nommé en tant qu'autorité de délivrance ou qu'autorité désignée agit à titre personnel, et non judiciaire[90]. Qui plus est, le rôle joué par les deux autorités est limité. Pour délivrer un mandat, une autorité de délivrance doit seulement être convaincue qu'il y a des motifs raisonnables de croire qu'il va grandement contribuer à la collecte de renseignements importants par rapport à une infraction de terrorisme[91]. L'autorité n'a pas à se demander s'il y a d'autres méthodes efficaces de recueillir les éléments de preuve, ou, dans le cas d'un mandat pour interrogatoire et détention, si la détention est nécessaire. Ce sont des questions que le procureur général prend en considération lorsqu'il consent à la demande de mandat[92]. Un juge qui agit comme autorité désignée peut superviser et diriger le processus d'interrogation, mais ces pouvoirs sont aussi limités. Par exemple, une autorité désignée ne peut généralement pas donner à l'interrogatoire une direction qui est incompatible avec les modalités d'un mandat[93].

---

86. Pour les mandats pour interrogatoire, *ASIO Act*, articles 34D, 34E et paragraphe 34R(6). La durée maximale est prolongée, passant de 24 à 48 heures si une personne est interrogée et qu'un interprète est présent (paragraphe 34R(11)). Pour les mandats pour interrogatoire et détention, *ASIO Act*, articles 34F, 34G et 34S.

87. En date d'octobre 2016, l'ASIO n'avait jamais présenté de demande de mandat pour interrogatoire et détention. Voir R. Gyles, *Certain questioning and detention powers in relation to terrorism*, Independent National Security Legislation Monitor, octobre 2016, p. 40.

88. *ASIO Act*, paragraphe 34AB(3).

89. *ASIO Act*, article 34B. Lorsque le ou la ministre est d'avis qu'il n'y a pas un nombre suffisant de personnes pour agir comme autorité désignée, il ou elle peut nommer un juge actuellement en service, ou un président ou un vice-président de l'Administrative Appeals Tribunal (paragraphes 34B(2) et (3)).

90. *ASIO Act*, paragraphe 34ZM(2); L. Burton et G. Williams, « The integrity function and ASIO's extraordinary questioning and detention powers », *Monash University Law Review*, 38(3), 2012, p. 4; Australian Human Rights Commission (AHRC), « A human rights guide to Australia's counter-terrorism laws », site Web de l'AHRC, 2008.

91. *ASIO Act*, articles 34E et 34G.

92. Le procureur général doit être convaincu qu'il serait inefficace de s'appuyer sur d'autres méthodes de collecte de renseignements, et que la personne non détenue, dans le cas d'un mandat pour interrogatoire et détention, pourrait alerter une personne impliquée dans une infraction de terrorisme que l'infraction fait l'objet d'une enquête, ne pas se présenter aux comparutions à des fins d'interrogation, ou détruire, endommager ou modifier un dossier ou une chose (paragraphes 34D(4) et 34F(4)); L. Burton et G. Williams, « The integrity function and ASIO's extraordinary questioning and detention powers », p. 4 et 5.

93. L. Burton et G. Williams, « The integrity function and ASIO's extraordinary questioning and detention powers », p. 5.

b. Rôle des tribunaux

Les décisions prises par rapport à des mandats concernant des pouvoirs spéciaux en matière de terrorisme ne sont pas soumises à un examen du bien-fondé, et l'*ASIO Act* exclut expressément la compétence des tribunaux étatiques et territoriaux pendant que le mandat est en vigueur[94]. Les décisions prises en vertu de l'*ASIO Act*, de l'ISA 2001 et d'autres textes législatifs sur le renseignement sont aussi exclues du cadre d'examen judiciaire prévu par la loi énoncé dans l'*Administrative Decisions (Judicial Review) Act 1977*[95]. Toutefois, une personne peut présenter à la Federal Court of Australia (cour fédérale de l'Australie) ou à la High Court of Australia (cour suprême de l'Australie) une demande de contrôle judiciaire des mesures prises par les agents du Commonwealth pour s'assurer que ces mesures sont exécutées dans le respect des limites législatives et constitutionnelles[96].

Le seul tribunal spécialisé qui fournit de la surveillance par rapport à des affaires liées au renseignement est la Security Division of the Administrative Appeals Tribunal (AAT), qui effectue un examen du bien-fondé de la plupart des catégories d'évaluations négatives sur la sécurité faites par l'ASIO[97]. Les audiences dans cette division se tiennent en privé, et le procureur général peut délivrer un certificat d'intérêt public pour exiger que les renseignements de sécurité nationale de nature délicate ne soient pas divulgués au demandeur[98]. Le contrôle judiciaire du processus d'évaluation de sécurité par l'ASIO est aussi possible par l'intermédiaire de la Federal Court et de la High Court[99].

c. Immunité et poursuites

Les membres du personnel et les agents de l'ASIS, de l'ASD et de l'AGO ont l'immunité pour ce qui est de la responsabilité civile et criminelle concernant les activités menées par les organismes dans le cadre de l'exécution appropriée de leurs fonctions, qui pourraient autrement être interdites en raison des conséquences imprévues de certaines lois australiennes[100]. Cette immunité ne peut être outrepassée que par d'autres lois du Commonwealth, d'États ou de territoires, si ces lois prévoient expressément le contraire[101]. De même, les agents de l'ASIO qui participent à une opération de renseignement spéciale ne s'exposent pas à une responsabilité civile ou criminelle relativement à leur conduite durant l'opération ou aux fins de celle-ci, et conformément au pouvoir accordé dans le cadre de l'opération. Cette immunité comporte des exceptions : c'est le cas d'une conduite qui cause la mort ou des blessures graves, qui constitue de la torture ou qui suppose la perpétration d'une infraction sexuelle, ou dans le cadre de laquelle le participant incite une autre personne à commettre une infraction que l'autre personne n'aurait pas eu l'intention de commettre[102].

---

94. *ASIO Act*, article 34ZW.
95. *Administrative Decisions (Judicial Review) Act 1977* (Cth), annexe 1.
96. L'accès à la compétence originale de la Cour suprême d'Australie est prévu au paragraphe 75(v) de la *Constitution*, et à celle de la Cour fédérale d'Australie, au paragraphe 39B(1) de la *Judiciary Act 1903* (Cth). Pour obtenir plus de renseignements, voir Administrative Review Council, *The scope of judicial review—report to the Attorney-General*, rapport n° 47, avril 2006, p. 5 à 7.
97. *ASIO Act*, section 4 de la partie 4; ASIO, *ASIO's security assessment function*; G. Downes, « The Security Appeals Division of the Administrative Appeals Tribunal—functions, powers and procedures », exposé présenté au National Security Law Course, Université de Sydney, 13 septembre 2006.
98. G. Downes, « The Security Appeals Division of the Administrative Appeals Tribunal—functions, powers and procedures ».
99. ASIO, *ASIO's security assessment function*.
100. ISA 2001 (Cth), article 14.
101. *Ibid.*, paragraphe 14(2AA).
102. *ASIO Act*, article 35K. Le paragraphe 35K(2) autorise le ministre à assortir cette immunité d'autres exigences/conditions par l'instrument législatif. À ce jour, cela n'a pas été fait.

Les tribunaux australiens ont traduit en justice des agents du renseignement et d'autres personnes auxquelles on a confié des renseignements secrets parce qu'ils ont divulgué sans autorisation de tels renseignements[103].

d. Irrecevabilité de la preuve

Les tribunaux ont déjà jugé irrecevables des renseignements qu'on a cherché à faire admettre en preuve dans des poursuites criminelles, en raison de l'irrégularité constatée dans le processus d'obtention des renseignements. Un exemple est l'affaire *R v. Ul-Haque* [2007] NSWSC 1251, où la preuve d'aveux faits par le défendeur à l'ASIO et à des agents de la police fédérale australienne (AFP) dans une poursuite liée à des activités de contre-terrorisme a été exclue par la Supreme Court of New South Wales en vertu de l'article 138 de l'*Evidence Act 1995* (Cth) (qui prévoit l'exclusion de preuves obtenues de façon inappropriée ou illégale) et de l'article 84 (qui exclut comme preuve des aveux qui ont été influencés par une conduite violente, oppressive, inhumaine ou dégradante)[104]. En qualifiant la preuve d'irrecevable, le juge au procès a fortement critiqué la conduite des agents de l'ASIO dans l'affaire, jugeant qu'ils se sont arrogé des pouvoirs illégaux de direction, de contrôle et de détention[105]. Le procès a par la suite été interrompu[106].

5. Communication de renseignements et coopération entre les organismes de surveillance

Les fonctions du PJCIS et de l'IGIS se complètent plutôt que de se chevaucher, et le PJCIS n'a pas l'autorisation d'aller chercher des « renseignements opérationnels de nature délicate », ce qui signifie que les occasions de coopération entre les deux sont assez limitées. Cependant, quelques renseignements sont communiqués entre eux, principalement de l'IGIS au PJCIS.

Comme on l'a mentionné plus haut, le PJCIS peut demander la tenue de séances d'information à l'IGIS. Dans le cadre de l'examen, par le PJCIS, de l'administration et des dépenses des organismes de l'AIC, l'IGIS présente des observations et fournit un témoignage lors d'audiences. L'IGIS fournit aussi souvent un témoignage dans le cadre d'enquêtes du PJCIS sur des textes législatifs proposés ou examinés qui sont pertinents pour le rôle de surveillance de l'IGIS ou, de façon plus générale, les fonctions des organismes de l'AIC, ainsi que dans le cadre des examens menés par l'INSLM[107]. Dans son rapport annuel pour 2015-2016, l'IGIS précise que sa coopération avec l'AAT et l'Australian Information Commissioner (commissaire à l'information de l'Australie) aide à « renforcer la surveillance et à favoriser les bonnes pratiques dans les organismes de l'AIC[108] ».

---

103. Voici des exemples : *R v Scerba (No 2)* [2015] ACTSC 359, où un jeune diplômé qui travaillait au ministère de la Défense a été condamné pour avoir téléchargé un document classifié de nature délicate du Defence Secret Network et l'avoir affiché sur un site Web de partage d'images; *Sievers v R* [2010] ACTA 9, où un agent de l'ASIO a été condamné pour avoir communiqué des renseignements en sa possession qui avaient été préparés ou acquis au nom de l'ASIO au sujet de ses fonctions ou de son rendement; *R v Lappas* (2003) 152 ACTR 7, où un employé de la Defence Intelligence Organisation a été condamné pour avoir fourni des documents classifiés à une personne non autorisée pour qu'elle les vende à un pays étranger.

104. *Evidence Act 1995*; *R v Ul-Haque* [2007] NSWSC 1251.

105. *R v Ul-Haque*, à 95.

106. « Terror charges against student dropped », site Web de SBS News, 12 novembre 2007.

107. Voir, par exemple, IGIS, Submission à PJCIS, *Review of administration and expenditure no. 15 (2015–2016)*, 8 décembre 2016; IGIS, Submission à PJCIS, *Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2014*, 10 novembre 2014; IGIS, Submission à l'INSLM, *Review of certain questioning and detention powers in relation to terrorism*, juillet 2016.

108. IGIS, *Annual report 2015–16*, p. 8 [TRADUCTION].

L'INSLM peut consulter l'IGIS lorsqu'il exécute des fonctions en vertu de la législation sur le contre-terrorisme et la sécurité nationale de l'Australie[109]. Le PJCIS peut renvoyer à l'INSLM une affaire dont il prend connaissance durant l'exécution de ses fonctions[110].

C. Faits nouveaux et réformes proposées

1. Compétence du PJCIS

Les fonctions du PJCIS ont été graduellement élargies au cours des dernières années, en réaction à ses propres recommandations[111]. Toutefois, ces changements sont en grande partie liés à des fonctions autres que la surveillance des organismes de l'AIC. Plus précisément, ses fonctions d'examen législatif ont été élargies et une nouvelle fonction a été incluse, soit la surveillance et l'examen des fonctions de lutte contre le terrorisme de la police fédérale australienne[112].

2. Projet de loi modifiant le PJCIS

La sénatrice de l'opposition Penny Wong a présenté le Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 (projet de loi modifiant le comité mixte du Parlement sur le renseignement et la sécurité de 2015) le 10 août 2015. Le projet de loi est devenu caduc avant l'élection fédérale de 2016, mais il a été rétabli dans le *Feuilleton des avis* le 31 août 2016[113]. Il modifierait la composition, les fonctions et les pouvoirs du PJCIS.

Le projet de loi permettrait au PJCIS de mener de sa propre initiative des enquêtes sur des affaires liées à au moins un des organismes de l'AIC, pourvu qu'il ait d'abord consulté le ministre responsable. Il n'aurait pas d'incidence sur les restrictions existantes empêchant le PJCIS d'enquêter sur des affaires opérationnelles.

Comme on l'a signalé plus haut, le PJCIS doit actuellement comprendre cinq sénateurs et six membres de la Chambre des représentants, avoir une majorité de membres du gouvernement et un président du gouvernement. Le projet de loi conserverait l'exigence d'une majorité du gouvernement, mais il assouplirait le ratio Sénat/Chambre des représentants, de sorte qu'il y aurait un sénateur et un député de la Chambre des représentants du gouvernement et de l'opposition, et les membres restants pourraient être choisis dans l'une ou l'autre des Chambres du Parlement. Cette modification proposée a pour but de fournir plus de souplesse afin qu'on s'assure que le PJCIS est composé des membres les plus qualifiés. Toutefois, le projet de loi n'exigerait pas de membres d'autre allégeance. Le sénateur australien du Parti vert Nick McKim a affirmé, à l'étape du débat en deuxième lecture, que le Parti vert proposerait un amendement selon lequel un sénateur qui ne fait pas partie du gouvernement ni de l'opposition serait un des 11 membres du PJCIS[114].

---

109. *INSLM Act*, paragraphe 10(2).

110. *Ibid.*, article 7A.

111. Voir les rapports consultatifs du PJCIS sur le *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, le *Australian Citizenship Amendment (Allegiance to Australia) Bill 2015*, le *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* et le *Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016*.

112. Ces changements apparaissent dans l'ISA 2001, aux alinéas 29(1)baa), bab), bac) et be) (fonction de l'AFP); et 29(1)bc) et ca) (examens législatifs); *Criminal Code Act 1995*, paragraphe 119.3(7) (examen des domaines déclarés par le ministre des Affaires étrangères); *Australian Citizenship Act 2007*, article 35AA (déclaration d'une organisation terroriste aux fins de la *Loi*).

113. Parlement d'Australie, page d'accueil du *Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015*, site Web du Parlement d'Australie. Le projet de loi s'inspire de travaux menés par l'ancien sénateur John Faulkner. Voir J. Faulkner, *Surveillance, intelligence and accountability: an Australian story*, 23 octobre 2014.

114. N. McKim, « Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 ».

Parmi d'autres modifications, le projet de loi obligerait aussi l'IGIS à fournir au PJCIS des exemplaires de ses rapports d'enquête dans les trois mois suivant leur transmission au premier ministre ou au ministre responsable, et exigerait l'ajout de l'INSLM et du National Security Adviser (conseiller à la sécurité nationale, au ministère du Premier ministre et du Cabinet) à la liste des titulaires de charge à qui le PJCIS peut demander une séance d'information.

3. Examen indépendant du renseignement en 2017

Le plus récent examen indépendant des organismes de l'AIC a été effectué en juin 2017, et une version publique du rapport est parue en juillet 2017[115]. Le rapport recommandait plusieurs changements concernant la surveillance des organismes de renseignement de l'Australie.

Selon les examinateurs, l'entreprise de renseignement qui soutient la sécurité nationale de l'Australie ne se limite plus aux six organismes de l'AIC et un cadre de référence plus approprié serait une communauté nationale du renseignement composée des six organismes de l'AIC, de l'Australian Criminal Intelligence Commission (commission australienne du renseignement criminel [ACIC]), de l'Australian Transaction Reports and Analysis Centre (centre de rapport et d'analyse sur les transactions de l'Australie [AUSTRAC]) et de parties de la police fédérale australienne et du ministère de l'Immigration et de la Protection des frontières (DIBP)[116]. Par conséquent, ils ont recommandé que la compétence du PJCIS et de l'IGIS soit élargie afin d'inclure l'AUSTRAC dans son intégralité ainsi que les fonctions de renseignement de la police fédérale australienne, de l'ACIC et du DIBP[117].

Les examinateurs ont aussi recommandé ce qui suit :

- qu'on fournisse au PJCIS la capacité de demander que l'IGIS fasse enquête sur la légalité et le bien-fondé d'activités opérationnelles particulières de n'importe lequel des 10 organismes mentionnés plus haut et produise un rapport à l'intention du PJCIS, du premier ministre et du ministre responsable (correspondant aux pouvoirs de l'Intelligence and Security Committee [comité du renseignement et de la sécurité] de la Nouvelle-Zélande);
- qu'on fournisse au PJCIS la capacité de lancer ses propres enquêtes relativement à l'administration et aux dépenses des 10 organismes mentionnés plus haut;
- qu'on habilite le PJCIS afin qu'il puisse demander des séances d'information à l'INSLM et lui renvoyer des affaires à des fins de rapports;
- que l'IGIS et le directeur général de l'Office of National Intelligence (bureau de renseignement national) proposé soient tenus de communiquer régulièrement des informations au PJCIS;
- qu'on augmente de façon importante les ressources de l'IGIS, les faisant passer de 17 à environ 50 employés à temps plein[118].

---

115. PM&C, *2017 Independent Intelligence Review*; M. Turnbull (premier ministre), *Press Conference with the Attorney-General, Senator the Hon. George Brandis QC, Minister for Immigration and Border Protection, The Hon. Peter Dutton MP and Minister for Justice, The Hon. Michael Keenan MP Parliament House, Canberra* (*Press Conference*), communiqué, 18 juillet 2017.

116. PM&C, *2017 Independent Intelligence Review*, p. 46 à 48, 115.

117. *Ibid.*, p. 116.

118. *Ibid.*, p. 111 à 125. Les examinateurs ont aussi recommandé qu'on apporte des changements à l'architecture des mécanismes de renseignement de l'Australie (y compris l'élargissement de l'ONA pour en faire un Office of National Intelligence [bureau de renseignement national] et la transformation de l'ASD en organisme statutaire distinct relevant du ministre de la Défense), ainsi qu'à leur capacité et à leur financement, et à la législation qui régit les organismes.

Bien qu'il ne s'agisse pas d'une recommandation figurant dans le rapport, le jour de la publication du rapport, le premier ministre a aussi annoncé la création d'un nouveau portefeuille des affaires intérieures (qui s'inspire de façon générale du Home Office du Royaume-Uni) qui va permettre de rassembler les organismes chargés de l'immigration, de la protection des frontières, de l'application de la loi et de la sécurité nationale en Australie dans un seul portefeuille[119].

Un groupe de travail dirigé par le ministère du Premier ministre et du Cabinet va examiner les recommandations issues de l'examen indépendant, puis gérer en tandem la mise en œuvre de celles qui sont adoptées et l'établissement du portefeuille des affaires intérieures[120].

119. M. Turnbull (premier ministre), *Press Conference*; M. Turnbull (premier ministre), G. Brandis (procureur général), P. Dutton (ministre de l'Immigration et de la Protection des frontières) et M. Keenan (ministre de la Justice), *A strong and secure Australia*, communiqué, 18 juillet 2017. Par rapport au portefeuille des affaires intérieures, voir aussi C. Barker et S. Fallon, *What we know so far about the new Home Affairs portfolio: a quick guide*, Research Paper Series, 2017–18, Parlement d'Australie, Bibliothèque du Parlement, 2017.

120. *Ibid.*

CANADA

A. Aperçu des organismes de renseignement

Les activités et les structures du gouvernement du Canada liées au renseignement font intervenir de nombreuses organisations. On en trouve une liste partielle à deux endroits :

- L'annexe 3 de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* comporte une liste de 17 institutions fédérales qui recueillent, analysent et diffusent de l'information dans le but de protéger le Canada contre les activités qui menacent sa sécurité;
- La stratégie antiterroriste nationale du Canada, adoptée en 2013, indique les 21 ministères et organismes ayant des responsabilités en matière d'antiterrorisme[121].

Puisque les renseignements sont créés et utilisés à des fins autres que la sécurité nationale, il est probable que ces deux listes ne brossent pas le tableau complet de la communauté de la sécurité et du renseignement du Canada.

Les principaux organismes de collecte de renseignement de sécurité du Canada sont les suivants[122] :

- Le Centre de la sécurité des télécommunications (CST) est l'organisme canadien qui recueille des renseignements électromagnétiques étrangers. Le CST compte quelque 2 000 employés[123]. Le CST est un organisme indépendant qui relève du ministère de la Défense nationale (MDN)[124] et, conformément au paragraphe 273.64(1) de la *Loi sur la défense nationale*, son mandat est le suivant :
  - acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers;
  - fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
  - fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

  Pour se protéger de toute responsabilité prévue dans la partie VI du *Code criminel*, interdisant l'interception non autorisée de communications privées, le CST demande au ministre de la Défense nationale l'autorisation de mener des activités de collecte de renseignements étrangers et de cyberdéfense en cas de risque inévitable d'une telle interception. Les autorisations ministérielles ne sont valides que pendant un an et sont assorties de certaines conditions que le CST doit respecter.

