

**GROUPE CONSULTATIF SUR LA
TRANSPARENCE DE LA SÉCURITÉ
NATIONALE (GCT-SN)
25 NOVEMBRE 2020**

RAPPORT INITIAL

**CE QUE NOUS AVONS ENTENDU AU COURS DE
NOTRE PREMIÈRE ANNÉE**

*PREMIER RAPPORT AU SOUS-MINISTRE DE LA SÉCURITÉ
PUBLIQUE SUR LA TRANSPARENCE DE LA SÉCURITÉ NATIONALE*

Le Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN) est un comité indépendant et autonome supporté financièrement et en nature par le gouvernement du Canada.

Les opinions et les points de vue exprimés dans le présent document sont strictement ceux des membres du GCT-SN collectivement et ne doivent pas être considérés comme le point de vue officiel du gouvernement du Canada.



Table des matières

Introduction : Premier rapport du Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN).....	4
Ce que nous avons entendu au cours de notre première année	4
<i>Gouvernance du milieu de la sécurité nationale</i>	5
<i>Culture du secret</i>	5
<i>Gouvernement numérique et ouvert</i>	6
<i>Secret entourant les mécanismes de surveillance et les procédures judiciaires</i>	7
<i>Gestion de l'information</i>	8
<i>Protection de la vie privée et sécurité</i>	8
<i>Relations avec les communautés racialisées et marginalisées et les autres communautés minoritaires</i>	9
<i>Culture du milieu de travail dans les organismes de sécurité nationale</i>	11
<i>Comment le gouvernement communique</i>	11
Prochaines étapes.....	12
Annexe 1 : Contexte de la transparence de la sécurité nationale	13
<i>Qu'est-ce que la transparence et pourquoi est-elle importante pour la sécurité nationale?</i>	13
<i>Engagement de transparence en matière de sécurité nationale</i>	13
<i>Loi de 2017 sur la sécurité nationale</i>	14
Annexe 2 : Contexte du Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN)	16
<i>Membres du GCT-SN en date du 7 octobre 2020</i>	17
Annexe 3 : Architecture du milieu de la sécurité nationale.....	18
<i>Qu'est-ce que la sécurité nationale?</i>	18
<i>Ministères et organismes responsables de la sécurité nationale au Canada</i>	18
<i>Architecture du milieu de la sécurité nationale à l'échelle fédérale</i>	20
Annexe 4 : Points saillants des réunions du GCT-SN, d'août 2019 à septembre 2020.....	21
Annexe 5.1 : Analyse internationale de la transparence de la sécurité nationale	26
Annexe 5.2 : Politiques relatives à la transparence de la sécurité nationale et du renseignement dans certaines organisations gouvernementales à l'échelle internationale.....	38

Introduction : Premier rapport du Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN)

Le milieu de la sécurité nationale au Canada n'a pas toujours été très transparent. Les sites Web officiels et les documents publics contiennent habituellement peu de renseignements, tandis que le système d'accès à l'information est fréquemment critiqué en raison de l'ampleur considérable du caviardage et de la lenteur des processus qui y sont associés. La situation s'est quelque peu améliorée au cours des dernières années, notamment grâce à la mise sur pied du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). L'établissement des deux organismes d'examen a permis d'améliorer l'examen et la surveillance du milieu canadien de la sécurité nationale et du renseignement.

En tant que Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN), notre travail au cours de la dernière année nous a convaincus de la nécessité de continuer d'améliorer la transparence de la sécurité nationale. Nous comprenons assurément que certains renseignements détenus par les institutions de sécurité nationale doivent demeurer classifiés. En même temps, la transparence est essentielle à une saine démocratie. Les organismes d'application de la loi et de renseignement doivent être perçus comme légitimes par la société qu'ils cherchent à protéger. Lorsqu'ils ont la confiance de la population, ils peuvent plus facilement établir des liens avec les collectivités. La transparence peut aussi faire en sorte que les professionnels de la sécurité nationale soient tenus responsables en cas de transgression. Lorsque les organismes ne croient pas qu'ils seront tenus responsables, ils continuent de prendre des mesures et d'adopter des comportements inappropriés; pourtant, lorsque les organismes de sécurité sont trop secrets et ne sont pas transparents, il est plus difficile pour les citoyens de leur faire confiance. Cela renforce une dynamique de méfiance et de soupçon.

SELON UN SONDAGE MENÉ EN 2020, 49 % DES CANADIENS SE SONT MONTRÉS D'ACCORD DANS UNE CERTAINE MESURE AVEC L'ÉNONCÉ SUIVANT : « JE PEUX ME FIER AU GOUVERNEMENT DU CANADA POUR TROUVER LE JUSTE ÉQUILIBRE ENTRE LA SÉCURITÉ ET LES LIBERTÉS CIVILES. » EN 2017, CE POURCENTAGE ÉTAIT DE 55 %.

Source : Bibliothèque et Archives Canada
– Rapport de recherche sur l'opinion publique 063-19.

Ce que nous avons entendu au cours de notre première année

Les principaux thèmes que nous avons explorés au cours de notre première année de travail comprennent les suivants : la gouvernance du milieu de la sécurité nationale; la place importante de la culture du secret; les défis associés au gouvernement numérique et ouvert; le secret entourant les mécanismes de surveillance et les procédures judiciaires; la gestion de l'information; le difficile équilibre entre la protection de la vie privée et la sécurité; les relations du milieu de la sécurité nationale avec les communautés racialisées et les autres communautés

minoritaires; le lien entre la transparence et la culture du milieu de travail dans la collectivité; et, enfin, la question plus technique sur comment le gouvernement communique.

Gouvernance du milieu de la sécurité nationale

Au cours de trois réunions tenues en personne et de plusieurs autres réunions virtuelles, nous avons entendu un éventail de représentants du milieu de la sécurité nationale exprimer leur point de vue sur la transparence. Un certain nombre de problèmes ont été soulevés. Premièrement, la taille compte : nous reconnaissons que le milieu de la sécurité nationale est vaste. Cela pose d'importantes difficultés en matière de coordination; l'amélioration de la transparence exige des efforts qui prennent du temps et qui ne peuvent être réalisés que par la mobilisation d'une grande volonté. Par conséquent, la coordination – l'alignement de plusieurs pièces mobiles – est complexe. Le milieu de la sécurité nationale fait face à de nombreux problèmes à cet égard, notamment en ce qui concerne son leadership : le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNR) au Bureau du Conseil privé et le sous-ministre de la Sécurité publique jouent tous deux un rôle de coordination, mais la répartition précise de leurs responsabilités n'est pas toujours clairement définie. Deuxièmement – sujet que nous examinerons au cours de notre deuxième année –, les questions de définitions sont également importantes : une plus grande transparence a des répercussions différentes pour différents organismes.

Il serait utile que le gouvernement puisse mieux expliquer ces complexités de façon directe et intéressante afin de permettre au public de mieux comprendre les questions relatives à la sécurité nationale. Cela pourrait se faire au moyen de discours publics tenus régulièrement par des représentants élus et des hauts fonctionnaires, ainsi que de meilleures communications écrites officielles transmises plus fréquemment par l'entremise de sites Web, de médias sociaux et de rapports. Il importe de mentionner qu'une transparence accrue n'est pas uniquement une question de quantité. Un plus grand nombre de communications est nécessaire, mais celles-ci doivent également être claires, compréhensibles et significatives. Le gouvernement pourrait aussi faire preuve d'une plus grande transparence dans la communication des points d'interaction possibles entre le public et le milieu de la sécurité nationale, notamment pour tenir celui-ci responsable (p. ex. mécanismes de traitement des plaintes, ombudsmans, etc.). Nous avons également entendu divers points de vue sur les changements éventuels de la portée de la sécurité nationale, de la gestion des frontières et des capacités de renseignement à la lumière de la pandémie de COVID-19. À l'avenir, nous avons l'intention de tenir compte des répercussions potentielles de ces récents changements sur la gouvernance et la transparence.

Culture du secret

Dans le milieu de la sécurité nationale, le réflexe dominant consiste à garder l'information aussi secrète que possible; l'approche par défaut est habituellement de protéger l'information. Bien que cela soit parfois nécessaire, les efforts visant à améliorer la transparence doivent s'accompagner de changements apportés à cette culture du secret. Ce problème n'est pas nouveau. Il y a une dizaine d'années, l'enquête sur l'affaire Air India a mis en lumière le fait que

l'une des plus grandes défaillances organisationnelles à l'origine de la tragédie était un manque systémique d'échange d'information entre les organismes gouvernementaux¹. La norme selon laquelle l'information doit être communiquée en fonction du « besoin de savoir » est souvent interprétée de façon trop stricte; comme l'ont fait valoir bon nombre de nos conférenciers invités, le milieu de la sécurité nationale doit plutôt être plus discipliné et rigoureux pour éviter la surclassification systématique des données.

Ce manque de transparence peut avoir des conséquences imprévues, car le manque d'information risque davantage d'être comblé par de la désinformation ou d'éveiller les soupçons. À une époque d'abondance d'information en ligne, dont une partie est disponible par l'entremise de sources ouvertes ou d'alliés du Canada, l'absence de divulgation de la part du gouvernement peut éveiller les soupçons.

La transparence est souvent l'une des dernières priorités dans les discussions sur la sécurité nationale, mais on reconnaît de plus en plus la nécessité de mener des réformes systémiques pour apporter des changements. En 2018, par exemple, la RAND Corporation, établie aux États-Unis, a publié un rapport intitulé « Secrecy in US National Security: Why A Paradigm Shift is Needed² ». Le rapport plaide en faveur d'un changement systémique des structures de gouvernance et des mentalités afin d'améliorer à la fois la responsabilisation et le rendement. Bon nombre des thèmes abordés dans ce rapport correspondent étroitement aux commentaires que nous avons entendus de la part des intervenants dans le cadre de nos propres discussions.

Gouvernement numérique et ouvert

Comme les réformes du gouvernement numérique et ouvert ont pris de l'ampleur au cours des dernières années, on reconnaît de plus en plus les avantages découlant de l'échange d'information à l'intérieur et à l'extérieur du gouvernement et de la participation significative des citoyens. Le gouvernement du Canada a pris un certain nombre de mesures pour améliorer son rendement, en ce qui concerne par exemple la divulgation proactive de l'information, la quantité de données ouvertes et leur qualité et la participation du public à un éventail d'enjeux stratégiques, notamment par l'entremise des engagements qu'il a pris à l'égard du Partenariat pour un gouvernement ouvert³. Malgré ces progrès, il reste encore beaucoup de travail à faire. Dans un rapport de 2016 sur les réformes du gouvernement numérique et de la gouvernance de Westminster publié par le Mowat Centre de l'Université de Toronto, on a observé, par exemple, que les fonctionnaires étaient incités à accumuler des renseignements rares et spécialisés plutôt

¹ « Réponse du gouvernement du Canada à la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat commis contre le vol 182 d'Air India ». Sécurité publique Canada, 21 décembre 2018, www.securitepublique.gc.ca/cnt/rsrccs/pblctns/rspns-cmmsn/index-fr.aspx.