---

121 Voir Sécurité publique Canada, « Annexe A : Rôles et responsabilités en matière d'antiterrorisme », *Renforcer la résilience face au terrorisme : Stratégie antiterroriste du Canada*, 2013.

122 Nous n'avons pas inclus dans cette liste le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), qui, même s'il est un organisme de renseignement financier, n'a pas la capacité ni les pouvoirs de chercher activement et de recueillir des données. En vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* du Canada, les institutions financières et les autres secteurs concernés sont obligés de lui communiquer des données.

123 Il s'agit de l'effectif moyen. Voir Gouvernement du Canada, *Répertoire des organisations et intérêts fédéraux*. Pour trouver les données sur la « Gestion des personnes » du CST, il faut d'abord trouver la rubrique « Défense nationale » et cliquer sur « Centre de la sécurité des télécommunications ».

124 Avant le décret en conseil pris en décembre 2011 qui en faisait un organisme indépendant, le CST relevait du ministre de la Défense nationale, par le truchement du sous-ministre de la Défense nationale, pour les questions de nature financière et administrative, et du conseiller national en matière de sécurité pour les questions de nature opérationnelle et stratégique. Le CST relève aujourd'hui directement du ministre de la Défense nationale.

- Le Service canadien du renseignement de sécurité (SCRS) fournit des renseignements sur les menaces à la sécurité du Canada en utilisant surtout, mais pas exclusivement, des sources humaines. Il s'appuie sur un effectif de plus de 3 200 personnes[125] et fait partie du portefeuille de Sécurité publique Canada (SPC)[126]. Son mandat lui est conféré par l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*). S'il doit utiliser des techniques d'enquête intrusives, le SCRS est tenu, en application de l'article 21 de la *Loi sur le SCRS*, d'obtenir un mandat de la Cour fédérale, laquelle a chargé un groupe de juges d'examiner ces demandes du SCRS dans le cadre d'audiences *ex parte* (d'une seule partie) ou *in camera* (à huis clos). En 2015, la *Loi sur le SCRS* a été modifiée par deux projets de loi distincts[127] visant, entre autres, à donner à la Cour fédérale le pouvoir d'émettre des mandats permettant au SCRS d'utiliser des mesures intrusives dans ses activités à l'étranger et l'autorisant à mener des activités de réduction des menaces.
- Le Commandement du renseignement des Forces canadiennes (COMRENSFC) utilise une gamme complète de méthodes de collecte pour fournir des renseignements de défense aux Forces armées canadiennes et au MDN. Le COMRENSFC reçoit ses ordres du chef du renseignement de la Défense, qui tient ses pouvoirs de la *Loi sur la défense nationale*. La plus grande partie, mais pas la totalité, des renseignements recueillis par le COMRENSFC sont étrangers, et c'est pourquoi la plupart de ses activités de collecte et de communication d'information se font en vertu de la prérogative de la Couronne[128]. Toutefois, les activités de contre-ingérence du COMRENSFC peuvent exiger la collecte de renseignements sur des Canadiens. Pour le moment, le MDN s'appuie sur les mécanismes de responsabilisation internes mis en place pour s'assurer que les activités de contre-ingérence du Commandement sont menées de manière légale et en conformité avec les politiques et règlements du Ministère. Toutefois, il se peut que certains éléments de responsabilisation externe soient mis en place en application de mesures législatives, dont il sera question plus loin.
- La Gendarmerie royale du Canada (GRC), en tant qu'organisme fédéral d'application de la loi, est chargée, en vertu de la *Loi sur les infractions en matière de sécurité*, de mener des enquêtes criminelles sur les infractions en matière de sécurité nationale, par exemple la facilitation ou l'exécution d'actes de terrorisme ou d'espionnage. La GRC – qui peut aussi sur demande fournir des services de police dans l'ensemble des provinces et des territoires du Canada, à l'exception de l'Ontario et du Québec – tient son mandat de la *Loi sur la Gendarmerie royale du Canada* (*Loi sur la GRC*). Son effectif est d'environ 6 500 personnes[129].

---

125 Voir Service canadien du renseignement de sécurité, « Un milieu de travail unique en son genre », *Rapport public 2014-2016*.

126 Sécurité publique Canada comprend l'Agence des services frontaliers du Canada, la Gendarmerie royale du Canada, le Service canadien du renseignement de sécurité, Service correctionnel Canada et la Commission des libérations conditionnelles du Canada.

127 Le projet de loi C-44, Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et d'autres lois, a reçu la sanction royale le 23 avril 2015, et le projet de loi C-51, Loi édictant la Loi sur la communication d'information ayant trait à la sécurité du Canada et la Loi sur la sûreté des déplacements aériens, modifiant le Code criminel, la Loi sur le Service canadien du renseignement de sécurité et la Loi sur l'immigration et la protection des réfugiés et apportant des modifications connexes et corrélatives à d'autres lois, a reçu la sanction royale le 18 juin 2015. Voir Holly Porteous, Dominique Valiquet et Julie Béchard, *Résumé législatif du projet de loi C-44 : Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et d'autres lois*, publication n° 41-2-C44-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 28 novembre 2014. Voir aussi Julie Béchard, Tanya Dupuis, Christine Morris, Dominique Valiquet et Holly Porteous, *Résumé législatif du projet de loi C-51 : Loi édictant la Loi sur la communication d'information ayant trait à la sécurité du Canada et la Loi sur la sûreté des déplacements aériens, modifiant le Code criminel, la Loi sur le Service canadien du renseignement de sécurité et la Loi sur l'immigration et la protection des réfugiés et apportant des modifications connexes et corrélatives à d'autres lois*, publication n° 41-2-C51-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 19 juin 2015.

128 Ministère de la Défense nationale, « Résumé », *Examen du renseignement de défense : Rapport présenté au CEMD*, Ottawa, 20 mai 2004, p. iv. Document obtenu en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* (demande n° A0280236).

129 Gouvernement du Canada, *Répertoire des organisations et intérêts fédéraux*. Pour accéder aux données sur la « Gestion des personnes » de la GRC, il faut aller à la rubrique « Sécurité publique et Protection civile » et cliquer sur « Gendarmerie royale du Canada ».

B. Surveillance : résumé

Même si les ministres de la Sécurité publique et de la Défense nationale sont responsables des activités menées par les organismes de leurs portefeuilles respectifs, c'est au bout du compte le premier ministre qui doit rendre compte au Parlement des questions touchant la sécurité nationale. C'est pourquoi le premier ministre est président du Comité du Cabinet chargé du renseignement et de la gestion des urgences[130].

Le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNRPM)[131] est à la fois les yeux et les oreilles du premier ministre pour tout ce qui concerne la sécurité et le renseignement. Le CSNRPM assure également la coordination de la communauté fédérale de la sécurité et du renseignement, mais il n'a pour tout outil que sa capacité de persuasion, puisqu'il est titulaire d'un rôle sans pouvoirs légaux. Avec le CSNRPM adjoint, le CSNRPM supervise les activités du Secrétariat de l'évaluation du renseignement et du Secrétariat de la sécurité et du renseignement du Bureau du Conseil privé[132].

À l'heure actuelle, le pouvoir exécutif s'appuie sur trois organismes d'experts lorsqu'il faut mener des enquêtes sur des plaintes ou examiner la légitimité des activités des organismes chargés du renseignement et de la sécurité nationale du Canada (une analyse plus détaillée suit) :

- le Comité de surveillance des activités de renseignement de sécurité (CSARS);
- le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST);
- la Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP).

---

130 Le ministre de la Sécurité publique et de la Protection civile préside un autre comité important du Cabinet, le Comité du Cabinet chargé du Canada dans le monde et de la sécurité publique, responsable de questions relatives à la sécurité nationale et internationale.

131 Le titre du conseiller à la sécurité nationale auprès du premier ministre a été changé le 28 avril 2017; le conseiller est maintenant le conseiller à la sécurité nationale *et au renseignement* auprès du premier ministre [SOULIGNÉ PAR L'AUTEUR]. Voir Bureau du Conseil privé, *Numéro C.P. : 2017-0411*, 28 avril 2017.

132 Le Bureau du Conseil privé est un organisme de la fonction publique. Il appuie le premier ministre ainsi que le Cabinet et ses structures décisionnelles de façon impartiale.

Chacun de ces organismes a été établi par la loi. Ils se disent tous indépendants, mais la loi les oblige tous les trois à présenter un rapport annuel au ministre dont ils relèvent[133], et ils doivent tous respecter les directives ou les contraintes du pouvoir exécutif[134]. Après avoir reçu des versions non classifiées de ces rapports, les ministres doivent les présenter à chacune des Chambres du Parlement dans les 15 premiers jours de séance qui suivent.

Aucun des organismes chargés du renseignement et de la sécurité nationale n'a à présenter un rapport annuel au Parlement. Le SCRS prépare néanmoins des rapports publics. Toutefois, ces rapports ne sont pas présentés à date fixe, et le plus récent rapport de l'organisme concerne une période de deux ans. Au fil du temps, ces rapports sont devenus de plus en plus minces, et ils traitent souvent de généralités.

La principale obligation de rapport au Parlement, pour les ministères et organismes fédéraux, a trait aux documents budgétaires[135]. C'est au moyen du processus budgétaire que les organismes fédéraux demandent au Parlement l'approbation de dépenser des fonds; ils exposent leurs besoins en financement dans le Budget principal des dépenses et le Budget supplémentaire des dépenses. Les ministères et organismes préparent en outre des plans organisationnels où ils fournissent aux parlementaires de plus amples informations sur les objectifs qu'ils espèrent atteindre avec les ressources qui leur seront fournies. À la fin de l'exercice, ils expliquent dans des rapports sur le rendement ministériel comment l'argent a été dépensé et les objectifs qu'ils ont atteints.

Cependant, ni le SCRS ni le CST ne préparent de plans organisationnels ou de rapports sur le rendement. Les parlementaires reçoivent toutefois une information financière générale dans le cadre des budgets principal et supplémentaire des dépenses. Ainsi, exception faite des réponses qu'ils peuvent obtenir en questionnant les responsables pendant les audiences publiques des comités, les

---

133 Le commissaire du CST relève du ministre de la Défense nationale, tandis que les présidents du CSARS et de la CCETP relèvent du ministre de la Sécurité publique et de la Protection civile. Puisque l'ensemble des provinces et territoires du Canada, à l'exception de l'Ontario et du Québec, utilisent à contrat les services de police de la GRC, le président de la CCETP doit de plus présenter un rapport annuel aux ministres provinciaux qui sont les principaux responsables des services de police et qui ont conclu ces marchés. Chaque rapport annuel, dont un exemplaire est envoyé au ministre de la Sécurité publique et de la Protection civile, et un autre au commissaire de la GRC, présente un exposé du nombre et de la nature des plaintes relatives à la conduite de membres de la GRC pour chaque province, décrit la façon dont ces plaintes ont été traitées et signale les tendances.

134 Par exemple, soutenant que les lois en vigueur permettaient à son organisme de collaborer avec le CSARS, le commissaire du CST notait ceci dans son rapport annuel 2011-2012 :

> Le paragraphe 273.63(6) de la *Loi sur la défense nationale* permet au gouverneur en conseil de m'autoriser à me « livrer à toute activité connexe ». L'article 54 de la *Loi sur le Service canadien du renseignement de sécurité* permet au ministre de la Sécurité publique et de la Protection civile de demander au Comité de surveillance « un rapport spécial sur toute question qui relève de sa compétence ». Je suis d'avis que mon Bureau et le Comité de surveillance pourraient, en vertu de ces dispositions, être invités à mener de manière conjointe ou complémentaire une enquête sur certaines activités qui concernent à la fois le Centre et le SCRS.

Voir Bureau du commissaire du Centre de la sécurité des télécommunications, « Message du commissaire », *Rapport annuel 2011-2012*, juin 2012. Pour l'instant, l'article 45.34 de la *Loi sur la Gendarmerie royale du Canada* prévoit que le commissaire de la CCETP, avant de décider d'entreprendre un examen de sa propre initiative, doit présenter une justification au ministre de la Sécurité publique et de la Protection civile lorsqu'il estime que la Commission n'a pas des ressources suffisantes pour faire cet examen, et doit aussi préciser pourquoi l'examen ne répète pas ce qui a déjà été fait dans le cadre d'un autre examen ou d'une autre enquête.

135 Pour en savoir plus sur le cycle financier du Parlement du Canada, voir Alex Smith, *Le cycle financier parlementaire*, publication n° 2015-41-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 27 janvier 2016.

parlementaires ne disposent d'aucune information sur les plans, les activités ou les résultats de ces organismes, même s'ils leur accordent un financement important. Lorsque ces organismes demandent des fonds supplémentaires – dont le montant peut être substantiel – en cours d'année, au moyen du Budget supplémentaire des dépenses, ils ne fournissent pour ainsi dire aucune explication. Sans cette information supplémentaire, les parlementaires ont beaucoup de difficulté à assurer une surveillance financière efficace de ces organismes.

Le 22 juin 2017, le projet de loi C-22, Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement et modifiant certaines lois en conséquence (ci-après, la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* ou LCPSNR), a reçu la sanction royale[136]. Cette loi, entrée en vigueur le 6 octobre 2017[137], créera un autre corps d'examen exécutif – le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) – qui relèvera du premier ministre. Les membres du CPSNR auront accès à des informations classifiées, y compris des avis juridiques, mais seront astreints au secret à perpétuité.

Certaines personnes ont exprimé leur déception quant à la LCPSNR en soulignant que la création d'un comité de parlementaires, plutôt que d'un comité parlementaire, ne sert qu'à placer le Canada dans la situation où se trouvait le Royaume-Uni en 2012, quand son comité du renseignement et de la sécurité relevait toujours du pouvoir exécutif. Au Canada, l'idée d'un comité d'examen parlementaire, dont les membres pourraient entendre et voir de l'information classifiée, a été évoquée dans de nombreuses commissions d'enquête, la première étant la Commission Mackenzie de 1969, qui se penchait sur l'état du système de sécurité du Canada dans le sillage d'une série de scandales d'espionnage soviétique.

Puisque ni les membres des comités sénatoriaux ni ceux des comités de la Chambre des communes n'ont l'autorisation d'accéder à l'information classifiée, le corps législatif canadien ne peut procéder à un examen exhaustif des activités touchant la sécurité nationale et le renseignement. Le pouvoir législatif s'appuie plutôt sur un certain nombre d'« agents du Parlement » qui peuvent, au besoin, accéder à certaines informations et installations classifiées qui présentent un intérêt dans le cadre de leur mandat respectif. Nommés par décrets[138], ces agents effectuent des examens obligatoires et rendent compte de leurs observations au Parlement. Les agents du Parlement travaillent certes dans la confidentialité, mais les rapports qu'ils présentent au Parlement et les témoignages qu'ils peuvent par la suite lui présenter ne doivent pas être classifiés.

Ni le Sénat ni la Chambre des communes n'a créé de comité permanent dont l'unique mandat consiste à examiner les dossiers liés à la sécurité nationale. Au contraire, le Comité sénatorial permanent de la sécurité nationale et de la défense (SECD) et le Comité permanent de la sécurité publique et nationale de la Chambre des communes (SECU) traitent les enjeux liés à la sécurité nationale comme faisant partie d'un ensemble plus large de sujets d'étude potentiels. Étant donné leur mandat relativement étendu, ces deux comités traitent généralement des dossiers de sécurité nationale, y compris le renseignement, de façon épisodique.

---

136 Pour un résumé du texte original du projet de loi C-22, voir Holly Porteous et Dominique Valiquet, *Résumé législatif du projet de loi C-22 : Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement et modifiant certaines lois en conséquence*, publication n° 42-1-C22-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 22 août 2016.

137 « Décret fixant à la date de prise du présent décret la date d'entrée en vigueur de la loi », TR/2017-63, *Gazette du Canada*, partie II, vol. 151, n° 21, 18 octobre 2017, p. 2902.

138 Un décret est un instrument juridique pris par le gouverneur en conseil en vertu d'un pouvoir légal ou, à l'occasion, de la prérogative royale. Tous les décrets sont pris sur recommandation du ministre responsable et entrent en vigueur une fois approuvés par le gouverneur général. Voir Bibliothèque et Archives Canada, « Décrets du Conseil ».

Les dispositions de la LCPSNR obligeant le Sénat et la Chambre des communes à soumettre les rapports annuels et spéciaux du CPSNR à l'étude de ces deux comités obligeront également le Parlement à s'intéresser plus régulièrement aux questions touchant la sécurité nationale. Toutefois, à moins que l'on réduise la portée du mandat de ces deux comités, rien ne garantit que les rapports du CPSNR seront soumis à un examen et à un débat approfondis.

De temps à autre, on a mis sur pied des comités parlementaires spéciaux pour explorer plus en détail certaines politiques relatives à la sécurité nationale. Il en est ainsi par exemple du Comité sénatorial spécial sur la *Loi antiterroriste*, créé en 2004 aux fins de l'examen obligatoire des lois antiterroristes adoptées en 2001. Ce comité a toutefois été dissous en 2013[139].

C. Surveillance par le pouvoir exécutif

1. Comité de surveillance des activités de renseignement de sécurité

Le CSARS a été créé en 1984 en vertu de la *Loi sur le SCRS*[140]. Le CSARS compte un président et au moins deux membres, mais pas plus de quatre membres. Les membres du comité sont tous membres du Conseil privé et ont été nommés par le gouverneur en conseil après la consultation par le premier ministre des chefs des partis de l'opposition. Le CSARS se réunit environ neuf fois par année pour établir ses priorités et passer en revue le travail de son personnel. Selon le paragraphe 39(2) de la *Loi sur le SCRS*, le CSARS dispose d'un accès illimité à toute l'information que contrôle le SCRS, à l'exclusion des documents confidentiels du Cabinet.

Un directeur exécutif supervise les activités quotidiennes du personnel du CSARS. Avec le budget fédéral de 2017-2018, le CSARS a reçu un peu moins de 1,9 million de dollars canadiens en « financement stratégique » (à savoir un financement temporaire) s'étendant jusqu'en 2019-2020, et il dit qu'il s'en servira pour augmenter son effectif, qui passera de 13,7 à 24,5 postes (en équivalents temps plein) pour les tâches d'examen de la légalité et les enquêtes sur les plaintes[141]. Comme il s'agit d'un financement temporaire, le CSARS affirme n'avoir d'autre choix, pour pourvoir ces postes, que de s'appuyer sur des options de dotation à court terme, comme les détachements, ce qui constitue pour l'organisation un véritable défi en matière de ressources humaines.

---

139 Certains membres du comité étaient mécontents de la dissolution du Comité sénatorial spécial sur la Loi antiterroriste. Le sénateur Serge Joyal était contre cette dissolution; il disait craindre que cela reviendrait à éliminer le seul comité sénatorial qui s'occupait de façon continue des enjeux liés à la sécurité nationale. Le président du comité, le sénateur Hugh Segal, était en faveur de la dissolution, mais il espérait que le comité serait remplacé par un nouveau comité permanent inspiré du comité du renseignement et de la sécurité du Royaume-Uni. Voir Sénat du Canada, *Débats*, 1re session, 41e législature, 29 mai 2013 (l'honorable Serge Joyal); Sénat du Canada, *Débats*, 1re session, 41e législature, 6 juin 2013 (l'honorable Hugh Segal).

140 Le SCRS et son organe d'examen, le CSARS, ont été créés au lendemain de révélations touchant des activités de perturbation discutables menées par le Service de sécurité de la GRC au début des années 1970. Ces activités de perturbation de la GRC ont fait l'objet en 1981 de la *Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada* (la Commission McDonald), qui a recommandé la création d'un organisme de renseignement de sécurité civil distinct, qui rendrait des comptes par le truchement d'un organisme d'examen indépendant, et la création d'un comité parlementaire mixte. La première recommandation est la seule à avoir été mise en œuvre.

141 Comité de surveillance des activités de renseignement de sécurité (CSARS), « Dépenses et ressources humaines ».

Avant l'élimination du poste d'inspecteur général du SCRS en juin 2012, le ministre de la Sécurité publique et de la Protection civile, ministre responsable du SCRS, pouvait compter sur le titulaire pour fournir une attestation annuelle du respect des politiques et directives du ministre dans toutes les activités et opérations du Service. Aujourd'hui, c'est le CSARS qui s'acquitte des tâches de l'inspecteur général[142].

Si on laisse de côté les fonds non permanents, le budget annuel total du CSARS est aujourd'hui d'environ 2,8 millions de dollars canadiens[143]. À titre comparatif, le budget annuel du SCRS est d'environ 577 millions de dollars canadiens[144].

2. Bureau du commissaire du CST

Le Bureau du commissaire du CST (BCCST) a été créé en juin 1996 par décret. Le CST et le BCCST fonctionnaient par décret avant que la *Loi sur la défense nationale* soit modifiée, en 2001, pour codifier les autorités et les tâches du CST et du BCCST[145].