² Bruce, James B. et coll. « Secrecy in U.S. National Security: Why a Paradigm Shift Is Needed ». RAND Corporation, 1^{er} novembre 2018, www.rand.org/pubs/perspectives/PE305.html.

³ « Canada ». Partenariat pour un gouvernement ouvert, 2020, <https://www.opengovpartnership.org/fr/members/canada/>.

qu'à les communiquer⁴. Comme le signale le rapport, faisant écho à bon nombre des conclusions de l'étude de RAND mentionnée ci-dessus, le changement de mentalité ne peut découler que d'un changement culturel à grande échelle.

Le changement doit venir à la fois des échelons supérieurs – les dirigeants peuvent et doivent être plus ouverts et transparents – et des échelons inférieurs, notamment par une meilleure formation et une sensibilisation accrue. Il s'agit d'un point important. Au moins un de nos conférenciers invités a souligné qu'il ne suffisait pas de simplement demander au personnel des échelons inférieurs du gouvernement de faire preuve d'une plus grande transparence; la direction doit lui fournir les outils et les compétences nécessaires pour le faire. Enfin, nous notons que les efforts de transparence exigent également des investissements financiers dans les ressources humaines, dans des moyens technologiques permettant d'appuyer les mesures de transparence et dans des activités de mobilisation. En l'absence de ces ressources supplémentaires expressément désignées à cette fin, les nouvelles initiatives de transparence ne font qu'alourdir la charge de travail des fonctionnaires.

Secret entourant les mécanismes de surveillance et les procédures judiciaires

Le secret entourant les mécanismes de surveillance de la sécurité nationale et les procédures judiciaires représente un autre domaine où la transparence accrue est essentielle pour favoriser la confiance du public. Même dans les procédures pénales et civiles ordinaires, le principe de la publicité des débats judiciaires a des limites. Les procédures relatives à la sécurité nationale ne font pas exception. Néanmoins, l'optimisation de la transparence par les organismes d'examen et de surveillance de la sécurité nationale et dans le cadre des procédures judiciaires pourrait aider à réduire les soupçons et le manque de confiance.

Au cours de notre première année, nous avons reçu des observations portant sur le besoin d'une transparence accrue quant à l'interprétation et à la mise en œuvre, sur le plan juridique, des mandats et des pouvoirs des organismes de sécurité nationale. À cet égard, mentionnons la question des interprétations juridiques qui a été soulevée dans le cadre d'une récente décision publique de la Cour fédérale⁵. La Cour a conclu que, en raison de défaillances organisationnelles au Service canadien du renseignement de sécurité (SCRS) et au ministère de la Justice, le SCRS a manqué à son obligation de franchise envers la Cour puisqu'il n'a pas divulgué de manière proactive qu'il avait inclus, à l'appui de demandes de mandats, des renseignements probablement tirés d'activités illégales. En 2013⁶ et en 2016⁷, la Cour fédérale avait également conclu que le SCRS avait manqué à son obligation de franchise concernant des demandes de mandats.

⁴ Johal, Sunil et coll. « Reprogramming Government for the Digital Era ». Mowat Centre, Munk School of Public Policy & Governance, 11 septembre 2014, https://munkschool.utoronto.ca/mowatcentre/wp-content/uploads/publications/100_reprogramming_government_for_the_digital_era.pdf. Page 12.

⁵ Cour fédérale, 16 juillet 2020, <https://www.fct-cf.gc.ca/Content/assets/pdf/base/2020-07-16-CONF-1-20-SCRS-obligation-franchise.pdf>.

⁶ Cour fédérale, 22 novembre 2013, <https://decisions.fct-cf.gc.ca/fc-cf/decisions/fr/66439/1/document.do>.

⁷ Cour fédérale, 4 octobre 2016, <https://decisions.fct-cf.gc.ca/fc-cf/decisions/fr/212832/1/document.do>.

Les organismes chargés de l'examen de la sécurité nationale doivent également établir un équilibre entre l'importance de la transparence et la nécessité du secret dans l'exercice de leurs responsabilités. En 2017, un ancien organisme d'examen de la sécurité nationale, le Comité de surveillance des activités de renseignement de sécurité (CSARS, maintenant remplacé par l'OSSNR), a rejeté une plainte contre le SCRS et a cherché à limiter la capacité du plaignant de la commenter publiquement en rendant une « ordonnance de confidentialité⁸ ». Par la suite, la Cour fédérale a autorisé la divulgation du dossier non classifié du CSARS, affirmant que « la conclusion contraire aurait pour effet de subordonner systématiquement le principe de la publicité des débats judiciaires aux pratiques de n'importe quel tribunal autorisé à mener ses propres audiences à huis clos⁹ ».