Le BCCST est dirigé par un juge surnuméraire qui est nommé par le gouverneur en conseil et dont le mandat, en vertu du paragraphe 273.63(2) de la *Loi sur la défense nationale*, consiste à mener des enquêtes sur les plaintes du public, à traiter ces plaintes et à examiner la légalité des activités du CST. Dans le cas où le commissaire du CST estime que le CST a mené des activités illégales, il doit immédiatement en informer le ministre de la Défense nationale et le procureur général du Canada. Les pouvoirs du commissaire du CST lui sont conférés par la partie II de la *Loi sur les enquêtes*, et ce dernier a un accès illimité à l'information que détient le CST (à l'exception des documents confidentiels du Cabinet), ainsi qu'aux installations et au personnel du CST. Conformément au paragraphe 273.65(8) de la *Loi sur la défense nationale*, le commissaire du CST doit examiner les activités du CST menées avec autorisation ministérielle et confirmer cette autorisation dans un rapport annuel qu'il présente au ministre de la Défense nationale.

Le paragraphe 273.63(3) de la *Loi sur la défense nationale* prévoit ce qui suit :

> Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

---

142 L'Université d'Ottawa tient à jour des archives en ligne des rapports de l'inspecteur général du SCRS de 2000 à 2010. Voir Université d'Ottawa, Centre d'études en politiques internationales, *Archives des certificats annuels de l'inspecteur général du SCRS*.

143 CSARS, « Dépenses et ressources humaines ».

144 Le budget total du SCRS pour 2015-2016 était de 537 millions de dollars canadiens. Selon le budget principal des dépenses de 2017-2018, ce budget passerait à 577 millions de dollars canadiens. Voir Service canadien du renseignement de sécurité, « Ressources financières », *Rapport public 2014-2016*; Secrétariat du Conseil du Trésor du Canada, « Dépenses par programme ou par fin 2017-2018 : Service canadien du renseignement de sécurité », *Plan de dépenses du gouvernement et Budget principal des dépenses (parties I et II)*, 23 février 2017.

145 Dans le cas du CST, les décrets étaient classifiés.

Le commissaire du CST travaille à temps partiel seulement, mais il peut s'appuyer sur un petit effectif de 11,5 employés à temps plein (y compris le directeur exécutif), dont 8,5 (en équivalents temps plein) sont des experts en la matière, responsables des tâches d'examen proprement dites[146]. Le BCCST reçoit un financement annuel total de 2,1 millions de dollars canadiens, dont une tranche de 1,6 million de dollars canadiens sert aux tâches d'examen. Dans son plan ministériel 2017-2018, le BCCST disait avoir l'intention de demander un financement permanent supplémentaire qui permettrait d'embaucher un employé de plus, pour les tâches d'examen, et de moderniser ses « ressources technologiques[147] ». À titre comparatif, le budget annuel total du CST est aujourd'hui de 596 millions de dollars canadiens[148].

3. Commission civile d'examen et de traitement des plaintes relatives à la GRC

La Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP) a été créée en 2014 par un texte législatif modifiant la *Loi sur la GRC*[149]. Cette loi confère à la CCETP le mandat d'examiner les plaintes du public relatives au comportement de membres de la GRC lorsqu'ils sont de service. La CCETP a également le pouvoir de lancer des examens des activités de la GRC dans l'intérêt public, mais elle doit auparavant présenter une justification au ministre de la Sécurité publique et de la Protection civile[150]. La CCETP compte 67 employés (équivalents temps plein), dont 45 sont affectés aux enquêtes. Son budget annuel total est d'un peu moins de 10 millions de dollars canadiens, et une part de 7,3 millions de dollars canadiens sert aux activités d'examen[151]. À titre comparatif, le budget annuel total de la GRC est d'environ 3,4 milliards de dollars canadiens[152].

D. Surveillance parlementaire

Les organismes de sécurité nationale et de renseignement du Canada font l'objet d'une surveillance par plusieurs agents du Parlement. Les comités parlementaires qui examinent les rapports de ces agents peuvent donc aussi examiner les activités des organismes de sécurité nationale et de renseignement. Par exemple, le Comité permanent des comptes publics de la Chambre des communes examine les rapports du vérificateur général du Canada, qui, de temps à autre, mène une enquête sur la gestion des programmes du domaine de la sécurité nationale.

---

146 Pour connaître le nombre exact d'experts en la matière parmi le personnel du BCCST, voir Bureau du commissaire du Centre de la sécurité des télécommunications, « Programme 1.1 : Le programme d'examen du commissaire », *Rapport sur les plans et priorités 2016-2017*.

147 Bureau du commissaire du Centre de la sécurité des télécommunications, « Dépenses et ressources humaines », *Plan ministériel 2017-2018*. Voir aussi Alex Boutilier, « Review agency for Canada's spies says it needs more funding », *The Toronto Star*, 14 mars 2017.

148 Secrétariat du Conseil du Trésor du Canada, « Budget principal des dépenses – Budget des dépenses 2017-2018 : Centre de la sécurité des télécommunications », *Plan de dépenses du gouvernement et Budget principal des dépenses (parties I et II)*.

149 Voir Lyne Casavant et Dominique Valiquet, *Résumé législatif du projet de loi C-42 : Loi modifiant la Loi sur la Gendarmerie royale du Canada et apportant des modifications connexes et corrélatives à d'autres lois*, publication n° 41-1-C42-F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, 7 novembre 2012.

150 Voir la note 13.

151 Voir Commission civile d'examen et de traitement des plaintes relatives à la GRC, « Dépenses et ressources humaines », *Plan ministériel 2017-2018*.

152 Voir GRC, « Dépenses et ressources humaines », *Plan ministériel de la Gendarmerie royale du Canada 2017-2018*.

De la même façon, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (ETHI) examine les rapports du commissaire à la protection de la vie privée du Canada et ceux du commissaire à l'information du Canada, puisque leurs tâches concernent de plus en plus les organismes de sécurité nationale et de renseignement, lesquels sont assujettis à la *Loi sur la protection des renseignements personnels* et à la *Loi sur l'accès à l'information*. L'ETHI, dans le cadre de son étude récente de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*, dont il a déjà été question, a en outre entendu des témoignages fournis directement par des représentants des ministères et organismes concernés de même que des trois organismes d'experts responsables d'examens.

Même si l'examen par le Parlement des activités de sécurité nationale et de renseignement réparti entre plusieurs comités a l'avantage de permettre l'examen des différents enjeux sous de nombreuses perspectives, l'envers de la médaille est qu'il limite la capacité de chaque parlementaire d'acquérir une expertise sur les thèmes traités. Puisqu'ils examinent les organismes de sécurité nationale à partir de données non classifiées et sous un angle étroit, les parlementaires ont de la difficulté à étudier les questions y afférentes de façon réellement exhaustive.

Si l'on veut que ces comités acquièrent les connaissances et l'expertise nécessaires pour demander des comptes aux organismes de sécurité nationale et de renseignement, il faudra replacer les enjeux dans un cadre stratégique; par exemple, il faudrait définir les priorités du Canada au chapitre du renseignement et vérifier régulièrement dans quelle mesure les capacités nationales répondent à ce besoin.

Cependant, le SECD de même que le SECU ont le potentiel d'acquérir cette expertise, puisque leur mandat consiste à examiner les questions de sécurité nationale. Voici une analyse de ces deux comités.

1. Comité sénatorial permanent de la sécurité nationale et de la défense

Le Sénat a créé le SECD le 15 mars 2001 et, selon son mandat, ce dernier « peut être saisi de toute question concernant la sécurité nationale et la défense en général, notamment les anciens combattants[153] ». Auparavant, le Sénat n'examinait les enjeux liés à la sécurité nationale et au renseignement que dans le contexte de comités spéciaux, par exemple le Comité sénatorial du renseignement, qui s'est réuni en 1987, en 1988 puis une autre fois en 1999 pour étudier les activités de la lutte antiterroriste. Le Comité sénatorial du renseignement avait une particularité : son président a essayé d'inciter les représentants des organismes à répondre avec franchise en leur faisant témoigner à huis clos.

Bien que les ordres de renvoi du SECD puissent changer d'une session à l'autre, ce comité affirme que son large mandat lui permet de se pencher sur les capacités du MDN, des Forces armées canadiennes et de SPC, les relations de travail entre les divers organismes qui s'occupent de la collecte et de l'analyse de renseignements, les mécanismes d'examen des organismes de renseignement ainsi que la sécurité des frontières et des infrastructures essentielles[154].

---

153 Voir Sénat du Canada, « Chapitre douze : Comités », *Règlement du Sénat du Canada*, par. 7(15).

154 Comité sénatorial permanent de la sécurité nationale et de la défense, *Introduction au Comité sénatorial permanent de la sécurité nationale et de la défense*.

Le SECD s'occupe de dossiers non classifiés. En vertu de l'article 12-9(2) du *Règlement du Sénat du Canada*, le SECD peut exiger la comparution de témoins et la production de documents.

2. Comité permanent de la sécurité publique et nationale de la Chambre des communes

Le SECU a été créé grâce à une motion modifiant le *Règlement de la Chambre des communes*, adoptée le 5 avril 2006. Jusque-là, tous les dossiers concernant la sécurité publique et nationale étaient renvoyés à un comité qui s'appelait le Comité permanent de la justice, des droits de la personne, de la sécurité publique et de la protection civile de la Chambre des communes ou à un de ses sous-comités. Conformément à l'article 104 du *Règlement de la Chambre des communes*, le SECU comprend 10 membres. À l'heure actuelle, six de ses membres, y compris le président, viennent du parti au pouvoir – le Parti libéral du Canada –, et les quatre autres, des deux partis de l'opposition (trois du Parti conservateur du Canada et un du Nouveau Parti démocratique du Canada). Le président et les deux vice-présidents (représentant chacun un parti de l'opposition) du SECU sont élus par les membres du Comité.

L'article 108 du *Règlement* précise le mandat de certains comités permanents et prévoit que ces derniers sont autorisés à se pencher et à faire enquête sur toutes les questions qui leur sont renvoyées par la Chambre des communes et à faire rapport à ce sujet. À titre de comité permanent, le SECU est autorisé à convoquer des personnes et à exiger la production de documents et de dossiers ainsi qu'à déléguer à des sous-comités la totalité ou une partie de ses pouvoirs. Il peut se réunir pendant que la Chambre siège et pendant les périodes d'ajournement. Le SECU peut également siéger conjointement avec d'autres comités permanents.

Le SECU s'occupe de dossiers non classifiés, et son mandat lui permet d'examiner les politiques et les activités d'un des plus grands portefeuilles ministériels qui soit – SPC – de même que les quelque 140 lois que ce ministère et ses organismes administrent. Plus précisément, le SECU a pour mandat d'examiner les politiques, les programmes et les lois touchant SPC, l'Agence des services frontaliers du Canada, le SCRS, le Service correctionnel du Canada, la Commission des libérations conditionnelles du Canada, la GRC, le CSARS, la CCETP, le Bureau de l'enquêteur correctionnel et le Comité externe d'examen de la GRC[155].

Donc, comme on vient de l'évoquer, le SECU examine des enjeux liés à la sécurité nationale, mais il le fait uniquement dans le cadre de dossiers plus vastes qui comprennent des questions touchant le droit criminel, le système correctionnel et la mise en liberté sous condition de détenus sous responsabilité fédérale, la sécurité des frontières, les services de police et l'application de la loi, la prévention de la criminalité et la gestion des urgences.

Le SECU s'est penché récemment sur la LCPSNR et sur le document de consultation du gouvernement portant sur la sécurité nationale, et a présenté des rapports sur ces sujets. Conformément au *Règlement de la Chambre des communes*, lorsque le président d'un comité demande que l'on donne suite à un rapport, le gouvernement est tenu de présenter sa réponse dans les 120 jours suivant la présentation du rapport.

---

155 Le Comité externe d'examen de la GRC est un tribunal administratif qui procède à l'examen de cas et présente des conclusions et des recommandations en vue de décisions d'appel touchant certaines questions de relations de travail à la GRC.

E. Faits nouveaux et réformes proposées

1. Comité des parlementaires sur la sécurité nationale et le renseignement

Comme nous l'avons indiqué, le Parlement du Canada a adopté le 22 juin 2017 la LCPSNR, créant le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), chargé d'examiner les enjeux relatifs à la sécurité nationale et au renseignement. L'article 8 de cette loi donne au CPSNR le mandat d'examiner :

> a) les cadres législatif, réglementaire, stratégique, financier et administratif de la sécurité nationale et du renseignement;
>
> b) les activités des ministères liées à la sécurité nationale ou au renseignement, à moins qu'il ne s'agisse d'opérations en cours et que le ministre compétent ne détermine que l'examen porterait atteinte à la sécurité nationale;
>
> c) toute question liée à la sécurité nationale ou au renseignement dont il est saisi par un ministre.

Selon cette nouvelle loi, après avoir consulté les chefs des groupes parlementaires et des groupes reconnus au Sénat, le premier ministre choisit les membres du CPSNR, qui relèvent du premier ministre. Le 8 janvier 2016, six mois avant le dépôt du projet de loi à la Chambre des communes, le premier ministre a attribué au député David McGuinty un « rôle de direction » au sein du comité et a permis aux organismes de sécurité nationale et de renseignement de mettre M. McGuinty au courant des enjeux importants[156]. Comme condition de leur nomination au CPSNR, tous les membres seront astreints au secret à perpétuité. Puisque le CPSNR ne sera pas un comité parlementaire, ses membres ne jouiront pas du privilège parlementaire, et cela s'applique aussi à toute divulgation non autorisée qu'ils pourraient faire dans le cadre de leur travail à d'autres titres au Parlement.

Les 11 membres du CPSNR seront des parlementaires en exercice qui n'assument pas de fonctions de ministre ou de secrétaire parlementaire. Le comité peut comprendre jusqu'à trois membres venant du Sénat, et jusqu'à cinq des huit autres membres seront du parti au pouvoir à la Chambre des communes. Le président n'aura droit de vote qu'en cas d'égalité.

À bien des égards, l'étendue de la compétence du CPSNR sera déterminée par sa capacité à obtenir l'information demandée. Par exemple, le texte original de la législation aurait privé le CPSNR de la capacité d'examiner les activités de renseignement de défense en ne lui donnant pas accès aux renseignements concernant les activités de renseignement de défense en cours qui soutiennent des opérations militaires, notamment la nature et la teneur de plans soutenant de telles opérations. Cette proposition a été supprimée de la loi, de même que la proposition qui aurait interdit au CPSNR d'exercer une surveillance directe sur le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), l'organisme du renseignement financier du Canada. La LCPSNR permet au CPSNR d'accéder aux analyses stratégiques du CANAFE ou à toute autre information que le CANAFE n'a pas communiquée et qui ne révèle pas l'identité de personnes ou d'entités.

---

156 Cela signifiait pour de nombreuses personnes que M. McGuinty allait présider le nouveau comité parlementaire. Voir Premier ministre du Canada, *Le premier ministre du Canada annonce un nouveau rôle de direction pour le député McGuinty*, communiqué, 8 janvier 2016. Pour obtenir une copie (caviardée) des documents d'information communiqués à M. McGuinty, obtenue grâce à une demande faite en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, veuillez communiquer avec la Bibliothèque du Parlement du Canada.

En application de la LCPSNR, les membres du comité se verront automatiquement refuser l'accès aux documents confidentiels du Cabinet, aux informations révélant le nom de sources humaines confidentielles actuelles ou prévues, et à l'information relative à une enquête menée par un organisme d'application de la loi qui est susceptible de déboucher sur des poursuites. D'importantes limites seront également imposées au comité quant à l'accès à certains types d'information, en particulier aux renseignements opérationnels spéciaux. Toutefois, si un ministre invoquait la disposition pour refuser au CPSNR l'accès à une information qui est sous le contrôle d'un ministère et à laquelle il aurait pu avoir accès (article 16), le ministre devra informer le comité de sa décision et présenter ses justifications. Dans le cas où l'information refusée est contrôlée par le SCRS, le CST ou la GRC, le ministre concerné devra aussi informer de sa décision l'organisme d'experts qui surveille l'entité concernée et fournir ses justifications. Cette procédure vise à s'assurer que le CPSNR ne pourra pas passer outre au refus du ministre et demander l'accès à l'information à un des organismes d'experts. La LCPSNR cherche à limiter le recours par les ministres à ce pouvoir en demandant au CPSNR de présenter, dans ses rapports annuels, une liste de toutes les décisions de refuser l'accès prises en vertu de l'article 16.

En se concentrant surtout sur les questions d'efficacité, le CPSNR examinera les politiques, l'administration et les activités de l'ensemble de la communauté de la sécurité nationale et du renseignement. De manière générale, il devrait procéder à l'examen *ex post* (après les faits) des activités de sécurité nationale, mais la LCPSNR prévoit qu'un ministre puisse permettre un examen des activités opérationnelles en cours[157].

Le CPSNR sera soutenu par un petit secrétariat dirigé et doté en personnel par un directeur exécutif désigné qui aura le statut de sous-ministre[158]. Il n'existe que très peu d'information publique quant au budget du secrétariat du CPSNR. Selon un des tableaux compris dans l'annexe de l'Exposé économique de l'automne 2016 du gouvernement fédéral, il semble toutefois que le secrétariat disposera d'un budget annuel d'environ 3,2 millions de dollars canadiens, ce qui suffira à payer les salaires du directeur exécutif, du personnel des services internes et de trois ou quatre chercheurs[159].

F. Autres faits nouveaux

L'adoption de la LCPSNR s'inscrit dans toute une série de changements récents apportés aux pouvoirs et au cadre de gouvernance de la communauté de la sécurité et du renseignement du Canada. Certains des changements plus controversés ont été apportés au moment de l'adoption en juin 2015 du projet de loi C-51, une loi antiterroriste omnibus qui donnait de nouveaux pouvoirs de « réduction de la menace » au SCRS, élargissait le pouvoir du ministre de la Sécurité publique de refuser de communiquer des renseignements touchant la sécurité nationale qui ont servi à établir des certificats de sécurité visés par la section 9 de la *Loi sur l'immigration et la protection des réfugiés* et prévoyait un échange d'information

---

157 L'alinéa 8(1)b) de la loi interdit au CPSNR d'examiner des opérations en cours si un ministre a déterminé qu'un tel examen porterait atteinte à la sécurité nationale. Les paragraphes 8(2) et 8(3), respectivement, précisent que le ministre doit donner ses motifs, lorsqu'il détermine que l'examen porterait atteinte à la sécurité nationale, et qu'il doit informer le CPSNR lorsqu'il détermine que l'examen ne porterait plus atteinte à la sécurité nationale.

158 Le fait de donner ce titre au directeur exécutif du secrétariat du CPSNR soulève quelques questions intéressantes. Le titulaire aurait un rang supérieur non seulement à celui de tous les représentants du pouvoir exécutif chargés de la surveillance, mais aussi à celui du conseiller à la sécurité nationale et au renseignement auprès du premier ministre, qui exerce ses fonctions sans fondement législatif. Toutefois, si le projet de loi C-59, Loi concernant les questions de sécurité nationale, présenté à la Chambre des communes le 20 juin 2017, était adopté, le CSARS et le BCCST seraient remplacés par un nouvel organisme d'experts en matière d'examen, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. Ce nouvel organisme d'experts serait dirigé par un sous-ministre, soit quelqu'un de rang égal à celui du directeur du secrétariat du CPSNR.

159 Voir Gouvernement du Canada, « Mesures stratégiques prises depuis le dépôt du budget de 2016 : Tableau A1.4 », dans « Annexe 1 – Précisions au sujet des projections économiques et budgétaires », *Énoncé économique de l'automne 2016*, 1er novembre 2016.

fortement accru entre les ministères et organismes ayant des responsabilités en matière de sécurité nationale. Le gouvernement actuel, qui est arrivé au pouvoir en octobre 2015, a mené sa campagne en promettant d'annuler les dispositions « problématiques » du projet de loi C-51[160], et il a l'intention de le faire en déposant, le 20 juin 2017, le projet de loi C-59, Loi concernant des questions de sécurité nationale[161].

Si le projet de loi C-59 était adopté, il modifierait profondément les organismes qui, aujourd'hui, scrutent les organismes de sécurité nationale et de renseignement. Par exemple, le projet de loi C-59 fusionnerait le CSARS et le BCCST pour former un organisme unique, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). La CCETP resterait en place, mais toutes ses tâches liées à la sécurité nationale seraient transférées à l'OSSNR. L'Office, en plus d'examiner les activités du SCRS et du CST, aurait pour mandat (en vertu de l'article 8) d'examiner « les questions liées à la sécurité nationale ou au renseignement dont il est saisi par un ministre ». Cela veut dire que l'étendue des compétences de l'OSSNR serait à peu près équivalente à celle du CPSNR. Enfin, l'OSSNR aurait pour mandat d'examiner non seulement la légitimité des activités liées à la sécurité nationale et au renseignement, mais aussi leur caractère raisonnable et leur nécessité, créant ainsi un mécanisme supplémentaire motivant la modification des lois ou des règlements.

Le projet de loi C-59 prévoit en outre la création d'un poste de commissaire au renseignement, qui serait confié à un juge à la retraite. Ce dernier aurait pour mandat d'examiner le caractère raisonnable des conclusions sur lesquelles reposent des autorisations accordées par les ministres pour certains types d'activités du CST et certaines déterminations ministérielles touchant la collecte, la conservation, la consultation et l'exploitation d'ensembles de données par le SCRS. Contrairement à l'OSSNR, qui serait un organisme d'examen, le commissaire au renseignement jouerait un rôle de surveillance et pourrait empêcher ou modifier la réalisation de certaines activités planifiées.