Gestion de l'information

Tout au long de notre première année, nous avons entendu parler d'un certain nombre de problèmes dans le domaine de la gestion de l'information qui nuisent aux efforts visant à améliorer la transparence du milieu de la sécurité nationale. Le Canada, en particulier, ne dispose pas d'une stratégie globale de déclassification, ce qui entrave souvent considérablement la diffusion d'anciens documents classifiés. Le processus d'accès à l'information est largement critiqué en raison de sa lenteur excessive, et les documents ne sont généralement communiqués qu'une fois qu'ils ont été largement caviardés. De plus, différents ministères et organismes gouvernementaux utilisent une gamme de technologies et de systèmes de gestion de l'information. Bon nombre de ces derniers ne communiquent pas facilement entre eux, ce qui complique l'échange d'information au sein du gouvernement, entre les organismes de sécurité et avec le grand public. Les efforts de réforme précédents n'ont souvent entraîné que des changements marginaux.

Protection de la vie privée et sécurité

Comme les gouvernements recueillent et traitent des données et des renseignements provenant d'un plus grand éventail de sources, bon nombre de gens ont soulevé des préoccupations au sujet des risques pour la vie privée. Comme l'ont souligné de nombreux intervenants (y compris les commissaires à la protection de la vie privée et à l'information du Canada), il est essentiel de faire preuve de transparence quant à la façon dont les organismes de sécurité nationale accèdent aux données concernant l'identité et les actes des membres du public, les communiquent et les analysent. Les nouveaux outils découlant de l'intelligence artificielle et des applications d'appareils

SELON UN SONDAGE MENÉ EN 2019, 92 % DES CANADIENS SONT À TOUT LE MOINS QUELQUE PEU PRÉOCCUPÉS PAR LA PROTECTION DE LEUR VIE PRIVÉE.

Source : Bibliothèque et Archives Canada
– Rapport de recherche sur l'opinion publique [055-18](#).

⁸ « Rapport annuel 2017-2018 du CSARS ». Comité de surveillance des activités de renseignement de sécurité, 20 juin 2018, http://www.sirc.gc.ca/anrran/2017-2018/index-fra.html#section_3. Section 3.

⁹ Cour fédérale, 31 octobre 2018, <https://decisions.fct-cf.gc.ca/fc-cf/decisions/fr/349913/1/document.do>.

mobiles offrent de meilleures occasions d'améliorer les capacités de sécurité tout en approfondissant les questions sur la protection de la vie privée. En raison des progrès réalisés à l'égard de l'apprentissage automatique, on craint également que les métadonnées puissent révéler des renseignements sur les gens d'une manière qui renforce la discrimination et les préjugés. L'analyse prédictive est un outil attrayant, mais elle peut entraîner des résultats indésirables qui nuisent à des collectivités déjà marginalisées. Bien que de nombreuses lois protègent le droit à la vie privée des personnes vivant au Canada, ce droit est contesté par des dispositions législatives sur la sécurité nationale qui peuvent le limiter ou l'annuler, ce qui rend impératif l'établissement d'un équilibre approprié entre l'ouverture et le secret. Nous avons également consulté divers experts quant aux répercussions, touchant la protection des renseignements personnels et la sécurité, d'applications de recherche de contacts pour les téléphones mobiles pendant la pandémie de COVID-19, un exemple important de la façon dont la surveillance de la santé publique, la sécurité nationale et la gouvernance des données peuvent devenir encore plus interreliées et, par conséquent, accroître les questions de protection de la vie privée, de sécurité et de transparence.

La protection de la vie privée exige également une infrastructure sécurisée pour le stockage et l'échange de données, un défi croissant pour tous les secteurs à mesure que les systèmes infonuagiques massifs prennent de l'expansion et soutiennent l'activité en ligne. En plus de leurs propres systèmes, les gouvernements sont confrontés à des difficultés externes en matière de protection de la vie privée liées au chiffrement, ce qui peut améliorer la protection de la vie privée, d'une part, et faciliter les activités malveillantes et les nouvelles menaces, d'autre part. L'établissement de capacités modernes et novatrices en matière de cybersécurité pour tenir compte des diverses facettes concurrentes du chiffrement constitue une nouvelle priorité pour les organismes de sécurité nationale, étroitement liée aux questions de transparence, ainsi qu'à la culture du secret et aux structures mentionnées précédemment, qui peuvent entraver les progrès à cet égard. Pour surmonter ces difficultés, il sera essentiel de veiller à ce que la transparence ne soit pas délaissée au profit de la protection de la vie privée et de la sécurité. Cela nécessite des solutions technologiques créatives et un travail continu avec la communauté internationale sur les normes et les solutions en matière de données ouvertes.

SELON UN SONDAGE MENÉ EN 2018, 41 % DES CANADIENS SE DISENT PRÉOCCUPÉS LORSQU'IL EST QUESTION DE L'INFORMATION QUE LES SERVICES DE RENSEIGNEMENT RECUEILLENT SUR EUX.

Source : Bibliothèque et Archives Canada
— Rapport de recherche sur l'opinion publique [101-17](#).

Relations avec les communautés racialisées et marginalisées et les autres communautés minoritaires

Les organismes de sécurité nationale doivent admettre la présence de racisme systémique et de préjugés inconscients en leur sein et reconnaître que ces préjugés se manifestent dans leurs interactions avec certains membres du public. Si les organismes de sécurité nationale ne reconnaissent pas l'existence de ces préjugés et ne s'y attaquent pas vigoureusement, ils risquent, individuellement ou collectivement, de ne pas détecter les risques réels qui menacent la société et de ne pas agir en conséquence.