En même temps, le projet de loi C-59 accorderait d'importants nouveaux pouvoirs aux organismes de renseignement du Canada. Par exemple, la *Loi sur le SCRS* serait modifiée pour créer un régime selon lequel le SCRS serait autorisé à recueillir et à utiliser des ensembles de données concernant des Canadiens, dans la mesure où ces ensembles de données auraient une « pertinence » au regard de l'accomplissement des tâches du SCRS. Ces modifications à la *Loi sur le SCRS* semblent faire suite à une décision de la Cour fédérale de 2016, dans laquelle le SCRS a été réprimandé pour avoir manqué à son obligation de franchise envers la Cour relativement à sa pratique de collecte et de conservation de métadonnées sur des Canadiens ne faisant l'objet d'aucune enquête[162].

Le CST se verrait lui aussi conférer d'importants nouveaux pouvoirs. Selon le mandat habilitant proposé par le projet de loi C-59, la Loi sur le Centre de la sécurité des télécommunications, le CST sera autorisé à mener des « cyberopérations actives » ciblant des personnes, des États, des organisations ou des groupes terroristes étrangers. Le CST serait également habilité à fournir un soutien technique et opérationnel pour les cyberopérations actives menées dans le contexte de missions militaires. Les Forces canadiennes n'avaient pas jusqu'ici eu l'autorisation de mener des cyberopérations de ce genre.

Pour terminer, le CST pourrait également fournir des conseils et des services visant à protéger les éléments critiques de l'infrastructure d'information, y compris les éléments d'infrastructure appartenant au secteur privé et exploités par celui-ci, et les systèmes et réseaux utilisés par les parlementaires et les cours fédérales.

---

160 Voir Parti libéral du Canada, « Assurer la sécurité des Canadiennes et des Canadiens : Projet de loi C-51 », *Changer ensemble : le bon plan pour renforcer la classe moyenne*, octobre 2015, p. 59.

161 Projet de loi C-59, Loi concernant des questions de sécurité nationale, 1re session, 42e législature.

162 Voir Cour fédérale, 2016 CF 1105.

NOUVELLE-ZÉLANDE

A. Aperçu des organismes de renseignement

Il y a en Nouvelle-Zélande deux organismes responsables du renseignement et de la sécurité. Le New Zealand Security Intelligence Service (service du renseignement de sécurité de la Nouvelle-Zélande [NZSIS]) se spécialise dans les activités de renseignement humain. Le Government Communications Security Bureau (bureau de la sécurité des communications du gouvernement [GCSB]) se spécialise dans les activités de renseignement électromagnétique, d'assurance de l'information et de cybersécurité[163].

Les deux organismes assument les fonctions suivantes[164] :

- recueillir et analyser des renseignements conformément aux priorités du gouvernement;
- fournir tous les renseignements recueillis et les analyses de ces renseignements au ministre responsable de l'organisme en question (le ministre responsable), à l'administrateur en chef du ministère du Premier ministre et du Cabinet et à toute autre personne (en Nouvelle-Zélande ou à l'étranger) qui a reçu l'autorisation du ministre responsable;
- fournir des services, des conseils et un soutien en matière de sécurité protective aux autorités publiques et à d'autres personnes autorisées (en Nouvelle-Zélande ou à l'étranger);
- dans le cas du GCSB, mener des activités d'assurance de l'information et de cybersécurité au profit des autorités publiques et d'autres personnes autorisées (en Nouvelle-Zélande ou à l'étranger) et faire tout ce qu'il est nécessaire et souhaitable de faire pour protéger la sécurité et l'intégrité des infrastructures de communication et d'information importantes pour le gouvernement;
- collaborer avec l'autre organisme de renseignement et de sécurité, et collaborer avec la police nationale et les forces armées de la Nouvelle-Zélande et leur fournir des conseils et de l'aide;
- collaborer avec diverses entités, et leur fournir des conseils et de l'aide, quand elles interviennent en cas de menace imminente pour la vie ou la sécurité des personnes suivantes :
  - toute personne se trouvant en Nouvelle-Zélande;
  - tout citoyen ou résident permanent de la Nouvelle-Zélande qui se trouve à l'étranger;
  - toute personne se trouvant dans une région dans laquelle la Nouvelle-Zélande a des responsabilités en matière de recherche et de sauvetage en vertu de lois internationales;
  - toute personne se trouvant hors de la juridiction territoriale d'un pays quelconque.

Les organismes doivent respecter les lois de la Nouvelle-Zélande et mener leurs activités de manière à faciliter la surveillance démocratique[165].

En plus du NZSIS et du GCSB, la New Zealand Intelligence Community (la communauté du renseignement de la Nouvelle-Zélande) comprend le National Assessments Bureau (bureau des évaluations nationales), qui fait partie du ministère du Premier ministre et du Cabinet. Les forces armées de la Nouvelle-Zélande ont elles aussi des capacités en matière de renseignement, et toute une gamme d'autres ministères et organismes gouvernementaux, notamment la police nationale, le service des douanes et Immigration New Zealand, ont des unités consacrées au renseignement[166].

---

163 *Intelligence and Security Act 2017* (ISA 2017), art. 7 et 8.

164 *Ibid.*, art. 10 à 14.

165 *Ibid.*, art. 17.

166 New Zealand Intelligence Community, *About us*.

B. Faits nouveaux

L'*Intelligence and Security Act 2017* (loi sur le renseignement et la sécurité de 2017 [ISA 2017]) a reçu la sanction royale le 28 mars 2017. Cette loi remplace les quatre lois qui s'appliquaient jusque-là aux organismes de renseignement et de sécurité et à leurs organismes de surveillance, et elle met en œuvre la réponse du gouvernement au récent examen indépendant du renseignement et de la sécurité[167].

Une modification apportée en 2013 à la *New Zealand Security Intelligence Committee Act 1996* (loi de 1996 sur le comité du renseignement de sécurité de la Nouvelle-Zélande) exige qu'un examen des organismes de renseignement et de sécurité soit effectué tous les cinq à sept ans[168]. Le rapport concernant le premier examen périodique réalisé a été publié en février 2016[169]. Les examinateurs avaient notamment pour mandat de déterminer si les mécanismes de surveillance actuels fournissaient une protection suffisante aux niveaux opérationnel, judiciaire et politique pour que l'on puisse s'assurer que les organismes agiraient conformément à la loi et bénéficieraient toujours de la confiance du public[170].

L'examen a débouché sur une proposition selon laquelle les organismes de renseignement et de sécurité, leurs organismes de surveillance, voire les organismes d'évaluation du renseignement, devraient être couverts par un seul texte de loi. Cette loi comprendrait un nouveau régime d'autorisation complet exigeant un certain niveau d'autorisation pour toutes les activités des organismes liées au renseignement et à la sécurité qui nécessitent la collecte d'information sur des personnes ou des organisations, et le niveau d'autorisation serait proportionnel au niveau d'intrusion que la collecte suppose. Cette loi entraînerait de plus quelques changements visant à faciliter une surveillance accrue des organismes et une responsabilisation accrue quant à leurs activités[171].

Les recommandations formulées à la fin de l'examen, en ce qui a trait à la surveillance, sont notamment les suivantes[172] :

- les organismes devraient être intégrés au secteur public et être assujettis à la *State Sector Act 1988* (loi sur le secteur public de 1988), avec des exceptions et des exemptions appropriées;
- il faudrait examiner de plus près les autorisations visant les activités des organismes lorsqu'il s'agit d'activités plus intrusives ou qui ciblent des Néo-Zélandais;
- l'Inspector-General of Intelligence and Security (inspecteur général du renseignement et de la sécurité [IGIS]) devrait être nommé par le gouverneur général sur recommandation de la Chambre des représentants, plutôt que sur celle du premier ministre;
- le financement du bureau de l'IGIS devrait être distinct de celui des organismes;

---

167 New Zealand Intelligence and Security Bill, 2016 (projet de loi sur le renseignement et la sécurité de la Nouvelle-Zélande, 2016). Les quatre lois en question sont les suivantes : *New Zealand Security Intelligence Service Act 1969*; *Government Communications Security Bureau Act 2003*; *Inspector-General of Intelligence and Security Act 1996*; *Intelligence and Security Committee Act 1996* (loi sur le service du renseignement de sécurité, 1969, loi sur le bureau de la sécurité des communications du gouvernement de 2003, loi sur l'inspecteur général du renseignement et de la sécurité de 1996, loi sur le comité du renseignement et de la sécurité de 1996).

168 *Intelligence and Security Committee Amendment Act 2013*, art. 9.

169 Sir Michael Cullen, Dame Patsy Reddy, *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*, 2016.

170 *Ibid.*, p. 1.

171 *Ibid.*, p. 3.

172 *Ibid.*, p. 5 à 11.

- il faudrait étendre les pouvoirs et les fonctions de l'IGIS :
  - la catégorie des personnes qui peuvent porter plainte devrait être élargie pour inclure les personnes qui ne sont pas néo-zélandaises;
  - l'examen des autorisations ne devrait pas porter uniquement sur les questions procédurales mais devrait viser à brosser un tableau complet de la situation;
  - il faudrait supprimer l'interdiction de mener des enquêtes sur des questions opérationnelles de nature délicate;
- la taille maximale de l'Intelligence and Security Committee (comité du renseignement et de la sécurité [ISC]) devrait être augmentée, de façon à assurer une souplesse accrue de la représentation;
- le comité devrait pouvoir élire lui-même son président, qui ne serait pas nécessairement le premier ministre;
- le comité devrait être en mesure de demander, sans toutefois l'exiger, que l'IGIS mène une enquête, y compris sur des questions opérationnelles de nature délicate.

L'ISA 2017 englobait la plupart des recommandations de l'examen, mais pas toutes[173].

Quelques dispositions de l'ISA 2017 sont entrées en vigueur le 1er avril 2017. Les autres dispositions sont entrées en vigueur le 28 septembre 2017[174].

C. Surveillance : résumé

Toutes les activités des organismes de renseignement et de sécurité font l'objet d'une surveillance par le pouvoir exécutif, le parlement, le pouvoir judiciaire et un organisme indépendant. Le premier ministre, à titre de ministre de la Sécurité nationale et du Renseignement, a la responsabilité de diriger le système de la sécurité nationale. Le ministre responsable de chacun des organismes assure la surveillance ministérielle, dans le cadre fixé par le premier ministre[175]. Les ministres responsables peuvent de manière autonome délivrer certains mandats relatifs au renseignement et doivent collaborer avec le commissaire aux mandats de renseignement, un ancien juge, pour la délivrance des autres types de mandat. L'examen parlementaire des politiques, de l'administration et des dépenses des organismes est effectué par l'ISC. L'IGIS exerce une surveillance indépendante des organismes pour s'assurer qu'ils agissent de façon appropriée et qu'ils travaillent dans la légalité et avec efficacité.

Le NZSIS et le GCSB sont des départements d'État[176]. Leurs directeurs généraux sont nommés par le State Services Commissioner (commissaire à la fonction publique), qui fait l'examen de leur rendement et peut les renvoyer, conformément à la *State Sector Act 1988*[177]. Chaque organisme doit remettre à son ministre responsable un rapport annuel contenant toute l'information que les ministères sont obligés de fournir conformément à la *Public Finance Act 1989* (loi sur les finances publiques de 1989) de même que des renseignements supplémentaires sur ses propres activités conformément à l'ISA 2017. Le ministre doit remettre un exemplaire de ce rapport à l'ISC, ainsi qu'un exemplaire au Parlement qui peut avoir été caviardé. Le rapport remis au Parlement doit être publié sur le site Internet de l'organisme concerné[178].

---

173 New Zealand Intelligence and Security Bill 2016.

174 ISA 2017, art. 2.

175. National Security and Intelligence role created, 6 octobre 2014.

176. ISA 2017, art. 7 et 8.

177. *State Sector Act 1988*, art. 35, 39 et 43.

178. ISA 2017, art. 221; *Public Finance Act 1989*, art. 45.

D. Surveillance parlementaire

1. Intelligence and Security Committee

L'ISC a été créé en vertu de l'*Intelligence and Security Committee Act 1996*. Jusque-là, l'examen parlementaire des organismes de renseignement et de sécurité était réalisé par un comité spécial de l'administration du gouvernement[179]. La création d'un comité statutaire avait pour objectif d'étendre la surveillance parlementaire exercée sur les organismes tout en tenant compte des considérations relatives à la sécurité nationale[180]. Le Parlement a conservé son pouvoir de mener des enquêtes sur les organismes, mais, en pratique, la Chambre adopte un ordre sessionnel, pour chaque législature, interdisant qu'un comité spécial procède à l'examen des organismes de renseignement et de sécurité[181].

L'ISA 2017 augmente l'interaction entre l'ISC et l'IGIS. L'ISC peut maintenant demander à l'IGIS de mener une enquête visant à établir la conformité avec la loi ou le caractère approprié des activités des organismes. L'ISC examine également, maintenant, le rapport annuel de l'IGIS et en discute avec l'auteur[182].

a. Fonctions

Les fonctions de l'ISC sont les suivantes :

- examiner les politiques, l'administration et les dépenses des organismes de renseignement et de sécurité;
- recevoir et examiner les rapports annuels des organismes;
- après avoir reçu le rapport annuel de chaque organisme, effectuer un examen annuel de l'organisme au regard de l'exercice précédent;
- examiner tout projet de loi, toute pétition et toute autre question touchant un organisme que lui renvoie la Chambre;
- demander à l'IGIS de mener une enquête sur :
  - toute question liée au respect, par un organisme, des lois de la Nouvelle-Zélande, y compris les lois touchant les droits de la personne;
  - le caractère approprié d'une activité donnée d'un organisme;
- examiner toute question, qui n'est pas liée directement aux activités d'un organisme, que le premier ministre lui renvoie parce qu'elle aurait des répercussions sur le renseignement ou la sécurité;
- examiner le rapport annuel de l'IGIS et en discuter avec lui.

---

179 Standing Orders of the House of Representatives, 1992, S.O. 345.

180 Intelligence and Security Agencies Bill, rapport du Committee on the Intelligence and Security Agencies Bill (comité du projet de loi sur les organismes de renseignement et de sécurité), p. ii, 1996.

181 Nouvelle-Zélande, Chambre des représentants, Sessional and other orders of continuing effect, Fifty-first Parliament (as at 21 October 2015); David McGee, Parliamentary practice in New Zealand, 4e éd., Mary Harris et David Wilson (dir.), Auckland, Oratia Books, 2017, p. 505.

182 Les articles 192 à 205 et l'article 223 ainsi que les articles 17 à 26 de l'annexe 3 de l'ISA 2017, en particulier, concernent l'Intelligence and Security Committee.

L’ISC n’exerce pas de fonctions touchant :

- les enquêtes sur des questions relevant de la compétence de l’IGIS;
- les enquêtes sur des questions opérationnelles de nature délicate, y compris celles qui concernent les méthodes de collecte et de production de renseignements, ou encore les sources d’information;
- les enquêtes sur des plaintes déposées par des personnes au sujet des activités d’un organisme, lorsque ces plaintes pourraient être réglées en vertu d’une autre mesure législative.

L’examen des organismes de renseignement et de sécurité doit être effectué tous les cinq à sept ans. Avant de nommer les examinateurs ou de définir les modalités de cet examen, le premier ministre doit consulter l’ISC. Les examinateurs remettent leur rapport à l’ISC; ce dernier, après l’avoir étudié et avoir exclu toute information qui ne peut pas être divulguée, le présentera à la Chambre.

b. Pouvoirs et exercice des fonctions

Le directeur général d’un organisme de renseignement et de sécurité doit comparaître devant l’ISC lorsque celui-ci le convoque. L’ISC peut demander à toute autre personne de comparaître et de fournir un témoignage, ou encore de communiquer un document ou toute autre information dont il pourrait avoir besoin.

Lorsqu’une personne se voit demander par l’ISC de communiquer un document ou une information en sa possession, cette personne peut soit répondre à la demande, soit informer l’ISC du fait que le document ou l’information en question ne peut être communiqué parce que le directeur général de l’organisme concerné juge qu’il s’agit d’une information délicate, au sens de l’ISA 2017. La divulgation d’une information de nature délicate n’est pas interdite dans les cas où le directeur général de l’organisme concerné estime que la divulgation peut être faite en toute sécurité. Les documents et informations de nature délicate doivent être communiqués à l’ISC dans les cas où le premier ministre estime que cette divulgation est souhaitable dans l’intérêt public.

Les délibérations de l’ISC sont des délibérations parlementaires aux fins de l’article 9 du *Bill of Rights 1688* (déclaration des droits de 1688) et de la *Parliamentary Privilege Act 2014* (loi sur le privilège parlementaire de 2014). Les réunions de l’ISC doivent être convoquées par le président. Elles doivent se dérouler conformément aux règles et aux pratiques de la Chambre des représentants. L’ISC tient ses réunions à huis clos, sauf lorsqu’il procède à un examen financier annuel ou dans les cas où le contraire est décidé à l’unanimité.

L’ISC doit présenter au Parlement un rapport annuel sur ses activités, tout en tenant compte de manière générale des exigences en matière de sécurité. La Chambre peut demander à l’ISC de lui remettre une copie d’une partie ou de l’ensemble de ses documents, y compris les rapports, les éléments de preuve et les conseils fournis à l’ISC, qu’il détient en raison de l’exécution des quatre premières fonctions exposées ci-dessus. Avant de remettre une copie d’un document quelconque à la Chambre, l’ISC doit en supprimer toute information dont la divulgation à la Chambre est interdite.

L’ISC ne doit pas communiquer au Parlement un rapport contenant :

- toute information qui, si elle était rendue publique, pourrait porter atteinte au lien de confiance qui doit exister lorsqu’une information est communiquée sous le sceau de la confidentialité au gouvernement de la Nouvelle-Zélande :
  - par le gouvernement d’un autre pays ou tout organisme de ce gouvernement;
  - par une organisation internationale;

- toute information qui, si elle était rendue publique, pourrait menacer la sécurité d'une personne;
- toute information de nature délicate communiquée à l'ISC.

Sauf dans les cas où il existe des raisons impérieuses de le faire, dans l'intérêt public, l'ISC ne doit pas inclure dans un rapport qu'il présente au Parlement :

- l'identité de toute personne qui est ou a été agent, employé ou mandataire d'un organisme de renseignement et de sécurité, autre que le directeur général, ou toute information à partir de laquelle on pourrait raisonnablement déduire l'identité de cette personne;
- toute information qui, si elle était rendue publique :
  - porterait probablement atteinte à l'exercice continu des fonctions d'un organisme;
  - porterait probablement atteinte à la sécurité ou aux mesures de défense de la Nouvelle-Zélande, ou aux relations internationales qu'entretient le gouvernement de la Nouvelle-Zélande.

c. Composition et nomination

L'ISC doit compter de cinq à sept membres, et le nombre est déterminé par le premier ministre, qui consulte le chef de l'opposition. L'ISC doit compter parmi ses membres :

- le premier ministre;
- le chef de l'opposition;
- des parlementaires proposés par le chef de l'opposition, avec l'accord du premier ministre, après consultation du chef de chaque parti qui ne siège pas au gouvernement ou n'appartient pas à la coalition du parti au pouvoir;
- des parlementaires proposés par le premier ministre après consultation du chef de chaque parti siégeant au gouvernement.

Si l'ISC compte cinq membres, un de ces membres doit être proposé par le chef de l'opposition, et deux, par le premier ministre. S'il compte six ou sept membres, deux membres doivent être proposés par le chef de l'opposition, les autres étant proposés par le premier ministre. Au moment de procéder aux mises en candidature, le chef de l'opposition et le premier ministre doivent tenir compte des exigences en matière de sécurité et de la représentation proportionnelle des partis politiques siégeant au Parlement. Dans l'exercice de ses fonctions de membre de l'ISC, un membre agit en sa capacité officielle de parlementaire.

Le premier ministre doit soumettre à l'approbation de la Chambre le nom des candidats. Si la Chambre refuse une mise en candidature, le premier ministre doit proposer le nom d'un autre membre, proposé par le chef de l'opposition ou le premier ministre, selon le cas, et obtenir son approbation.

L'ISC est présidé par le premier ministre ou, de temps à autre, par un autre membre de l'ISC désigné par le premier ministre.

d. Ressources

L'ISC peut compter dans la conduite de ses activités sur le soutien d'agents nommés par le dirigeant principal du ministère du Premier ministre et du Cabinet, avec l'accord de l'ISC.

E. Surveillance par un organisme indépendant

1. Inspector-General of Intelligence and Security

Le poste d'IGIS est une charge indépendante créée par une loi. Ni le ministre responsable d'un organisme de renseignement et de sécurité, ni le premier ministre ni aucun ministre ne donne à l'IGIS d'orientation concernant la façon dont il doit s'acquitter de ses responsabilités. L'IGIS supervise le NZSIS et le GCSB. Mais l'IGIS n'a aucune compétence sur les fonctions relatives au renseignement et à la sécurité d'autres organismes, notamment le National Assessments Bureau, les services de renseignement des forces armées de la Nouvelle-Zélande, et les unités du renseignement d'Immigration New Zealand, du service des douanes et de la police nationale[183].

La charge d'IGIS a été créée en vertu de l'*Inspector-General of Intelligence and Security Act 1996* (loi sur l'inspecteur général du renseignement et de la sécurité de 1996). Cette nouvelle charge a remplacé celle du Commissioner of Security Appeals (commissaire aux appels relatifs à la sécurité), dont le rôle consistait à mener des enquêtes sur des plaintes relatives au NZSIS. Les compétences de la nouvelle charge ont été étendues au GCSB, et les enquêtes et examens ont été intégrés à ses fonctions. Jusqu'en 2013, cette charge devait être confiée à un ancien juge de la Cour suprême, qui l'occupait à temps partiel[184].

Les changements apportés en 2013 visaient à renforcer le rôle de l'IGIS. Des dispositions prévoyaient la nomination d'un inspecteur général adjoint du renseignement et de la sécurité et une augmentation de son effectif. Un conseil consultatif a été mis sur pied pour conseiller l'IGIS, qui n'était plus nécessairement un ancien juge[185]. L'ISA 2017 supprime l'interdiction pour l'IGIS de mener des enquêtes sur des questions opérationnelles de nature délicate et précise que le titulaire peut examiner les mandats sur des questions de fond de même que sur des motifs procéduraux[186].

a. Fonctions

L'IGIS exerce les fonctions suivantes :

- à la demande du ministre responsable, de l'ISC ou de son propre chef, mener une enquête sur les questions suivantes :
  - toute affaire liée au respect, par un organisme de renseignement et de sécurité, des lois de la Nouvelle-Zélande, y compris les lois sur les droits de la personne;
  - toute affaire permettant de croire qu'une personne de la Nouvelle-Zélande a été ou pourrait être lésée par un acte, une omission, une pratique, une politique ou une procédure d'un organisme;
- à la demande du premier ministre, du ministre responsable, de l'ISC ou de son propre chef, mener une enquête sur le sujet suivant :
  - le caractère approprié d'activités d'un organisme;

183 Office of the Inspector-General of Intelligence and Security, *Annual report for the year ended 30 June 2016*, p. 3 et 4.

184 *Ibid.*, p. 1, 3 et 4; Inspector-General of Intelligence and Security (IGIS), *Annual report 1997*, p. 2.

185 Office of the Inspector-General of Intelligence and Security, *Annual report for the year ended 30 June 2014*, p. 9.

186 Les articles 157 à 191 et l'article 222 ainsi que les articles 6 à 12 de l'annexe 3 de l'ISA 2017, en particulier, s'appliquent à l'inspecteur général du renseignement et de la sécurité.

- traiter les plaintes concernant un organisme déposées par :
  - une personne de la Nouvelle-Zélande;
  - un employé ou un ancien employé d'un organisme, lorsque tous les recours internes prévus ont été épuisés ou lorsque le directeur général de l'organisme concerné donne son accord par écrit;
  - le Président de la Chambre des représentants au nom d'au moins un parlementaire;
- effectuer des examens au moins tous les ans ainsi que des vérifications impromptues de l'efficacité et du caractère approprié :
  - des procédures mises en œuvre par chaque organisme pour assurer le respect de l'ISA 2017, pour tout ce qui concerne l'obtention et l'exécution d'une autorisation;
  - les systèmes de conformité de chaque organisme en ce qui concerne les activités opérationnelles;
- de son propre chef, examiner toute activité d'un organisme menée dans le cadre de ses fonctions en vue de collaborer avec une entité qui intervient en cas de menace imminente pour la vie ou la sécurité;
- effectuer un examen relativement à une autorisation et/ou à l'exécution d'une activité autorisée;
- effectuer des examens des permissions accordées pour donner accès à des renseignements à diffusion restreinte ainsi que des approbations accordées pour obtenir des documents commerciaux d'opérateurs de réseau de télécommunications et de fournisseurs de services financiers;
- préparer, publier et mettre en œuvre un programme de travail annuel.

b. Pouvoirs et exercice des fonctions

Au moment de mener une enquête, l'IGIS dispose des pouvoirs suivants :

- convoquer et interroger sous serment toute personne que l'IGIS juge capable de fournir des renseignements pertinents;
- exiger que toute personne fournisse toute information, tout document ou toute chose en sa possession ou sur lesquels cette personne exerce un contrôle, que l'IGIS considère possiblement pertinents;
- à tout moment raisonnable et après avoir donné un préavis au directeur général de l'organisme, pénétrer dans des installations ou des lieux occupés ou utilisés par un organisme de renseignement et de sécurité.

Au moment de mener une enquête ou de procéder à un examen, l'IGIS doit tenir compte de tout énoncé de politique ministériel fournissant une orientation à l'organisme et de la mesure dans laquelle cet organisme a tenu compte de cet énoncé.

À la fin d'une enquête, l'IGIS prépare un rapport où il expose ses conclusions et recommandations. Si l'enquête concernait une plainte, le rapport peut comprendre des recommandations visant à remédier à la plainte, y compris le paiement d'un dédommagement.

L'IGIS doit envoyer son rapport au ministre responsable ainsi qu'au directeur général de l'organisme concerné par l'enquête. Le rapport doit aussi être envoyé au premier ministre, dans le cas où l'enquête a été menée à la demande du premier ministre, ou à l'ISC, si l'enquête a été menée à sa demande.

L’IGIS peut également envoyer un rapport d’enquête à l’ISC dans les cas suivants :

- l’enquête a été menée du propre chef de l’IGIS ou à la demande du ministre responsable, et le ministre responsable est d’accord;
- l’enquête a été menée à la demande du premier ministre, et le premier ministre est d’accord.

Le ministre responsable doit communiquer sa réponse au rapport à l’IGIS et au directeur général de l’organisme concerné. Si l’enquête a été menée à la demande de l’ISC, le ministre doit également fournir sa réponse à l’ISC, et il peut aussi le faire si l’enquête n’a pas été menée à la demande de l’ISC.

Dans le cas où l’enquête concernait une plainte, l’IGIS doit communiquer ses conclusions au plaignant en les formulant de manière à ne pas porter atteinte à la sécurité ou à la défense de la Nouvelle-Zélande ni aux relations internationales du gouvernement.

Le rapport d’enquête doit également être publié sur le site Internet de l’IGIS. Certaines restrictions s’appliquent à la divulgation de certaines informations.

L’IGIS doit présenter un rapport annuel portant sur ses activités à chacun des ministres responsables et au premier ministre. Le premier ministre doit soumettre ce rapport au Parlement, accompagné d’une déclaration précisant si des questions qui en ont été exclues. Le premier ministre doit également communiquer au chef de l’opposition un exemplaire du rapport reçu de l’IGIS. L’IGIS doit publier le rapport, tel qu’il a été communiqué au Parlement, sur Internet. L’IGIS peut en tout temps, avec l’accord du premier ministre, fournir un compte rendu de portée générale ou sur un sujet particulier à l’ISC.

c. Nomination

L’IGIS est nommé par le gouverneur général sur recommandation de la Chambre des représentants. Avant qu’une recommandation soit faite, le premier ministre doit consulter l’ISC à propos de cette nomination et informer la Chambre des résultats de la consultation. L’IGIS est nommé pour un mandat d’au plus cinq ans et peut obtenir un second mandat d’au plus trois ans.

L’IGIS peut être démis ou suspendu de ses fonctions par le gouverneur général, sur intervention de la Chambre des communes, pour incapacité, faillite, manquement à son devoir, inconduite ou défaut de détenir une habilitation de sécurité appropriée.

d. Ressources

En juin 2016, le bureau de l’IGIS était composé de l’inspecteur général, de l’inspecteur général adjoint et de six employés, y compris quatre enquêteurs[187].

Les dépenses totales prévues pour 2015-2016 s’élevaient à 1 498 000 $, soit environ un pour cent du budget prévu du NZSIS et du GCSB[188].

187 IGIS, *Annual report*, 2016, p. 4.

188 *Ibid.*, p. 32.

F. Surveillance judiciaire

1. Commissaires aux mandats de renseignement

Les demandes de délivrance d'un mandat de renseignement doivent être présentées par le directeur général de l'organisme concerné au ministre ayant le pouvoir de l'autoriser, c'est-à-dire le ministre responsable de l'organisme, dans le cas d'un mandat de type 2, et au ministre qui peut l'autoriser et à un commissaire aux mandats de renseignement dans le cas d'un mandat de type 1[189].

Un mandat de type 1 autorise un organisme à mener une activité qui serait autrement illégale dans le but de recueillir de l'information au sujet d'un citoyen ou d'un résident permanent de la Nouvelle-Zélande ou de faire toute autre chose qui soit directement liée à cette personne. Un mandat de type 2 autorise un organisme à mener une activité qui serait autrement illégale dans le but de recueillir de l'information, ou de faire toute autre chose, dans les cas où un mandat de type 1 n'est pas requis.

Sur recommandation du premier ministre, le gouverneur général peut nommer jusqu'à trois commissaires aux mandats de renseignement, dont un sera le commissaire en chef. Avant de présenter sa recommandation, le premier ministre doit consulter le chef de l'opposition au sujet de la nomination proposée. Les commissaires aux mandats de renseignement doivent avoir déjà occupé un poste de juge à la Cour suprême[190].

Les commissaires exercent les fonctions suivantes :

- examiner les demandes de mandat de renseignement de type 1, conseiller le ministre responsable sur ces demandes et en discuter avec lui;
- délivrer des mandats de type 1 avec le ministre;
- examiner avec le ministre les demandes de permission d'accès à des informations à diffusion restreinte, par exemple les photographies des permis de conduire, les renseignements fiscaux ou relatifs à une adoption, et les numéros d'identification nationaux des étudiants tertiaires;
- examiner avec le ministre les demandes d'approbation pour l'obtention de documents commerciaux d'opérateurs de réseaux de télécommunications et de fournisseurs de services financiers;
- effectuer un examen sur avis du directeur général du GCSB selon lequel il existe ou pourrait exister un risque important pour la sécurité des réseaux de télécommunications publics;
- effectuer un examen des décisions ministérielles de refuser de délivrer un passeport ou un document de voyage néo-zélandais, ou d'annuler ou de saisir ce document.

Le ministre qui peut l'autoriser peut, s'il est convaincu que la situation est urgente et qu'il est nécessaire de le faire, délivrer un mandat de type 1 sans en aviser un commissaire. Un tel mandat expirera après 48 heures, sauf si une demande de mandat a été présentée selon les procédures normales et que le ministre ainsi qu'un commissaire confirment que le mandat de renseignement est urgent. Au moment de délivrer un mandat de renseignement urgent, le ministre qui peut l'autoriser doit immédiatement aviser le commissaire en chef aux mandats de renseignement, qui pourra révoquer le mandat à tout moment pendant la période de validité de 48 heures.

189 Les articles 52 à 84 de l'ISA 2017, en particulier, s'appliquent aux mandats de renseignement.

190 Les articles 112 à 117 ainsi que les articles 1 à 5 de l'annexe 3 de l'ISA 2017, en particulier, s'appliquent aux commissaires aux mandats de renseignement.

ROYAUME-UNI

A. Aperçu des organismes de renseignement

Le Royaume-Uni compte trois services chargés du renseignement et de la sécurité, collectivement appelés « the Agencies[191] ». Il s'agit :

- du Secret Intelligence Service[192] (service secret du renseignement [SIS], souvent appelé MI6), chargé de la collecte de renseignements étrangers secrets;
- du Security Service[193] (service de sécurité, souvent appelé MI5), chargé de protéger le Royaume-Uni contre les menaces pour la sécurité nationale organisées en secret;
- du Government Communications Headquarters[194] (quartier général des communications du gouvernement [GCHQ]), chargé de recueillir des renseignements par l'interception de communications.

De plus, certains ministères abritent des organismes faisant partie de ce qu'on appelle le *national intelligence machinery*[195] (appareil national de renseignement). Il s'agit des organismes suivants :

- La Defence Intelligence (service du renseignement de défense), est un organisme faisant partie intégrante du ministère de la Défense. L'organisme mène diverses activités liées au renseignement, notamment la prestation de produits, d'évaluations et de conseils afin d'orienter des décisions sur les politiques et les missions des forces armées, d'éclairer les décisions relatives à la recherche et à l'équipement pour la défense, et de soutenir des opérations militaires.
- Le National Security Secretariat (secrétariat de la sécurité nationale), établi au Cabinet Office (bureau du Cabinet) appuie le National Security Council (conseil de la sécurité nationale [NSC]) en assurant la coordination, à l'échelle du gouvernement, des dossiers liés à la sécurité et au renseignement d'importance stratégique. Le NSC est la tribune principale pour la discussion collective des objectifs du gouvernement en matière de sécurité nationale. Le dirigeant du secrétariat du NSC, le National Security Adviser (conseiller à la sécurité nationale), est chargé de conseiller le premier ministre.
- Le Joint Intelligence Committee (comité mixte du renseignement [JIC]), est soutenu par la Joint Intelligence Organisation (organisation mixte du renseignement) et fait également partie du Cabinet Office. Le JIC est chargé d'évaluer les renseignements bruts recueillis par les Agencies et de les présenter aux ministres afin d'éclairer les décisions d'ordre stratégique.
- L'Office of Security and Counter-Terrorism (bureau de la sécurité et du contre-terrorisme) est une unité faisant partie du Home Office (ministère de l'Intérieur).
- Le Joint Terrorism Analysis Centre (centre commun d'analyse du terrorisme [JTAC]) est une organisation constituée de représentants de 16 ministères et organismes du gouvernement. Le centre se trouve au siège du MI5. Le JTAC analyse et évalue tous les renseignements concernant le terrorisme international. Il décide du niveau de menace et lance des avertissements relatifs aux menaces et à d'autres points d'intérêt liés au terrorisme. Il produit également des rapports détaillés sur les tendances, les réseaux terroristes et les capacités. Le JTAC rassemble l'information obtenue de la police et des ministères et organismes du gouvernement pour qu'elle soit analysée et traitée conjointement.

---

191 Les trois organismes sont appelés les « intelligence agencies » dans la législation, par exemple à l'article 263 de l'*Investigatory Powers Act 2016.*

192 *Intelligence Services Act 1994* (ISA 1994), art. 1.

193 *Security Service Act 1989*, art. 1.

194 ISA 1994, art. 3.

195 Pour de plus amples renseignements, consultez les sites Gov.uk et Mi5.gov.uk (consultés le 28 mars 2017).

B. Surveillance : résumé

Au sein du gouvernement, le premier ministre est responsable de l'ensemble des questions ayant trait à la sécurité. Le Home Secretary (ministre de l'Intérieur) est responsable du Security Service; le Foreign and Commonwealth Secretary (ministre des Affaires étrangères et du Commonwealth) est responsable du SIS et du GCHQ; et le Defence Secretary (ministre de la Défense) est responsable du personnel de la Defence Intelligence. Le Parlement a toujours exercé une certaine surveillance des Agencies, dans la mesure où les ministres responsables des divers services de renseignement doivent rendre des comptes au Parlement.

Les activités quotidiennes des Agencies sont supervisées par les chefs de ces organismes. La loi prévoit que chaque chef doit produire annuellement des rapports à l'intention du premier ministre et des ministres respectifs.

Les comptes des Agencies sont soumis à des vérifications par le National Audit Office (bureau national de vérification). Ils sont également communiqués au président du Public Accounts Committee (comité des comptes publics). Les comptes ne sont pas publiés pour des raisons de sécurité nationale. Cependant, l'état financier de l'instrument de financement des Agencies, le Single Intelligence Account, est publié une fois par année[196].

L'*Intelligence Services Act 1994* (loi de 1994 sur les services de renseignement [ISA 1994]) a donné une base législative au SIS et au GCHQ et a établi l'Intelligence and Security Committee (comité du renseignement et de la sécurité [ISC]). Les membres de l'ISC sont proposés par le premier ministre et nommés par le Parlement, auquel l'ISC rend des comptes. L'ISC a pour fonction d'examiner les dépenses, l'administration, les politiques et les activités des trois principaux organismes de renseignement et de sécurité du Royaume-Uni. À cette fin, ses membres utilisent les données fournies par les ministres et d'autres hauts fonctionnaires afin de produire les rapports du comité. Les membres de l'ISC sont assujettis à l'alinéa 1(1)b) de l'*Official Secrets Act 1989* (loi de 1989 sur les secrets officiels) et ont accès à des documents hautement confidentiels dans le cadre de leur travail[197].

À la suite de l'adoption de la *Justice and Security Act 2013* (loi de 2013 sur la justice et la sécurité [JSA]), l'ISC est devenu un comité parlementaire, ce qui a élargi ses pouvoirs et son mandat. À l'origine, l'ISC était chargé de surveiller le MI5, le MI6 et le GCHQ. À présent, l'ISC s'intéresse également aux activités de la Defence Intelligence et du JIC, ainsi qu'à celles d'organismes d'application de la loi (la police et les douanes et l'accise).

En plus des fonctions ministérielles de nature générale liées aux Agencies, les ministres jouent un rôle précis dans la délivrance de mandats pour certaines activités, par exemple l'interception et l'effraction informatique[198]. On soutient que cela est nécessaire, vu que les ministres doivent rendre des comptes au sujet de leurs décisions autant au Parlement qu'au public et parce que, pour délivrer un mandat, il faut faire preuve de jugement politique dans le contexte de questions de nature délicate liées à la sécurité nationale et à la politique étrangère.

---

196 Voir *Security and Intelligence Agencies: Financial Statement 2015–16*, HC 363, juillet 2016.

197 En vertu de l'alinéa 1(1)b), la divulgation non autorisée de renseignements classifiés constitue une infraction.

198 Présentement, cela est prévu dans la *Regulation of Investigatory Powers Act 2000* et l'*Intelligence Services Act 1994*. L'*Investigatory Powers Act 2016*, récemment adoptée, aura pour effet de réviser la procédure en introduisant une « protection double » par laquelle le ministre compétent devra approuver le mandat, suivi d'un examen par un commissaire judiciaire, avant que le mandat puisse être exécuté.

L'Investigatory Powers Commissioner (commissaire aux pouvoirs d'enquête [IPC]) est chargé d'exercer une surveillance indépendante de l'utilisation de pouvoirs intrusifs par les Agencies. Le commissaire présente un rapport annuel au premier ministre qui est ensuite publié et présenté au Parlement après avoir été caviardé[199].

Enfin, les plaintes relatives à l'utilisation illégale de techniques secrètes par les autorités publiques font l'objet d'une enquête avant d'être jugées par l'Investigatory Powers Tribunal (tribunal des pouvoirs d'enquête [IPT]). Le tribunal a été établi en octobre 2000 en vertu de la *Regulation of Investigatory Powers Act 2000* (loi de 2000 sur la réglementation des pouvoirs d'enquête [RIPA]) afin de donner un droit de recours à toute personne croyant avoir été victime d'une activité illégale sous le régime de la RIPA ou d'une violation plus générale des droits de la personne à la suite de la violation de la *Human Rights Act 1998* (loi de 1998 sur les droits de la personne).

C. Faits nouveaux

L'*Investigatory Powers Act 2016* (loi de 2016 sur les pouvoirs d'enquête [IPA]) a regroupé, justifié et, dans certains cas, étendu les pouvoirs d'enquête des Agencies, de la police et d'autres organismes d'application de la loi[200]. Une fois son entrée en vigueur complète, la loi aura pour effet d'apporter un certain nombre de modifications importantes aux mécanismes de surveillance, y compris :

- l'introduction de contrôles judiciaires relativement à l'émission des mandats;
- la refonte du régime de surveillance indépendante afin qu'un seul Investigatory Powers Commissioner soit responsable de l'utilisation de pouvoirs d'enquête par les Agencies;
- la création d'un droit d'appel d'une décision de l'Investigatory Powers Tribunal.

D. Surveillance parlementaire

1. Intelligence and Security Committee

a. Fonctions

L'ISC est chargé de surveiller les dépenses, l'administration, les politiques et les activités des trois organismes de renseignement. Il est également habilité à examiner ou à surveiller d'autres dossiers relatifs au renseignement et à la sécurité, conformément aux protocoles d'entente conclus entre le premier ministre et l'ISC.

L'ISC est habilité à examiner des questions opérationnelles seulement dans les cas suivants :

- Il n'y a pas de lien avec des opérations en cours et c'est dans l'intérêt national.
- Le premier ministre en a fait la demande.
- L'examen porte uniquement sur l'information fournie volontairement par les Agencies ou les ministères.

---

199 Pour de plus amples renseignements, consultez le site Web de l'Investigatory Powers Commissioner's Office.

200 Pour plus de renseignements contextuels à propos de l'IPA, consultez les documents d'information de la Bibliothèque de la Chambre des communes suivants : CBP 7371 *Draft investigatory Powers Bill*, 19 novembre 2015; CBP 7518 *Investigatory Powers Bill*, 11 mars 2016; CBP 7578 *Investigatory Powers Bill: Committee Stage Report*, 2 juin 2016; CBP 7746 *Investigatory Powers Bill: Lords amendments*, 28 octobre 2016.

b. Pouvoirs et exécution des fonctions

L'annexe 1 de la JSA établit les pouvoirs de l'ISC relativement à l'accès à l'information et à d'autres questions. L'ISC peut demander aux dirigeants des trois Agencies de lui divulguer de l'information. Les organismes doivent rendre l'information accessible à l'ISC, sauf dans les cas où le ministre y a opposé son veto. Il en va de même pour l'information demandée aux ministères.