Quels renseignements les organismes de sécurité nationale sont-ils autorisés à recueillir, à qui peuvent-ils les communiquer et qu'est-ce qui est approprié et légal? Les organismes répondent souvent mal à ces questions, et ce manque de transparence alimente la méfiance et les soupçons. Cela nuit encore plus au sentiment d'appartenance, à la cohésion sociale et à la sécurité publique pour tous. Comme l'a souligné un de nos conférenciers invités, de nombreux membres des communautés autochtones, noires, racialisées et marginalisées et d'autres communautés minoritaires se méfient des organismes de sécurité nationale, et la nature de leurs interactions avec ces organismes gouvernementaux exacerbe souvent ces tensions.

Il est essentiel que les organismes de sécurité nationale, lorsqu'ils interagissent avec les gens de toutes les communautés, informent mieux le public de leurs mandats, de leurs responsabilités et de leurs pouvoirs, ainsi que des droits de la communauté ou de la personne. Ils pourraient aussi être plus sensibles à la réalité de certaines personnes vivant au Canada, qu'elles soient Canadiennes ou non, qui ont vécu des expériences négatives avec les autorités étatiques au Canada et dans d'autres pays pouvant façonner leur perception à l'égard des organismes de sécurité canadiens. Comme nous avons l'intention de l'examiner au cours de la deuxième année de notre travail, il est essentiel d'améliorer la diversité et l'inclusion dans le cadre des pratiques de gestion du personnel des organismes de sécurité nationale afin de prévenir les mauvais traitements et les pratiques d'exclusion. Cela comprend la prestation d'une formation sur la lutte contre le racisme et les préjugés inconscients à tous les échelons et la sensibilisation accrue aux expériences des communautés racialisées et marginalisées et d'autres communautés minoritaires au sein des organismes.

En ce qui concerne la sécurité nationale, les membres des communautés autochtones et noires et d'autres communautés racialisées peuvent avoir une certaine perception de la façon dont les organismes de sécurité nationale mènent leurs activités. Afin d'être plus transparents, les organismes de sécurité nationale peuvent mieux répondre aux demandes répétées des communautés en matière de responsabilisation, tenir compte de leurs préoccupations et répondre à leurs demandes. Les organismes de sécurité nationale ont également la possibilité de rendre des comptes lorsqu'il y a eu un manque de transparence dans le passé. Pour ce faire, ils doivent s'engager à rencontrer les communautés où elles se trouvent.

Les membres de ces communautés craignent parfois que les organismes de sécurité nationale communiquent avec eux pour recueillir du renseignement à des fins de sensibilisation; il est donc important que les organismes de sécurité nationale soient entièrement transparents au sujet de leur travail. Y a-t-il vraiment un besoin de sensibilisation? Quels sont les droits d'une personne en ce qui concerne de telles interactions? Ces droits devraient, avant toute autre communication avec une personne, être clairement définis et ne pas s'accompagner de contraintes. Les organismes de sécurité nationale doivent également faire preuve de prudence quant au contenu et à la prestation de leur formation (ce qui comprend, sans toutefois s'y limiter, la lutte contre l'extrémisme violent et la lutte contre le terrorisme). Ils doivent notamment s'assurer que la formation ne cible pas ou n'étiquette pas une communauté en particulier. Le contenu

stigmatisant et la prestation de leurs programmes de formation ont nui à la confiance envers les organismes fédéraux et ont contribué aux sentiments de malaise et de scepticisme à leur égard.

Enfin, l'utilisation d'étiquettes ou de mots stigmatisants au sujet d'une communauté ou d'une religion dans les rapports sur la sécurité nationale a eu une incidence négative sur les interactions entre les organismes locaux d'application de la loi et le public, puisque les communautés se sentent ciblées. Même si les organisations des différents échelons (municipal, provincial et fédéral) ont leur propre mandat, les mesures prises par l'une peuvent toucher les autres, car de nombreux membres du public perçoivent tous ces échelons de la même façon.

Culture du milieu de travail dans les organismes de sécurité nationale

Au cours des dernières années, les médias ont fait état d'un certain nombre de cas de harcèlement et de discrimination dans les organismes de sécurité nationale. Ces organismes gouvernementaux produisent des rapports publics expliquant où de tels problèmes sont survenus et comment ils ont été réglés, mais ils ne contiennent habituellement que des renseignements limités. Quelle est la fréquence de ces cas et comment le public peut-il avoir l'assurance que des efforts sérieux sont déployés pour améliorer la situation? Comment ces problèmes ont-ils une incidence sur les relations de ces organismes avec les communautés racialisées et les autres communautés minoritaires et la confiance que celles-ci leur témoignent? Nous croyons qu'une partie de notre rôle en tant que GCT-SN consiste à aider à attirer l'attention des gens sur ces questions et à expliquer comment un manque de transparence peut nourrir la méfiance.