Le ministre est autorisé à opposer son veto à la divulgation d'information seulement dans les deux cas suivants :

- Il s'agit d'information de nature délicate qui ne doit pas être divulguée à l'ISC dans l'intérêt de la sécurité nationale.
- La nature de l'information fait qu'il serait inapproprié pour le ministre d'accéder à une demande de divulgation de l'information devant un comité spécial ministériel de la Chambre des communes (pour des motifs ne se limitant pas à la sécurité nationale). Quand il prend sa décision, le ministre doit tenir compte des lignes directrices gouvernementales concernant la divulgation de renseignements par des fonctionnaires aux comités spéciaux[201].

Auparavant, les dirigeants des Agencies pouvaient refuser de divulguer de l'information s'ils jugeaient que les renseignements étaient de nature délicate.

Conformément au paragraphe 5 de l'annexe 1 de la JSA, un renseignement est jugé de nature délicate dans les cas suivants :

- Il pourrait permettre d'identifier une source d'information ou pourrait comprendre des détails sur cette source, d'autre aide, ou le fonctionnement opérationnel des Agencies ou d'autres éléments de l'appareil de renseignement.
- Il comprend de l'information à propos d'opérations actuelles ou futures.
- Il comprend de l'information provenant d'un pays dont le gouvernement n'a pas consenti à la divulgation.

Les renseignements fournis par des témoins à l'ISC ne peuvent pas être utilisés dans le cadre d'actions civiles, disciplinaires ou pénales, à moins que l'information n'ait été fournie de mauvaise foi.

L'ISC doit présenter un rapport annuel au Parlement sur l'exercice de ses fonctions. Il peut également produire d'autres rapports s'il le juge approprié.

Les Agencies peuvent demander que les renseignements de nature délicate soient caviardés dans les rapports dans le cas où leur divulgation pourrait nuire à leurs activités, par exemple si cela serait susceptible de révéler leurs cibles, leurs méthodes, leurs sources ou leurs capacités opérationnelles.

c. Composition et nomination

Conformément à l'article 1 de la JSA, la Chambre du Parlement appropriée (la Chambre des communes ou la Chambre des lords) nomme les membres de l'ISC, qui ont été proposés par le premier ministre.

La composition actuelle de l'ISC se trouve sur le site Web.

---

201 Cabinet Office, *Giving evidence to select committees: guidance for civil servants*, octobre 2014.

Le président du comité est élu par les membres. Dominic Grieve, c.r., un ex-procureur général, est le président actuel du comité.

Les membres siègent à l'ISC pour la durée de la législature durant laquelle ils ont été nommés. Un membre peut toutefois être destitué par résolution de la Chambre qui l'a nommé, ou s'il cesse d'être député ou devient ministre. Les membres ont également la possibilité de démissionner de leur propre gré.

d. Ressources

Depuis que la JSA a fait de l'ISC un « comité parlementaire », la responsabilité de fournir des ressources incombe principalement au Parlement. Cependant, une disposition a été ajoutée à la JSA afin que le gouvernement fournisse des fonds supplémentaires. Le paragraphe 3 de l'annexe 1 prévoit qu'un ministre de la Couronne peut :

- faire des paiements à l'une ou l'autre des Chambres du Parlement relativement à toute dépense engagée par l'ISC;
- fournir du personnel, des installations ou d'autres ressources, soit directement à l'ISC ou par l'intermédiaire du Parlement.

Selon le rapport annuel de 2015-2016, l'ISC est soutenu actuellement par quatre employés de base, six employés affectés à une enquête particulière[202] et un enquêteur à temps partiel. Le budget de base de l'ISC a été fixé à 1,3 million de livres, conformément à l'accord conclu avec le ministre des Affaires étrangères au nom du NSC. Ce montant exclut toutefois la sécurité, les TI, les télécommunications, la publication de rapports, les installations, les services publics (eau, gaz, électricité, etc.) et les services organisationnels centralisés. Ces services sont actuellement fournis par le National Security Secretariat et le Cabinet Office[203].

E. Surveillance par un organisme indépendant

L'IPA prévoit l'élimination du régime de surveillance indépendante, comprenant l'Intelligence Services Commissioner (commissaire aux services du renseignement), l'Interception of Communications Commissioner (commissaire à l'interception des communications) et le Surveillance Commissioner (commissaire à la surveillance). Le nouveau poste d'Investigatory Powers Commissioner (commissaire aux pouvoirs d'enquête [IPC]) remplace ces trois postes. Le premier IPC, le juge Fulford de la Chambre des lords, vient d'être nommé pour un mandat de trois ans[204].

L'IPC et certains commissaires judiciaires sont nommés par le premier ministre sur recommandation du grand chancelier, du lord juge en chef d'Angleterre et du pays de Galles, du lord président de la Court of Session et du lord juge en chef de l'Irlande du Nord. Le premier ministre doit également consulter les ministres écossais.

---

202 Il s'agit d'une enquête sur le rôle des organismes dans le traitement et la restitution des détenus. Il a été décidé, au lancement de l'enquête, qu'elle serait financée par le gouvernement.

203 Intelligence and Security Committee of Parliament, *Annual Report 2015–2016*, HC 444, juillet 2016.

204 Prime Minister's Office, *Investigatory Powers Commissioner appointed: Lord Justice Fulford*, communiqué, 3 mars 2017.

Ils seront tenus de surveiller, au moyen de vérifications, d'inspections et d'enquêtes, l'exercice par les autorités publiques de diverses fonctions statutaires, y compris en ce qui concerne[205] :

- l'interception de communications;
- l'acquisition ou la conservation de données de communication;
- l'effraction informatique;
- l'acquisition, la conservation et l'utilisation d'un grand nombre d'ensembles de données personnelles.

Conformément à l'article 230, le premier ministre peut également ordonner à l'IPC d'examiner d'autres fonctions des Agencies.

L'IPC devra présenter un rapport annuel au premier ministre. L'IPA décrit en détail ce que le rapport doit couvrir, soit :

- des statistiques sur l'utilisation de pouvoirs d'enquête;
- de l'information à propos des résultats ou de l'incidence de l'utilisation de pouvoirs d'enquête;
- de l'information à propos du fonctionnement des mesures de protection prévues dans l'IPA relativement aux éléments visés par le privilège juridique, aux documents journalistiques confidentiels et aux sources de matériel journalistique;
- de l'information sur l'utilisation de catégories précises de mandats.

Conformément à l'article 235, toute personne concernée doit fournir aux commissaires judiciaires les documents, l'information et l'aide nécessaires aux enquêtes, aux inspections ou aux vérifications. Une « personne concernée » peut être, entre autres, tout employé d'une autorité publique, ou un fournisseur de services de télécommunications ou de services postaux qui est visé par une exigence de l'IPA.

Le financement, les installations et le personnel de l'IPC sont prévus par l'article 238. Le ministre décide du financement à accorder en consultation avec l'IPC. Le ministère des Finances (Treasury) doit approuver le nombre des effectifs. Le salaire et les dépenses des commissaires judiciaires sont également fixés par le ministère des Finances.

F. Surveillance par le pouvoir exécutif

1. Mandats

Les ministres sont chargés de statuer sur les requêtes relatives à l'exécution de certaines activités des Agencies. Cela concerne ce qui suit :

- Les demandes de mandat en vertu de l'article 5 de l'ISA 1994, qui prévoit que le ministre compétent peut délivrer un mandat pour ingérence dans les biens ou la télégraphie sans fil si l'un des organismes de renseignement en fait la demande. La mesure autorisée par le mandat doit être nécessaire et proportionnelle à l'objectif du mandat.

---

[205] Article 229.

- Les autorisations en vertu de l'article 7 de l'ISA 1994, qui prévoit que le ministre peut autoriser le MI6 et le GCHQ à prendre des mesures en réaction à tout acte commis à l'extérieur des îles Britanniques qui aurait autrement entraîné des poursuites (au criminel ou au civil) aux îles Britanniques.
- Les demandes de mandat d'interception en vertu de l'article 5 de la RIPA, qui prévoit que le ministre peut délivrer un mandat pour certains motifs précis lorsque cela est nécessaire et proportionnel.

2. La doctrine Wilson

La convention qu'on appelle la doctrine Wilson prévoit que les organismes de renseignement n'intercepteront pas, en temps normal, les communications d'un député.

En 2015, l'IPT a rendu une décision dans une affaire dont l'a saisi Caroline Lucas, députée, et la baronne Jones de Moulsecoombe, à la suite de la divulgation de documents par Edward Snowden. Cette affaire concernait le statut, l'interprétation et l'effet de la doctrine Wilson[206].

Le tribunal a conclu que les Agencies doivent se conformer à leurs propres directives relativement à la doctrine, lesquelles ont été divulguées pour la première fois au cours des délibérations. Il est donc clair qu'il faut veiller tout particulièrement à déterminer si l'activité d'interception est nécessaire et proportionnelle. En outre, il faut consulter un conseiller juridique, le chef de la section des mandats et un agent principal des politiques. Le directeur général doit aussi en être informé. Avant de décider de délivrer ou non un mandat, le ministre doit consulter le premier ministre, par l'intermédiaire du secrétaire du Cabinet[207].

Les directives mentionnent également que la doctrine Wilson ne s'applique pas à l'interception des communications d'un député d'une administration dotée de compétences propres.

L'article 26 de l'IPA rendrait obligatoire, en vertu de la loi, d'obtenir l'autorisation du premier ministre. Il préciserait également qu'il s'applique aux députés du Parlement écossais, de l'Assemblée nationale du Pays de Galles, de l'Assemblée de l'Irlande du Nord et aux députés britanniques du Parlement européen.

G. Surveillance judiciaire

1. Mandats

Lorsque les dispositions en question entreront en vigueur, l'IPA introduira un niveau supplémentaire de contrôle judiciaire dans le processus d'émission des mandats aux Agencies.

Présentement, le ministre compétent est le seul responsable de l'octroi des mandats, comme cela a été décrit plus haut. Dans le cadre de la nouvelle procédure, les mandats pourront seulement être exécutés après avoir été examinés par un commissaire judiciaire.

---

206 [2015] UKIPTrib 14_79-CH.

207 Paragraphe 11 de la décision.

La nouvelle procédure s'appliquera aux mandats suivants :

- les mandats d'interception[208], y compris :
  - les mandats d'interception ciblée, qui autorisent l'interception ciblée de communications;
  - les mandats d'analyse ciblée, qui autorisent l'analyse ciblée du contenu d'un ensemble de données de communication;
  - les mandats d'aide mutuelle, qui autorisent les demandes ou la prestation d'aide mutuelle dans l'exécution de mandats dans lesquels les autorités d'un autre pays jouent un rôle;
- les mandats pour l'effraction informatique[209], y compris :
  - les mandats d'effraction ciblée;
  - les mandats d'analyse ciblée, qui sont applicables de la même façon que les mandats d'analyse ciblée pour l'interception;
- les mandats d'interception d'ensembles de données[210], qui autorisent l'interception d'ensembles de données de communications liées à l'étranger (de façon non ciblée);
- les mandats d'acquisition d'ensembles de données[211], qui autorisent l'accès à des ensembles de données de communications;
- les mandats d'effraction en masse[212], qui autorisent l'effraction visant un grand nombre d'appareils dans le but d'obtenir des communications, des données ou de l'information liées à l'étranger;
- les mandats relatifs aux ensembles de données personnelles[213], qui autorisent la conservation et l'analyse d'un grand nombre d'ensembles de données personnelles[214].

Les commissaires judiciaires doivent également approuver les décisions concernant le renouvellement ou la modification de ces genres de mandats.

Les commissaires judiciaires seront nommés en tant que membres du bureau de l'IPC. Ils doivent occuper ou avoir occupé de hautes fonctions judiciaires, et ils doivent examiner la décision du ministre à la lumière des principes qui seraient appliqués dans le cadre d'une demande de contrôle judiciaire.

---

208 Article 15.

209 Article 99. Les mandats pour l'effraction informatique autorisent l'effraction dans le but d'obtenir des communications ou certaines données.

210 Article 136.

211 Article 158.

212 Article 176.

213 Articles 204 et 205.

214 Les ensembles de données personnelles sont des ensembles de données, y compris des données personnelles, sur plus d'une personne, la majorité desquelles ne sont pas des personnes d'intérêt selon les services de renseignement.

Ces modifications ont soulevé une importante controverse lorsque le projet de loi a été présenté au Parlement. Les questions suivantes en particulier ont été soulevées pendant les débats[215] :

- Si l'autorisation politique ou l'autorisation judiciaire est plus appropriée dans ce contexte. Certains des participants aux débats étaient d'avis que la tâche de délivrer des mandats convient le mieux à des juges indépendants, qui ont l'habitude d'examiner les genres de facteurs pertinents pour rendre ce genre de décision et qui veilleraient à ce que le processus ait une apparence d'impartialité. Il a été reconnu que les ministres devraient jouer un rôle dans l'octroi des mandats dans les affaires comprenant d'importantes considérations liées à la politique étrangère et exigeant des décisions qui sont plus nettement d'ordre politique. D'autres ont soutenu que les juges ne sont pas les mieux placés pour évaluer l'importance des questions de sécurité nationale pour prendre des décisions sur ce genre d'affaires et qu'il était important de pouvoir rendre des comptes au Parlement par l'intermédiaire des ministres.
- Jusqu'à quel degré les commissaires judiciaires doivent approfondir leurs contrôles. L'IPA exige que les commissaires judiciaires examinent la décision du ministre en appliquant les mêmes normes que celles qui s'appliqueraient à un contrôle judiciaire. Il y a eu de nombreux débats sur ce que cela suppose en pratique. Certaines personnes ont soutenu que le contrôle judiciaire ne nécessiterait que l'examen du processus officiel par lequel la décision a été rendue, et que cela n'était pas suffisant. D'autres ont fait valoir que les normes relatives au contrôle judiciaire permettraient d'examiner le « bien-fondé » de la décision dans son ensemble et que le critère était donc suffisant. Le projet de loi a été modifié de façon à ce qu'il soit clair que, dans le cadre de l'examen de la décision d'un ministre, un commissaire judiciaire doit examiner la nécessité et la proportionnalité du mandat de façon suffisamment approfondie pour s'acquitter des obligations prévues à l'article 2 de l'IPA afin de protéger la vie privée des gens.
- L'impartialité des commissaires judiciaires. On a soulevé des questions concernant le rôle du premier ministre dans la nomination et la révocation des commissaires judiciaires, et le fait que cela pourrait avoir une incidence sur leur indépendance réelle ou apparente. Un autre conflit d'intérêts potentiel a été cerné dans le fait que les commissaires judiciaires jouent un rôle double, soit celui d'approuver directement les mandats et celui de surveiller et de vérifier de façon générale l'exercice des pouvoirs relatifs au processus d'émission des mandats.

2. Investigatory Powers Tribunal

La RIPA a établi l'IPT et l'a habilité à enquêter sur les plaintes relatives à l'utilisation de pouvoirs d'enquête par des organismes publics[216].

Les procédures de l'IPT font que la plupart de ses activités se déroulent en secret, car on estime que cela est nécessaire pour assurer la confiance et la coopération des Agencies.

Cependant, l'IPT s'est attiré certaines critiques. On lui a reproché d'être indûment opaque et inéquitable sur le plan procédural.

En réaction à certaines de ces critiques, l'IPA prévoit un droit d'appel sur une question de droit tranchée par l'IPT, devant la Court of Appeal (cour d'appel) en Angleterre et au Pays de Galles, ou la Court of Session en Écosse.

---

215 Pour de l'information contextuelle sur l'adoption du projet de loi au Parlement, consultez les documents d'information suivants de la Bibliothèque de la Chambre des communes : CBP 7371 *Draft investigatory Powers Bill*, 19 novembre 2015; CBP 7518 *Investigatory Powers Bill*, 11 mars 2016; CBP 7578 *Investigatory Powers Bill: Committee Stage Report*, 2 juin 2016; CBP 7746 *Investigatory Powers Bill: Lords amendments*, 28 octobre 2016.

216 L'article 65 de la *Regulation of Investigatory Powers Act 2000* établit la compétence du tribunal.

L’autorisation d’interjeter appel doit être accordée par l’IPT ou la cour d’appel, au motif qu’une question de principe ou de pratique importante serait soulevée, ou qu’il existe une autre raison convaincante.

Cette disposition n’est pas encore entrée en vigueur, et, à l’heure actuelle, il n’existe aucun moyen d’interjeter appel au Royaume-Uni à l’égard d’une décision de l’IPT. Par conséquent, les demandeurs doivent interjeter appel devant la Cour européenne des droits de l’homme.

H. Coopération

Actuellement, il existe un certain nombre de mécanismes de coopération entre les organismes de surveillance. Par exemple, l’Investigatory Powers Commissioner’s Office (bureau de l’IPC) a le devoir d’acquiescer à toute demande d’aide émise par l’IPT en lien avec une affaire, que ce soit pour l’enquête, pour l’analyse ou pour la décision. Cela peut comprendre l’opinion du commissaire sur toutes les affaires dont l’IPT est saisi, c’est-à-dire que le tribunal peut tirer profit de l’expertise du commissaire dans la prise de décisions[217].

L’IPA comprend un certain nombre de dispositions dont l’objectif est de faciliter la coopération encore plus, soit ce qui suit :

- L’article 230 prévoit que l’ISC peut demander au premier ministre d’ordonner à l’IPC de surveiller un nouveau domaine d’activité.
- En vertu de l’article 231, l’IPC doit avertir les personnes concernées lorsque des erreurs graves ont été commises dans l’utilisation des pouvoirs d’enquête, pourvu que cela soit dans l’intérêt du public. La personne concernée doit également être avisée du fait qu’elle a le droit de déposer une plainte devant l’IPT et doit également être mise au courant des détails nécessaires pour le dépôt de la plainte.
- L’article 236 s’applique à une situation où l’ISC découvre quelque chose qui devrait faire l’objet d’une enquête approfondie, mais pour laquelle il n’a pas la compétence. L’ISC doit alors déléguer l’affaire à l’IPC. Par la suite, l’IPC doit dire à l’ISC si d’autres mesures doivent être prises.

---

217 Article 232, *Investigatory Powers Act 1016*.

ANALYSE COMPARATIVE

Sauf indication contraire, la présente section du document est fondée sur les renseignements fournis plus haut au sujet des mécanismes de surveillance en place en Australie, au Canada, en Nouvelle-Zélande et au Royaume-Uni.

Comme cela a été mentionné précédemment, le Congressional Research Service n'a pas été en mesure de participer à la production du présent document. Par conséquent, il n'y a aucune section concernant les États-Unis en particulier dans le document. Toutefois, la présente section comprend de l'information sur les mécanismes en place aux États-Unis basée sur des recherches effectuées par Cat Barker et Samantha Godec.

A. La « communauté du renseignement »

Il existe des similitudes notables entre les communautés du renseignement du Groupe des cinq en ce qui a trait à la compétence, aux fonctions et aux règles.

- Les cinq pays ont des organismes responsables du **renseignement électromagnétique**.
- Chaque pays a un ou des organismes responsables de recueillir des **renseignements de sécurité**.
- Chaque pays a un organisme chargé du **renseignement militaire**, sous une forme ou une autre.
- Tous les pays ont des organismes spécialisés ou des capacités particulières en matière de **renseignement géospatial**.
- Chaque pays a un bureau ou un organisme responsable de **l'analyse toutes sources** afin d'analyser l'information provenant de l'ensemble de l'appareil gouvernemental.

Néanmoins, il y a des différences quant aux organismes qui sont considérés comme faisant partie de la communauté du renseignement.

- La communauté du renseignement de l'**Australie** est actuellement composée de six organismes responsables du renseignement de défense, du renseignement électromagnétique, du renseignement étranger, du renseignement géospatial et du renseignement de sécurité, ainsi que d'un organisme général d'évaluation national[218].
- Au **Canada**, la communauté du renseignement n'est pas distincte de l'ensemble de la communauté de la sécurité nationale, dont les organismes principaux sont responsables du renseignement de sécurité, du renseignement électromagnétique et du renseignement de défense ainsi que de l'application des lois nationales. Le Canada ne possède aucun organisme recueillant des renseignements étrangers outre-mer au moyen de sources humaines.
- En **Nouvelle-Zélande**, la communauté du renseignement est principalement formée de trois organismes responsables du renseignement de sécurité, du renseignement électromagnétique et d'évaluations nationales. À l'instar du Canada, la Nouvelle-Zélande n'a aucun organisme chargé de recueillir des renseignements étrangers outre-mer au moyen de sources humaines.

218 Comme cela a été mentionné plus tôt dans le présent document, un examen réalisé en 2017 a permis de conclure qu'un cadre de référence plus approprié serait une « communauté nationale du renseignement » englobant les six organismes de l'AIC, l'ACIC, l'AUSTRAC, et certains éléments de l'AFP et du DIBP.

- Au **Royaume-Uni**, il y a trois grands organismes, responsables du renseignement de sécurité, du renseignement étranger et du renseignement électromagnétique, qui font partie de ce qu'on appelle de façon générale le *national intelligence machinery*, qui comprend la Defence Intelligence et le Joint Intelligence Committee.
- Aux **États-Unis**, la communauté du renseignement est composée de 17 entités civiles ou militaires liées au renseignement, responsables notamment du renseignement de défense, du renseignement électromagnétique, du renseignement de sécurité et du renseignement étranger, mais aussi du renseignement énergétique, du renseignement en matière de drogues, du renseignement diplomatique et du renseignement financier[219].

Certaines des différences entre les communautés du renseignement reflètent simplement les différences dans la nature ou la portée de la collecte et de l'analyse des renseignements. D'autres différences reflètent la façon dont chaque pays a choisi de définir ou de caractériser sa communauté du renseignement.

B. Mécanismes de surveillance

Même si les mécanismes de surveillance des organismes de renseignement dans les cinq pays n'ont pas évolué au même rythme, il existe des convergences entre eux.

Premièrement, les pouvoirs et les mandats de pratiquement tous les organismes de renseignement sont régis dans une large mesure par un cadre législatif, ce qui a permis de créer des mécanismes de surveillance.

Deuxièmement, même si les organismes de renseignement étaient surveillés surtout par le pouvoir exécutif au départ, chaque pays a graduellement mis au point d'autres mécanismes de surveillance. De façon générale, la majorité des pays ont mis en place au moins un des mécanismes de surveillance suivants en plus de la surveillance effectuée par l'organe exécutif du gouvernement :

- comités spéciaux du Parlement ou du Congrès;
- inspecteurs généraux ou commissaires indépendants;
- surveillance judiciaire;
- contrôles indépendants des lois concernant la sécurité nationale.

C. Portée ou compétence des principaux mécanismes de surveillance

Il existe des différences entre les pays quant aux organismes qui font partie de la communauté du renseignement, et cela a un impact sur la surveillance. Par exemple :

- Certains organismes qui, aux États-Unis, seraient traités comme faisant partie de la communauté du renseignement et, par conséquent, s'inscrivent dans le cadre de surveillance des organismes de renseignement en sont exclus dans d'autres pays en raison de leur définition plus restrictive de la communauté du renseignement.
- Les mécanismes parlementaire et indépendants de surveillance des organismes de renseignement en Australie et en Nouvelle-Zélande sont très similaires, mais puisque l'Australie a adopté une définition plus vaste de la communauté du renseignement que la Nouvelle-Zélande, ces mécanismes s'appliquent de façon plus générale dans l'appareil de sécurité nationale en Australie qu'en Nouvelle-Zélande.

---

219 « Members of the IC », site Web de l'Office of the Director of National Intelligence. Voir aussi A. Daugherty Miles, « Defense Primer: National and Defense Intelligence », *In Focus*, IF10525, Congressional Research Service (CRS), 5 décembre 2016.

Les principaux comités parlementaires/du Congrès et organismes de surveillance indépendants diffèrent aussi, car le mandat de certains concerne des organismes précis et le mandat d'autres concerne des activités précises. Chaque système comporte un certain nombre d'avantages et de risques potentiels. Lorsque le mandat concerne des activités précises, cela veut dire que si d'autres organismes commencent à participer à ces activités, ils pourront être surveillés aussi, mais l'organisme de surveillance risque aussi de ne pas pouvoir examiner en détail le fonctionnement général des organismes. Lorsque le mandat concerne des organismes précis, l'organisme de surveillance peut examiner la totalité des activités des organismes, mais ce genre de mandat peut aussi limiter la capacité de l'organisme de surveillance d'examiner les activités qui dépassent le mandat. Le **tableau 1** compare la compétence des principaux organismes.

Tableau 1 : Organismes/éléments relevant des principaux organismes de surveillance[220]

	Parlementaire / du Congrès	**Indépendant**
Australie	PJCIS : tous les organismes de l'AIC (et les fonctions de lutte contre le terrorisme de la police fédérale australienne)	IGIS : tous les organismes de l'AIC
Canada	CPSNR : les activités liées à la sécurité nationale ou au renseignement	SCRS, CST et la GRC
Nouvelle-Zélande	ISC : NZSIS et GCSB	IGIS : NZSIS et GCSB
Royaume-Uni	ISC : surveille principalement le MI5, le MI6 et le GCHQ ainsi que d'autres activités gouvernementales liées au renseignement et à la sécurité, conformément au protocole d'entente conclu avec le premier ministre	IPC : fonctions statutaires précises; le premier ministre peut ordonner la surveillance d'autres fonctions des Agencies
États-Unis	Le Congrès surveille la totalité des organismes de l'USIC (la communauté du renseignement des États-Unis)[221]	Inspecteurs généraux, PCLOB et PIAB : tous les organismes de l'USIC[222]

Une question connexe est de savoir si les principaux organismes chargés de la surveillance des organismes de renseignement ont la compétence d'examiner de façon globale des questions liées au renseignement qui vont au-delà des organismes de base. Il s'agit là d'une question clé, étant donné qu'il y a, d'une part, une coopération croissante entre les organismes de renseignement et la communauté de la sécurité nationale en général et, d'autre part, de plus en plus d'échanges de renseignements entre les gouvernements et une utilisation accrue de ces renseignements par divers gouvernements. Les organismes de surveillance peuvent-ils examiner, par exemple, la façon dont un organisme qui ne fait pas partie de la « communauté du renseignement », comme un organisme chargé de protéger les frontières, utilise les renseignements de sécurité?

220. Voir la liste des acronymes aux pages 9 et 10 du présent document.

221. L. E. Halchin et F. M. Kaiser, *Congressional Oversight of Intelligence: Current Structure and Alternatives*, CRS Report for Congress, RL32525, CRS, 14 mai 2012; Z. K. Goldman, « The emergence of intelligence governance », dans Z. K. Goldman et S. J. Rascoff (dir.), *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, New York, Oxford University Press, 2016, p. 207 à 234.

222. W. Ginsberg et M. Greene, *Federal Inspectors General: History, Characteristics and Recent Congressional Actions*, CRS Report, R43814, CRS, 8 décembre 2014; US Government Accountability Office (GAO), *Inspectors General: reporting on independence, effectiveness, and expertise*, septembre 2011; Z. K. Goldman, « The emergence of intelligence governance ».

Le **Tableau 2** ci-dessous met en comparaison la mesure dans laquelle les principaux organismes de chaque pays peuvent examiner les questions liées au renseignement à tous les niveaux de leurs gouvernements nationaux respectifs. Dans chaque pays, au moins un des principaux mécanismes de surveillance des organismes de renseignement permet, dans une certaine mesure, d'examiner un ensemble plus vaste de questions liées au renseignement et à la sécurité. Cependant, dans la plupart des cas, ce pouvoir est assorti de restrictions claires. En outre, les comités du Parlement/du Congrès et les organismes indépendants effectuent habituellement différents types de surveillance; donc, dans les cas où seulement un organisme a la compétence d'examiner des questions qui vont au-delà des principaux organismes de la communauté du renseignement, il est difficile d'examiner toutes ces questions comme il faut.

Tableau 2 : Capacité des principaux organismes de surveillance d'examiner des questions liées au renseignement[223]

	Parlementaire / du Congrès	**Indépendant**
Australie	PJCIS : seulement les questions liées aux organismes de l'AIC (et certaines fonctions de l'AFP)	IGIS : peut seulement examiner les questions liées au renseignement ou à la sécurité concernant un autre organisme ou un autre ministère, à la demande du premier ministre
Canada	CPSNR : compétence relative aux activités liées à la sécurité nationale ou au renseignement et non à des organismes précis. Cela veut dire que des questions plus générales peuvent être examinées.	CSARS, BCCST, CCETP : chaque organisme a le mandat d'examiner les activités d'un organisme précis. Au moment de la publication du présent document, un projet de loi a été présenté au Parlement en vue de fusionner le CSARS et le BCCST en un seul organisme de surveillance (OSSNR) qui pourrait également examiner les plaintes présentées à la CCETP si cela concerne la sécurité nationale.
Nouvelle-Zélande	ISC : peut enquêter sur des questions liées à la sécurité ou au renseignement que lui renvoie le premier ministre, pourvu qu'elles ne soient pas directement liées aux activités du NZSIS ou du GCSB	IGIS : seulement les questions liées au NZSIS ou au GCSB
Royaume-Uni	ISC : peut examiner d'autres activités gouvernementales liées au renseignement ou à la sécurité, conformément au protocole d'entente conclu avec le premier ministre	IPC : la compétence dépend de fonctions statutaires précises des organismes; même si les fonctions comprennent celles des organismes de renseignement et de certains autres organismes, l'IPC n'a pas la compétence d'examiner des questions plus générales
États-Unis	Le Congrès a la compétence générale d'examiner des questions liées au renseignement[224].	Le PIAB et l'inspecteur général de la communauté du renseignement ont une compétence générale. Les activités du PCLOB sont principalement axées sur les questions liées à la protection de la vie privée et aux libertés civiles[225].

223. Voir la liste des acronymes aux pages 9 et 10 du présent document.

224. Halchin et Kaiser, *Congressional Oversight of Intelligence: Current Structure and Alternatives*; Z. K. Goldman, « The emergence of intelligence governance ».

225. Z. K. Goldman, « The emergence of intelligence governance »; Privacy and Civil Liberties Oversight Board (PCLOB), *About the Board*, site Web du PCLOB; Office of the Inspector General of the Intelligence Community, *What we do*, site Web de l'Office of the Director of National Intelligence.

D. Surveillance par le pouvoir exécutif

Dans tous les pays du Groupe des cinq, la surveillance des organismes de renseignement revient habituellement à l'organe exécutif du gouvernement, et la responsabilité incombe aux ministres compétents et, en dernier lieu, au premier ministre ou au président. Dans les cinq pays, il existe divers organismes d'examen relevant du pouvoir exécutif. La surveillance peut autant viser la période avant le fait que la période après le fait. Outre les organismes d'examen relevant de l'exécutif, en Australie, en Nouvelle-Zélande et au Royaume-Uni, le ministre compétent s'assure que le pouvoir exécutif surveille certains types de mandats et d'autorisations.

En **Australie**, la responsabilité de surveiller les organismes de renseignement incombe au procureur général, au ministre des Affaires étrangères et au ministre de la Défense et, en dernier lieu, au premier ministre. Les ministres sont responsables d'autoriser l'exécution de certains pouvoirs, y compris les perquisitions, l'interception de communications, l'installation d'appareils de surveillance, l'accès aux données informatiques et la collecte de renseignements sur les citoyens australiens par l'ASIS, l'AGO ou l'ASD.

Au **Canada**, les ministres de la Sécurité publique et de la Défense nationale, et en dernier lieu, le premier ministre, sont responsables des dossiers de sécurité nationale. Le premier ministre préside le Comité du Cabinet chargé du renseignement et de la gestion des urgences. Outre la responsabilité des ministres, la surveillance des organismes de renseignement est en grande partie effectuée par deux principaux organismes d'examen relevant de l'exécutif, qui sont uniquement habilités à tirer des conclusions et à formuler des recommandations[226]. Le CSARS examine les activités du SCRS *ex post facto*. Le CSARS est constitué de membres de divers partis politiques, mais ses fonctions sont définies par des ministres, et il doit leur rendre des comptes. Les activités du CST sont examinées par le commissaire du CST, un juge à la retraite ou à temps partiel, qui peut relever de ministres et qui doit leur rendre des comptes. Afin de recueillir des renseignements étrangers et de mener des activités de cyberdéfense, les activités du CST seront menées sous autorisation ministérielle.

En **Nouvelle-Zélande**, le premier ministre, en tant que ministre de la Sécurité nationale et du Renseignement est responsable de diriger l'appareil de sécurité nationale. Il incombe au ministre responsable de chaque organisme de renseignement et de sécurité d'exercer une surveillance ministérielle dans le cadre établi par le premier ministre. Les ministres ont la responsabilité unique d'émettre certains mandats et ont la responsabilité conjointe, avec le commissaire aux mandats de renseignement, d'en émettre d'autres.

Au **Royaume-Uni**, le premier ministre est responsable de la sécurité nationale. Le ministre de l'Intérieur est responsable du MI5, et le ministre des Affaires étrangères et du Commonwealth est responsable du MI6. Le ministre de la Défense est responsable du personnel de la Defence Intelligence. Les ministres compétents ont la responsabilité d'approuver les mandats et les autorisations pour diverses activités, y compris l'ingérence dans les biens, l'effraction informatique, les activités du MI6 ou du GCHQ à l'extérieur des îles Britanniques qui pourraient autrement mener à des poursuites au civil ou au criminel, et les mandats d'interception. L'interception des communications de députés nécessite l'approbation du premier ministre.

226 K. Roach, « Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps », dans Z. K. Goldman et S. J. Rascoff (dir.), *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, p. 196.

Aux **États-Unis**, le président est responsable de la sécurité nationale, même si la responsabilité en ce qui concerne les organismes distincts de l'USIC est répartie entre plusieurs membres du Cabinet (y compris les secrétaires d'État, de la Défense et de la Sécurité nationale) ainsi que deux fonctionnaires rattachés au Cabinet (les directeurs du renseignement national et de la Central Intelligence Agency (l'agence du renseignement national)[227]. Au sein de l'EOP, il y a plusieurs mécanismes de surveillance de la communauté du renseignement relevant du pouvoir exécutif, avec la collaboration d'un vaste réseau d'inspecteurs généraux et de conseillers juridiques. Au sein de l'EOP, le President's Intelligence Advisory Board (conseil consultatif du président chargé du renseignement [PIAB]) et le President's Privacy and Civil Liberties Oversight Board (conseil du président chargé de la surveillance de la protection des renseignements personnels et des libertés civiles [PCLOB]) fournissent des conseils au président[228]. Des commissions indépendantes, nommées soit par le président (p. ex. la commission sur les armes de destruction massive), soit par le Congrès (p. ex. la commission sur les attentats du 11 septembre) peuvent aussi jouer un rôle important dans la surveillance de la communauté du renseignement[229].

Dans chaque pays, la répartition des pouvoirs entre différents portefeuilles veut dire que, même si le chef du gouvernement a la responsabilité globale en ce qui concerne les dossiers de sécurité nationale, aucun ministre n'est responsable de l'ensemble des organismes et éléments de l'appareil du renseignement.

E. Surveillance exercée par le Parlement ou le Congrès

Dans chaque pays du Groupe des cinq, à l'exception notable du Canada, un ou plusieurs comités ont été établis par le Parlement ou le Congrès expressément afin d'examiner minutieusement les activités des organismes de renseignement. Le premier pays à avoir établi des comités séparés dont la fonction principale était d'examiner les activités liées au renseignement était les **États-Unis**, qui a établi par résolution le Senate Select Committee on Intelligence (comité spécial du Sénat sur le renseignement [SSCI]) et le House Permanent Select Committee on Intelligence (comité spécial permanent de la Chambre sur le renseignement [HPSCI]) en 1976 et 1977 respectivement[230]. Le SSCI et le HPSCI ont été établis, d'une part, afin d'améliorer, dans l'ensemble des comités permanents liés au renseignement, l'intégration des intérêts, des responsabilités et de l'expertise approfondie en matière de renseignement (et non de les remplacer) et, d'autre part, en réaction à l'opinion publique très répandue selon laquelle certains organismes de renseignement abusaient de leur pouvoir[231]. À la suite du scandale Iran-Contra des années 1980, le Congrès a renforcé sa surveillance en adoptant l'*Intelligence Authorization Act of 1991* (loi de 1991 sur l'autorisation du renseignement). L'objectif était que le Congrès soit tenu pleinement et rapidement au courant des activités des organismes de renseignement[232].

---

227 James Baker, « Intelligence Oversight », *Harvard Journal on Legislation*, vol. 45 (2008), p. 202 et 203. Voir aussi Bretton G. Sciaroni, « Theory and Practice of Executive Branch Intelligence Oversight », *Harvard Journal of Law and Public Policy*, vol. 12 (1989), p. 397.

228 Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6e éd., Washington D.C., Sage, CQ Press, 2015, p. 279. Voir aussi Executive Order 13462, *President's Intelligence Advisory Board and Intelligence Oversight Board*, signé par le président George H. W. Bush, 29 février 2008, https://www.hsdl.org/?view&did=483878.

229 James Baker, « Intelligence Oversight », p. 205.

230 Le SSCI a été établi par la Senate Resolution 400: *A resolution to establish a Standing Committee of the Senate on Intelligence Activities*, 94e Congrès, 2e session, S.Res. 400, 19 mai 1976. L'année suivante, la House Resolution 658 (H. Res. 658) a créé le HPSCI : *A resolution to amend the Rules of the House of Representatives and establish a Permanent Select Committee on Intelligence,* 95e Congrès, 1re session, 14 juillet 1977.

231 Frank Smist, *Congress Oversees the Intelligence Community*, 2e éd., Knoxville, University of Tennessee Press, 1994.

232 R. Morgan, « Oversight Through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities », dans Z. K. Goldman et S. J. Rascoff (dir.), *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, p. 63.

L'Australie, la Nouvelle-Zélande et le Royaume-Uni ont tous établi des comités similaires par voie statutaire. L'**Australie** a établi le comité parlementaire mixte sur l'ASIO en 1988. Des réformes législatives ont été effectuées en 1986 pour l'établissement du comité et de l'IGIS[233]. Le premier ministre de l'époque, quand il a annoncé pour la première fois l'établissement du comité, a mentionné que l'expérience d'autres pays en ce qui concerne la surveillance minutieuse des activités des organismes de sécurité et de renseignement par le Parlement montre que ce genre de comités peut être efficace[234]. Le mandat du comité a été élargi en 2002 et en 2005. Depuis 2005, le comité surveille les six organismes qui constituent la communauté du renseignement.

Ce qui s'est passé aux États-Unis a aussi influencé le **Canada**. Cependant, le Canada a toujours rejeté l'idée de renforcer le rôle des parlementaires dans la surveillance des activités du renseignement. Le Canada a plutôt intégré la surveillance des activités du renseignement dans le mandat des comités permanents. L'entrée en vigueur du projet de loi C-22 établira le premier comité parlementaire chargé d'examiner les affaires liées au renseignement, mais ce comité relèvera de l'organe exécutif plutôt que de l'organe parlementaire.

Au **Royaume-Uni**, l'ISA 1994 a établi l'ISC pour permettre aux parlementaires de surveiller les organismes de renseignement. Les pouvoirs et le mandat de l'ISC ont plus tard été élargis en vertu de la JSA. Des spécialistes ont mentionné l'influence potentielle de la Cour européenne des droits de l'homme et le désir d'éviter des décisions défavorables[235], ainsi que l'influence des organismes de surveillance parlementaires déjà établis aux États-Unis et en Australie[236].

La **Nouvelle-Zélande** a établi l'ISC en 1996. Ce comité et l'IGIS ont été établis notamment pour renforcer l'harmonisation avec les pratiques et procédures d'obligation redditionnelle en vigueur au Royaume-Uni, en Australie et au Canada relativement aux organismes de renseignement et de sécurité[237].

1. Mandats

Même si chaque pays, à l'exception du Canada, a établi un comité du Parlement ou du Congrès, les mandats de ces comités ne sont pas les mêmes.

Aux **États-Unis**, même si chaque comité compétent est restreint dans ce qu'il peut examiner (p. ex. il y a une distinction entre le renseignement militaire et les autres formes de renseignement), il n'y a aucune limite officielle quant à ce que ces comités, ensemble, peuvent examiner relativement aux activités de renseignement relevant du gouvernement des États-Unis.

---

233 Les projets de loi établissant le comité et l'IGIS ont été présentés conjointement en mai 1986.

234 R. Hawke, « Report and Ministerial statement: Royal Commission on Australia's Security and Intelligence Agencies », House of Representatives, *Debates*, 22 mai 1985, p. 2885 à 2892.

235 J. Moran et C. Walker, « Intelligence Powers and Accountability in the UK », dans Z. K. Goldman et S. J. Rascoff (dir.), *Global Intelligence Oversight: Governing Security in the Twenty-First Century*.

236 R. Morgan, « Oversight Through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities », p. 61.

237 Intelligence and Security Agencies Bill, selon le Committee on the Intelligence and Security Agencies Bill, 1996, p. ii.

Au **Royaume-Uni**, le mandat de l'ISC, même s'il est plus restrictif que celui des comités américains, permet l'examen des politiques, de l'administration et des dépenses des organismes de renseignement ainsi que des activités opérationnelles dans certains cas. L'ISC peut seulement enquêter sur des activités opérationnelles lorsque le premier ministre en fait la demande, lorsque les activités ne sont plus en cours ou lorsque l'information a été divulguée de façon volontaire.

L'ISC en **Nouvelle-Zélande** et le PJCIS en **Australie** ne sont pas habilités à examiner les activités opérationnelles. Ces organismes sont chargés d'examiner l'administration et les dépenses des organismes (et dans le cas de l'ISC, les politiques), ainsi que d'autres dossiers renvoyés par l'une des Chambres du Parlement ou par un ministre (en Nouvelle-Zélande, le premier ministre, et en Australie, un ministre responsable d'un organisme de renseignement). En Australie, le PJCIS ne peut pas enquêter sur des plaintes présentées par un particulier à propos des activités d'un organisme de renseignement. En Nouvelle-Zélande, l'ISC peut seulement enquêter sur des plaintes présentées par un particulier à propos des activités d'un organisme lorsque le problème ne peut pas être réglé en vertu d'une autre mesure législative.

Au **Canada**, le CPSNR aura le pouvoir d'examiner les politiques, l'administration et les dépenses des organismes de renseignement, de façon similaire à l'ISC en Nouvelle-Zélande. Comme ce qui se fait au Royaume-Uni, le CPSNR aura aussi le pouvoir d'examiner les activités pourvu qu'il ne s'agisse pas d'opérations en cours ou que le ministre compétent ne détermine pas que l'examen nuira à la sécurité nationale. Cependant, le CPSNR sera un comité de parlementaires (et non un comité parlementaire) et, par conséquent, relèvera du pouvoir exécutif.