Comment le gouvernement communique

Les efforts bien intentionnés du gouvernement pour être transparent sont souvent minés par des communications inefficaces; par exemple, les fonctionnaires ne savent parfois pas à qui s'adresser, tandis que les documents et les déclarations publiques – en particulier sur les sites Web du gouvernement – ont tendance à utiliser un langage aride ou technique, rendant l'information moins attrayante pour le public. L'amélioration de la transparence ne signifie pas simplement être *plus* transparent; il faut aussi améliorer la *façon* dont la transparence est mise en œuvre en pratique. Il s'agit d'un enjeu particulièrement important pour les interactions avec les communautés marginalisées et racialisées, où les préjugés, les problèmes de traduction ou les malentendus interculturels peuvent nuire à une communication efficace.

SELON UN SONDAGE MENÉ EN 2017, « SANS AIDE, SEULEMENT 3 % DES RÉPONDANTS ONT NOMMÉ CORRECTEMENT LE CST OU LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS COMME L'ORGANISME GOUVERNEMENTAL CHARGÉ D'INTERCEPTER ET D'ANALYSER LES COMMUNICATIONS ÉTRANGÈRES ET D'AIDER À PROTÉGER LES RÉSEAUX INFORMATIQUES DU GOUVERNEMENT. LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ (SCRS) EST BEAUCOUP PLUS SOUVENT NOMMÉ COMME L'ORGANISME DÉCRIT (CITÉ PAR 22 %) ».

Source : Bibliothèque et Archives Canada – Rapport de recherche sur l'opinion publique [128-16](#).

Nous croyons que les interactions du gouvernement avec les médias représentent un élément particulièrement important, mais parfois négligé, de l'équation. Le gouvernement interagit parfois directement avec les membres du public, soit en personne, soit au moyen de divers rapports, déclarations et sites Web. Cependant, l'information gouvernementale parvient aussi souvent au public après avoir été filtrée par les médias; les efforts visant à accroître la transparence devraient donc comprendre des initiatives permettant de mieux tirer parti du rôle des médias, notamment par l'offre de séances d'information améliorées. Cela est vrai pour les médias nationaux et grand public, mais aussi pour les médias d'information locaux, surtout ceux qui servent les communautés racialisées et minoritaires.

Prochaines étapes

Le GCT-SN produira deux rapports au cours de sa deuxième année (2020-2021). Le premier, qui sera publié dans la première moitié de 2021, portera sur la définition, la mesure et l'institutionnalisation de la transparence. Il existe de multiples définitions de la transparence, dans le domaine de la sécurité nationale et ailleurs, et il est difficile de la mesurer. Pourtant, il est essentiel d'avoir une compréhension de base de la transparence et de la façon de la mesurer et d'évaluer les progrès pour pouvoir l'améliorer. Nous proposons donc d'approfondir ces questions. En même temps, pour qu'une transparence accrue soit durable, elle doit être institutionnalisée et intégrée aux activités courantes. Des structures et des processus doivent être mis en place pour intégrer la transparence dans le travail quotidien du milieu de la sécurité nationale. Le rapport examinera également l'évolution du gouvernement ouvert à la lumière de la pandémie de COVID-19, alors que nous cherchons à comprendre les répercussions potentielles sur la transparence du gouvernement en général – et l'engagement de transparence en matière de sécurité nationale en particulier – en fonction de cette nouvelle réalité.

Le deuxième rapport, qui sera publié plus tard en 2021, portera sur les relations entre les organismes de sécurité nationale (en particulier la GRC, le SCRS et l'ASFC) et les communautés racialisées et les autres communautés minoritaires. Dans le cadre de ce rapport, nous communiquerons avec un éventail de personnes et d'organisations de diverses communautés au cours de la deuxième année, ainsi qu'avec les organismes eux-mêmes.

Annexe 1 : Contexte de la transparence de la sécurité nationale

Qu'est-ce que la transparence et pourquoi est-elle importante pour la sécurité nationale?

Les membres du public doivent avoir confiance dans les efforts déployés en matière de sécurité nationale pour maintenir l'efficacité opérationnelle, la résilience démocratique et la crédibilité des institutions du gouvernement. Ce dernier a le devoir de favoriser cette confiance en fournissant en temps opportun au public des renseignements pertinents sur la sécurité nationale et les activités de renseignement connexes afin de permettre l'engagement civique dans l'élaboration des politiques et des activités de sécurité nationale et d'assurer la responsabilisation du public.

Pour obtenir d'autres précisions sur la sécurité nationale et son architecture, veuillez consulter l'annexe 3.

Engagement de transparence en matière de sécurité nationale

L'engagement de transparence en matière de sécurité nationale a été annoncé en 2017. Il vise à améliorer la responsabilisation démocratique du Canada en expliquant au public ce que fait le gouvernement du Canada pour assurer la sécurité nationale, comment il le fait et pourquoi il estime important de le faire.

L'engagement de transparence en matière de sécurité nationale définit six principes directeurs concernant la transparence de la sécurité nationale, regroupés en trois grands domaines :

Transparence des renseignements

1. Les ministères et les organismes diffuseront de l'information expliquant les principaux éléments de leurs activités de sécurité nationale et la portée de ces activités.
2. Dans toute la mesure du possible, les ministères et les organismes aideront et appuieront les Canadiens qui souhaitent accéder à de l'information touchant la sécurité nationale, à condition que l'intérêt national, l'efficacité des opérations ou la sécurité d'une personne ne soit pas compromis.