2. Pouvoirs

a. Lancement d'enquêtes

Les comités du Parlement et du Congrès peuvent lancer leurs propres enquêtes :

- aux **États-Unis** et au **Royaume-Uni**, sur toute affaire relevant de la compétence du comité;
- en **Nouvelle-Zélande**, seulement sur les politiques, l'administration et les dépenses des organismes de renseignement et de sécurité;
- en **Australie**, seulement sur l'administration et les dépenses des organismes de renseignement;
- au **Canada** (le CPSNR), sur n'importe quelle affaire relevant de sa compétence (excluant les opérations en cours, comme il est mentionné plus haut).

En Australie et en Nouvelle-Zélande, l'une ou l'autre des Chambres du Parlement, un ministre ou le premier ministre respectivement peuvent demander aux comités d'examiner des dossiers qui, habituellement, ne font pas partie de leur compétence.

Même s'il ne peut pas entreprendre ce genre d'enquête de sa propre initiative, l'ISC de la Nouvelle-Zélande peut demander à l'IGIS d'entreprendre une enquête sur le respect de la loi par un organisme ou sur le bien-fondé des activités de cet organisme. On a recommandé qu'un pouvoir similaire soit accordé au PJCIS en Australie.

b. Collecte d'information

Même si le mandat de chaque comité est différent, les pouvoirs dont disposent les comités pour examiner les affaires relevant de leur mandat sont, de façon générale, équivalents.

Le président des **États-Unis** doit s'assurer que les comités du Congrès sont mis pleinement et rapidement au courant des activités liées au renseignement et avertis dès que possible des programmes de collecte et d'activités secrètes ainsi que de toute activité de renseignement illégale[238]. Les comités peuvent exiger que des fonctionnaires viennent témoigner dans le cadre d'audiences et demander que de l'information leur soit fournie.

En **Australie**, en **Nouvelle-Zélande** ou au **Royaume-Uni**, les comités ont des pouvoirs similaires pour ce qui est de demander aux dirigeants des organismes de renseignement de produire des documents ou un témoignage. Ils peuvent aussi demander à toute autre personne de fournir un témoignage ou de produire un document pour le comité. Cependant, dans tous les pays, il y a des limites à l'information qui peut être demandée ou exigée en vertu de ces pouvoirs afin de protéger l'information opérationnelle de nature délicate, comme cela est décrit plus bas.

c. Divulgation

Les comités ont un accès limité aux renseignements de nature délicate. En **Australie**, le PJCIS ne peut pas exiger qu'une personne ou un organisme divulgue de l'information opérationnelle de nature délicate ou des renseignements qui compromettraient ou pourraient compromettre la sécurité nationale de l'Australie ou ses relations avec d'autres pays. Les ministres peuvent également émettre des certificats empêchant la divulgation de renseignements opérationnels de nature délicate au PJCIS. En **Nouvelle-Zélande**, les dirigeants des organismes peuvent refuser de divulguer des renseignements de nature délicate. Cependant, le premier ministre peut passer outre au refus d'un dirigeant de divulguer de l'information s'il est dans l'intérêt public que cette information soit divulguée. Au **Royaume-Uni**, la situation est légèrement différente : les dirigeants des organismes peuvent seulement refuser de divulguer des renseignements à l'ISC si le ministre y oppose son veto. Ce droit de veto ne peut être exercé que si les renseignements sont de nature délicate et ne devraient pas être divulgués, dans l'intérêt de la sécurité nationale, ou si cela contrevient aux directives applicables. Aux **États-Unis**, un certain nombre de facteurs peuvent avoir une incidence sur la divulgation de renseignements, par exemple la nature délicate de l'information et des facteurs opérationnels. Par exemple, certains avis concernent des questions de nature si délicate que seulement huit membres du Congrès les reçoivent[239].

F. Surveillance indépendante

Chaque pays a une forme ou une autre de surveillance indépendante. En **Australie** et en **Nouvelle-Zélande**, cette fonction est assurée par l'IGIS. Au **Royaume-Uni**, cette fonction incombera au nouvel IPC. Au **Canada**, l'organe exécutif a confié cette tâche à trois organismes d'examen spécialisés : le CSARS, le CCETP et le BCCST. Si le projet de loi C-59 est adopté, le BCCST et le CSARS seront fusionnés en un seul organisme, l'OSSNR.

---

238 50 U.S.C. §§ 3091-3093. L'article 3092 régit la surveillance des activités de renseignement qui ne sont pas des activités secrètes, et l'article 3093 régit la surveillance des activités secrètes liées au renseignement.

239 Mark Lowenthal, *Intelligence: From Secrets to Policy*, p. 298. Le Gang of Eight (groupe des huit) comprend les chefs de chacun des deux partis politiques au Sénat et à la Chambre des représentants (le Président de la Chambre, le leader de la minorité à la Chambre, et les leaders de la minorité et de la majorité au Sénat) ainsi que les présidents (de la majorité) et les membres de haut rang (de la minorité) du HPSCI et du SSCI.

Aux **États-Unis**, il y a un système pangouvernemental d'inspecteurs généraux (IG), qui comprend des IG chargés de surveiller des organismes de renseignement précis et un IG responsable de la communauté du renseignement qui a compétence d'examiner l'ensemble des organismes[240]. Il y a également deux entités qui conseillent le président, le PIAB et le PCLOB[241].

1. Nomination

En **Australie** et en **Nouvelle-Zélande**, les IGIS sont nommés par le gouverneur général[242]. Au **Royaume-Uni**, à l'inverse, l'IPC est nommé par le premier ministre, et aux **États-Unis**, les membres du PCLOB et du PIAB sont nommés par le président. Il y a plusieurs méthodes de nomination aux États-Unis pour les IG. L'IG de la communauté du renseignement est nommé par le président sur recommandation du Sénat, qui doit donner son consentement, à l'instar d'un grand nombre d'IG chargés de surveiller chacun des organismes et d'autres éléments[243].

Au **Canada**, les membres du CSARS, du CCETP et le commissaire du Centre de la sécurité des télécommunications sont nommés par le gouverneur en conseil[244].

2. Fonctions

Les mandats de l'IGIS en **Australie** et en **Nouvelle-Zélande** sont similaires, et ils diffèrent de celui de l'IPC au Royaume-Uni. Dans les deux pays, l'IGIS est responsable d'examiner les activités opérationnelles des organismes de renseignement afin de veiller à ce qu'elles respectent les lois et soient bien fondées. Aux fins de son mandat, il a le pouvoir de mener des enquêtes sur certaines questions et d'effectuer des inspections. Il peut lancer des enquêtes de sa propre initiative, ou à la demande du ministre compétent ou du premier ministre. En Nouvelle-Zélande, l'ISC peut également demander des enquêtes. Dans les deux pays, l'IGIS a le pouvoir de convoquer et d'interroger des personnes, d'exiger la production de documents et d'entrer dans les bureaux des organismes. Vu les restrictions relativement strictes imposées à la surveillance parlementaire en Australie et en Nouvelle-Zélande, l'IGIS joue un rôle important dans la responsabilisation des organismes dans ces deux pays.

Au **Royaume-Uni**, le rôle de l'IPC diffère de celui de l'IGIS en Australie et en Nouvelle-Zélande. L'IPC a le mandat d'examiner certaines *fonctions* statutaires, au lieu d'avoir le pouvoir d'examiner de façon générale les *activités* des organismes de renseignement (à l'exception de l'examen d'autres fonctions des Agencies si le premier ministre en fait la demande). Plus précisément, l'IPC peut effectuer des vérifications, des inspections et des enquêtes relativement à l'interception des communications, à l'acquisition et à la conservation de données de communications, à l'effraction informatique et à l'acquisition, à la conservation et à l'utilisation d'ensembles de données personnelles. Ces pouvoirs d'examen s'ajoutent aux pouvoirs de l'IPC d'autoriser l'émission de certains types de mandats. On peut ainsi dire qu'il s'agit d'un organisme hybride qui peut à la fois approuver l'émission de mandats *avant le fait* et examiner certains types d'activités *après coup*.

---

240. W. Ginsberg et M. Greene, *Federal Inspectors General: History, Characteristics and Recent Congressional Actions*; GAO, *Inspectors General: reporting on independence, effectiveness, and expertise.*

241. Z. K. Goldman, « The emergence of intelligence governance ».

242. En Australie, le premier ministre recommande une personne après avoir consulté le chef de l'opposition. En Nouvelle-Zélande, le Parlement recommande la personne.

243. W. Ginsberg et M. Greene, *Federal Inspectors General: History, Characteristics and Recent Congressional Actions*, p. 3 à 5; GAO, *Inspectors General: reporting on independence, effectiveness, and expertise*, p. 21 à 24.

244 Au Canada, les dirigeants du CSARS, du BCCST et du CCETP sont tous nommés par le Cabinet. Le premier ministre canadien consulte le Parlement seulement en ce qui concerne la nomination du dirigeant du CSARS.

Au **Canada**, les organismes d'examen spécialisés ont le mandat d'enquêter sur les plaintes et d'examiner la légalité des activités des organismes de renseignement et de sécurité nationale du Canada.

Aux **États-Unis**, les IG responsables d'organismes précis et l'IG de la communauté du renseignement peuvent effectuer des vérifications et des enquêtes relativement aux programmes et aux opérations des organismes couverts par leur mandat. Le PIAB surveille le respect, par la communauté du renseignement américaine, des lois pertinentes, les décrets-lois et les directives présidentielles, alors que le PCLOB est chargé de veiller à ce que les efforts du gouvernement fédéral pour combattre le terrorisme ne soient pas disproportionnés relativement au besoin de protéger la vie privée et les libertés civiles[245]. Les deux conseils font partie du pouvoir exécutif, mais ils emploient des experts externes pour conserver un certain niveau d'indépendance[246].

En outre, l'**Australie** et le **Royaume-Uni** ont tous deux des contrôleurs indépendants de la législation – l'INSLM et l'Independent Reviewer of Terrorism Legislation (l'examinateur indépendant des lois sur le terrorisme) respectivement. Dans les deux pays, les contrôleurs indépendants ont le pouvoir d'examiner le fonctionnement et l'efficacité des lois sur la sécurité nationale, et non les organismes eux-mêmes. Cependant, dans l'exercice de leurs fonctions, ils examinent la façon dont les organismes appliquent les lois et peuvent recommander des modifications aux lois, aux processus et aux mécanismes de surveillance[247].

G. Surveillance judiciaire

Dans le passé, l'organe judiciaire a fait preuve de déférence en ce qui concerne la sécurité nationale. La surveillance judiciaire des organismes de renseignement demeure limitée et diffère entre les cinq pays.

En **Australie**, l'organe judiciaire participe peu en ce qui concerne les autorisations liées à l'exercice des pouvoirs. Cela revient en grande partie aux ministres. Les décisions prises en vertu des lois régissant les organismes de renseignement sont exclues du cadre législatif applicable aux contrôles judiciaires des décisions exécutives, mais les particuliers ont une certaine marge de manœuvre pour demander un contrôle judiciaire de la légalité de mesures prises par les agents du renseignement. La Security Division of the Administrative Appeals Tribunal peut procéder à un examen du bien-fondé de la plupart des évaluations en matière de sécurité émises par l'ASIO dont le résultat est défavorable (lesquelles sont prises en considération dans toute une série de décisions administratives, par exemple l'annulation d'un passeport), à huis clos.

---

245 PCLOB, *About the Board.*

246 Z. K. Goldman, « The emergence of intelligence governance », p. 226.

247 L'Independent National Security Legislation Monitor a même la fonction précise « d'évaluer si les lois australiennes relatives à la sécurité nationale ou à la lutte contre le terrorisme sont utilisées à d'autres fins que d'assurer la sécurité nationale ou de combattre le terrorisme » (*INSLM Act*, alinéa 6(1)d)) [TRADUCTION] . L'UK Independent Reviewer of Terrorism Legislation est habilité à examiner le fonctionnement du *Terrorism Act 2000* et de la partie I du *Terrorism Act 2006* (article 36 de la loi de 2006); à examiner le fonctionnement du *Terrorism Prevention and Investigation Measures Act 2011* (article 20 de cette loi); à examiner la *Terrorist Asset-Freezing etc. Act 2010* (partie I) (article 31 de la loi); à produire des rapports sur le fonctionnement de trois autres lois, en tout ou en partie : l'*Anti-Terrorism Crime and Security Act 2001*, la *Counter-Terrorism Act 2008* et la *Counter-Terrorism and Security Act 2015* (article 44 de la *Counter-Terrorism and Security Act 2015*). L'Independent Reviewer peut, à la demande de ministres ou de sa propre initiative, mener des examens et produire des rapports sur des questions précises.

Au **Canada**, des juges spécialement désignés à la Cour fédérale approuvent les mandats demandés par le SCRS pour les activités de surveillance électronique et d'autres formes de surveillance. Les juges peuvent également approuver, seulement aux fins de la perturbation de menaces, des mandats permettant au SCRS de violer des lois canadiennes ou de restreindre des droits garantis par la *Charte* au Canada ou à l'étranger[248]. Il n'y a pas de surveillance judiciaire du CST, l'organisme canadien de renseignement électromagnétique, qui n'a pas besoin de mandats pour mener ses activités. Toutefois, si le projet de loi C-59 est adopté, certaines autorisations ministérielles proposées relativement au CST seront assujetties à l'approbation d'un nouveau commissaire au renseignement, qui doit être un juge d'une cour supérieure à la retraite.

En **Nouvelle-Zélande**, un commissaire aux mandats de renseignement, qui doit être un ancien juge de la Cour suprême, a la responsabilité conjointe, avec le ministre compétent, d'émettre des mandats de type 1, qui autorisent un organisme à mener des activités qui, autrement, seraient illégales relativement à un citoyen ou un résident permanent de la Nouvelle-Zélande. La responsabilité pour l'émission de mandats de type 2, qui autorisent des activités qui seraient illégales autrement et qui ne concernent pas des citoyens ou des résidents permanents de la Nouvelle-Zélande, incombe uniquement au ministre compétent et n'exige aucune intervention d'un commissaire.

Au Royaume-Uni et aux États-Unis, des tribunaux spéciaux ont été créés pour traiter les questions liées au renseignement, même si leurs mandats sont distincts. Au **Royaume-Uni**, l'IPT instruit les plaintes relatives à l'utilisation illégale de techniques secrètes par les autorités publiques et accorde un droit de recours aux victimes d'actes illégaux en leur donnant également un droit d'appel sur une question de droit (mais ce droit d'appel n'était pas en vigueur au moment de la publication du présent document). Aux **États-Unis**, le Foreign Intelligence Surveillance Court approuve les mandats pour la collecte de renseignement, surveille des programmes de renseignement et émet des ordonnances servant à mener des enquêtes afin de recueillir des renseignements étrangers, y compris la surveillance électronique et les fouilles manuelles[249].

1. Affaires récentes

Malgré le contrôle judiciaire limité exercé sur les organismes de renseignement, il y a récemment eu des affaires judiciaires impliquant des organismes de renseignement, notamment en ce qui concerne l'échange de renseignements. Depuis 2013, la Cour fédérale du Canada a conclu à deux reprises que le SCRS avait manqué à son obligation de franchise en omettant d'informer la Cour qu'il avait recours à l'aide de partenaires du Groupe des cinq dans l'exécution d'ordonnances de surveillance et lorsqu'il avait omis d'informer la Cour pendant une décennie qu'il conservait des métadonnées recueillies sur des personnes qui n'étaient pas visées par un mandat[250]. De même, au Royaume-Uni, l'IPT a conclu que l'échange de renseignements entre le Royaume-Uni et les États-Unis contrevenait à la Convention européenne des droits de l'homme en raison du manque de clarté publique sur le cadre juridique relatif à cet échange de renseignements[251]. En outre, la Cour de justice de l'Union européenne a conclu que des organismes américains, en vertu du Safe Harbour Agreement (accord sur la sphère de sécurité des données) conclu entre l'Union européenne et les États-Unis, accédaient à des données auxquelles ils

248 K. Roach, « Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps », p. 193.

249 Frederic Manget, « Intelligence and the Rise of Judicial Intervention: Another System of Oversight », *Studies in Intelligence* (une publication du Center for the Study of Intelligence de la CIA), vol. 39, n° 5 (1996), p. 47.

250 Voir X (Re), 2013 CF 1275 et 2016 CF 1105, respectivement.

251 *Liberty v Secretary of State for the FCO and Others*, UKIPT 13-77-H.

n'avaient pas le droit d'accéder en vertu des règles de l'Union européenne en matière de protection de la vie privée[252]. L'échange de renseignements est donc une question qui fait l'objet d'un contrôle judiciaire.

Le pouvoir de conservation de données a également fait l'objet d'un contrôle judiciaire récemment. Au Royaume-Uni, la Cour suprême a récemment conclu que la loi britannique sur la conservation des données en cas d'urgence, la *Data Retention and Investigatory Powers Act 2014*, violait les règles de l'Union européenne en matière de protection des données, en grande partie en raison des lacunes du régime de surveillance créé par la loi[253].

H. Information sur les budgets

Chacun des pays examinés rend publics certains renseignements sur les crédits budgétaires alloués aux organismes de renseignement, mais aucun d'entre eux ne rend publics les montants alloués à chacun d'eux.

En **Australie**, les documents budgétaires nationaux comprennent les affectations spécifiques à l'ASIO, l'ASIS et l'ONA (bien qu'il semble que tous les fonds ne soient pas inclus, du moins pour l'ASIO et l'ASIS). Les crédits attribués aux trois organismes du portefeuille de la Défense sont inclus dans le budget du ministère de la Défense.

La situation au **Canada** et en **Nouvelle-Zélande** est similaire à celle de l'Australie. Les budgets du SCRS, du CST, de la GRC (dans le cas du Canada), du NZSIS et du GCSB (dans le cas de la Nouvelle-Zélande) sont rendus publics, tandis que d'autres fonds liés au renseignement sont inclus dans les budgets pour des portefeuilles plus vastes, sans toutefois être ventilés.

Au **Royaume-Uni**, le gouvernement publie un compte unique pour les organismes de renseignement (Single Intelligence Account) qui rend compte du financement total accordé au MI5, au MI6 et au GCHQ (bien que le GCHQ reçoive également un financement dans le cadre du National Cyber Security Programme [programme national de la cybersécurité])[254]. D'autres fonds liés au renseignement sont inclus dans le budget général du ministère de la Défense.

Le gouvernement des **États-Unis** publie les budgets totaux alloués aux deux principaux éléments de son budget du renseignement – le National Intelligence Program (programme national du renseignement) et le Military Intelligence Program (programme du renseignement militaire). Cependant, une partie du financement relatif au renseignement ne relève pas de ces programmes[255].

---

252 *Schrems v Data Protection Commissioner*, 6 octobre 2015, Case C-362/14.

253 *Davis and Others v Secretary of State for the Home Department,* EWHC 2092 (Admin) 2015. Dans le cadre d'un appel interjeté devant la Cour d'appel, l'affaire a été renvoyée à la Cour de justice de l'Union européenne, qui a conclu que le pouvoir de conserver des données excédait la limite de ce qui est strictement nécessaire et ne pouvait être justifié dans une société démocratique. L'affaire a été renvoyée à la Cour d'appel, et le jugement reste à venir.

254 *Security and intelligence agencies financial statement 2015 to 2016*, site Web du gouvernement du Royaume-Uni; « GCHQ funding and financial controls », site Web du GCHQ.

255 « U.S. intelligence community budget », site Web de l'Office of the Director of National Intelligence. Voir aussi A. Daugherty Miles, *Intelligence Community Spending: Trends and Issues*, CRS Report, R44381, CRS, 8 novembre 2016; A. Daugherty Miles, *Intelligence Community Programs, Management and Enduring Issues*, CRS Report, R44681, 8 novembre 2016.

CONCLUSION

Dans une société démocratique, il y aura toujours une certaine tension entre le besoin des organismes de renseignement d'agir avec un degré de confidentialité et le besoin que ces organismes rendent compte de leurs actes. Les cadres élaborés par les cinq pays examinés dans le présent document représentent les compromis trouvés entre ces deux impératifs.

Le présent document de recherche met en relief les différences dans la façon dont chaque pays a choisi de mener ses activités de surveillance de la communauté du renseignement. Ce qui peut fonctionner bien dans un pays ne sera peut-être pas cohérent avec les institutions et les normes d'un autre pays. Les cadres de surveillance reflètent la structure politique de chaque pays ainsi que son histoire et sa culture, et c'est pourquoi il y a des différences particulières. Cependant, chaque pays a élaboré un cadre qui comprend un système de freins et de contrepoids où les divers pouvoirs gouvernementaux jouent un rôle, afin de s'assurer que les organismes sont tenus responsables de leur administration, de leurs dépenses, et de la légalité et du bien-fondé de leurs activités.

Les communautés du renseignement ont évolué pour répondre aux nouveaux défis à mesure qu'ils surviennent, et elles vont continuer à le faire. Il sera important que les mécanismes de surveillance évoluent au même rythme que ces changements, et les pays abordés dans le présent document auront peut-être des leçons à retenir les uns des autres à mesure qu'ils continuent d'examiner et de renforcer leurs mécanismes de surveillance.