Transparence des pouvoirs exécutifs

3. Les ministères et les organismes expliqueront comment leurs activités de sécurité nationale sont autorisées par la loi, et comment ils interprètent et appliquent leurs

pouvoirs dans le respect des valeurs canadiennes, dont celles qui sont énoncées dans la *Charte*.

4. Les ministères et les organismes expliqueront, pour ce qui touche à la sécurité nationale, les fondements de leurs processus décisionnels et comment ces processus respectent les valeurs canadiennes, y compris celles qui sont énoncées dans la *Charte*.

Transparence des politiques

5. Le gouvernement informera les Canadiens des enjeux stratégiques ayant une incidence sur la sécurité nationale, et des mesures en cours et des plans prévus pour donner suite à ces enjeux.
6. Dans la mesure du possible, le gouvernement consultera les intervenants et les Canadiens pendant l'élaboration de propositions de politiques d'importance, et il enchâssera la transparence dans la conception des programmes et activités relatifs à la sécurité nationale.

L'engagement a été présenté à la suite des commentaires reçus dans le cadre de la consultation sur la sécurité nationale tenue en 2016¹⁰. Des Canadiens, des intervenants et des experts en la matière ont participé à cette vaste consultation sur des questions liées à la sécurité nationale, y compris la surveillance et la reddition de comptes. Au cours d'une période de quatre mois, les Canadiens ont fourni 58 933 réponses à un questionnaire en ligne et ont envoyé 17 862 courriels. Ils ont également participé à des assemblées publiques, à des événements de mobilisation dirigés par des députés, à des séances en personne, à des événements sur des plateformes numériques et à une table ronde¹¹. De nombreuses réponses ont fait état d'un manque perçu de transparence, ainsi que d'une méfiance à l'égard des institutions de sécurité nationale et d'application de la loi du Canada.

Loi de 2017 sur la sécurité nationale

Le projet de loi C-59, maintenant connu sous le nom de *Loi de 2017 sur la sécurité nationale*, découle également de la consultation sur la sécurité nationale. La *Loi* a établi plusieurs initiatives clés visant à promouvoir la transparence de la sécurité nationale, y compris la création d'un nouvel organisme global d'examen de la sécurité nationale appelé [Office de surveillance des activités en matière de sécurité nationale et de renseignement](#) et la nomination d'un [commissaire au renseignement](#). L'approbation législative de la *Loi* a donné de la crédibilité à l'engagement, une initiative connexe, ce qui a permis d'entreprendre sérieusement la mise en œuvre.

¹⁰ « Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris ». Sécurité publique Canada, 21 décembre 2018, <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/2017-nsc-wwlr/index-fr.aspx>.

¹¹ *Ibid.*

L'objectif de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement est de s'assurer que le travail passé et actuel des institutions de sécurité nationale du Canada est raisonnable, nécessaire et conforme au droit canadien¹². L'Office de surveillance des activités en matière de sécurité nationale et de renseignement agit de façon indépendante pour déterminer les activités gouvernementales à examiner et il a la capacité d'accéder à l'information de tout ministère ou organisme ayant des responsabilités en matière de sécurité nationale dans l'ensemble du gouvernement¹³. Il collabore avec le [Comité des parlementaires sur la sécurité nationale et le renseignement](#), qui a également un vaste mandat d'examen des institutions de sécurité nationale et de renseignement du gouvernement du Canada.

Le commissaire au renseignement exerce une fonction de surveillance puisqu'il examine et autorise de façon indépendante certaines activités de renseignement avant qu'elles ne soient menées. Cette surveillance s'applique au [Service canadien du renseignement de sécurité](#) et au [Centre de la sécurité des télécommunications](#).

L'engagement de transparence en matière de sécurité nationale ne s'accompagne pas de mécanismes d'examen ou de surveillance, mais demande plutôt aux ministères et organismes ayant des responsabilités relatives à la sécurité nationale d'échanger de manière proactive l'information liée à leur travail et de communiquer régulièrement avec le public canadien. Ainsi, l'engagement appuie le travail d'autres initiatives de transparence, notamment l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, le commissaire au renseignement, le Comité des parlementaires sur la sécurité nationale et le renseignement, le [commissaire à la protection de la vie privée](#) et la [commissaire à l'information](#), tout en rendant l'information plus accessible aux Canadiens.

¹² L'Office de surveillance des activités en matière de sécurité nationale et de renseignement a remplacé les organismes suivants et en assume les responsabilités : Comité de surveillance des activités de renseignement de sécurité, Bureau du commissaire du Centre de la sécurité des télécommunications et Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada.

¹³ « Adoption par le Parlement du projet de loi C-59 : la *Loi de 2017 sur la sécurité nationale* – Accroître la responsabilisation et la transparence : Aperçu des nouvelles mesures ». Sécurité publique Canada, 19 juin 2019, <https://www.canada.ca/fr/securite-publique-canada/nouvelles/2019/06/adoption-par-le-parlement-du-projet-de-loi-c-59-la-loi-de-2017-sur-la-securite-nationaleaccroitre-la-responsabilisation-et-la-transparenceapercu-de.html>.

Annexe 2 : Contexte du Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN)

Le Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN) représente une composante essentielle de la mise en œuvre de l'engagement de transparence en matière de sécurité nationale. Le GCT-SN est un groupe consultatif externe dont le mandat est de conseiller le sous-ministre de la Sécurité publique (et, par extension, d'autres ministères et organismes liés à la sécurité nationale) sur la mise en œuvre efficace de l'engagement. Le rapport annuel constitue le principal mécanisme de prestation de conseils du GCT-SN.

Le GCT-SN a été établi pour donner des conseils sur la façon de procéder pour¹⁴ :

- intégrer la transparence dans les politiques, les programmes, les pratiques exemplaires et les activités du Canada en matière de sécurité nationale d'une manière qui accroîtra la responsabilisation démocratique;
- accroître la sensibilisation et la mobilisation du public, ainsi que l'accès à de l'information sur la sécurité nationale et le renseignement associé;
- favoriser la transparence tout en veillant à la sécurité des Canadiens.

Le ministre de la Sécurité publique, Ralph Goodale, a officiellement lancé le GCT-SN en juillet 2019. Les membres ont été choisis en raison de la diversité de leur expérience et de leur expertise dans le milieu universitaire, la société civile et la fonction publique, dans des domaines comme la sécurité nationale, le gouvernement ouvert et les droits de la personne. Le coprésident gouvernemental du GCT-SN est nommé par le sous-ministre de la Sécurité publique. Le coprésident non gouvernemental est choisi par le groupe. Le premier sert de pont entre le gouvernement et le GCT-SN et assure la liaison avec les ministères et organismes chargés de la sécurité nationale, au besoin.

Réunions du GCT-SN

Le GCT-SN a le mandat de se réunir jusqu'à quatre fois par exercice pour discuter de questions liées à la transparence, entendre des conférenciers invités et formuler des conseils à l'intention du sous-ministre. Pour obtenir de plus amples renseignements sur le mandat, la composition et les réunions du GCT-SN, veuillez consulter le mandat du groupe¹⁵.

Entre l'été 2019 et l'hiver 2020, le GCT-SN s'est réuni trois fois en personne. La quatrième réunion était prévue pour la fin de mars 2020, mais, en raison de la pandémie de COVID-19, elle a été remplacée par une série de trois réunions virtuelles qui ont eu lieu tout au long de l'été 2020.

¹⁴ « Groupe consultatif sur la transparence en matière de sécurité nationale (GCT-SN) : Mandat ». Sécurité publique Canada, 31 janvier 2020, <https://www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale/groupe-consultatif-transparence-securite-nationale/mandat.html>.

¹⁵ *Ibid.*

Les premières réunions ont porté sur des exposés présentés par des représentants du gouvernement concernant les rôles et les responsabilités des principales institutions de sécurité nationale. Des représentants des organismes d'examen et de responsabilisation pertinents ont été invités à aider à situer le GCT-SN dans le contexte plus large de la transparence et de la responsabilisation en matière de sécurité nationale.

Au fur et à mesure des réunions, le GCT-SN a également entendu des membres de la société civile, y compris des experts en droit de la sécurité nationale, des représentants d'organisations des droits de la personne, des journalistes et des professionnels de la technologie du secteur privé. Plusieurs thèmes ont été abordés, allant de la diversité et de l'inclusion dans les institutions de sécurité nationale aux répercussions de la lutte contre les menaces numériques sur la vie privée. Pour obtenir un aperçu plus détaillé des sujets abordés, veuillez consulter le graphique de l'annexe 4.

Membres du GCT-SN en date du 7 octobre 2020.

1. **William Baker**, président du Comité ministériel de vérification d'Immigration, Réfugiés et Citoyenneté Canada, ancien sous-ministre de Sécurité publique Canada
2. **Khadija Cajee**, cofondatrice, No Fly List Kids
3. **Mary Francoli**, directrice, Collège des affaires publiques Arthur Kroeger, et doyenne associée, Faculté des affaires publiques
4. **Harpreet Jhinjar**, spécialiste des services de police communautaires et de la mobilisation du public
5. **Thomas Juneau (coprésident non gouvernemental)**, professeur agrégé à l'École supérieure d'affaires publiques et internationales de l'Université d'Ottawa
6. **Myles Kirvan**, ancien sous-ministre délégué de Sécurité publique Canada, ancien sous-ministre de la Justice et sous-procureur général du Canada
7. **Justin Mohammed**, défenseur des droits de la personne et des politiques à Amnesty internationale Canada
8. **Bessma Momani**, professeure de sciences politiques à l'Université de Waterloo et agrégée supérieure de recherche au Centre for International Governance and Innovation
9. **Dominic Rochon (coprésident gouvernemental)**, sous-ministre adjoint principal, Secteur de la sécurité et de la cybersécurité nationale, Sécurité publique Canada
10. **Jeffrey Roy**, professeur à l'École d'administration publique de la Faculté de gestion de l'Université Dalhousie

La durée d'un mandat au sein du GCT-SN est de deux ans, ce qui s'accompagne d'une option de renouvellement d'un an.

Annexe 3 : Architecture du milieu de la sécurité nationale

Qu'est-ce que la sécurité nationale?

Le gouvernement du Canada n'a pas établi de définition récente et officielle de « sécurité nationale ». La dernière politique de sécurité nationale, *Protéger une société ouverte*, adoptée en 2004, portait sur les grandes questions de sécurité nationale suivantes :

- protéger le Canada et les Canadiens, au pays et à l'étranger;
- s'assurer que le Canada n'est pas une source de menaces pour nos alliés;
- contribuer à la sécurité internationale.

Dans le paysage en évolution d'aujourd'hui, les activités de sécurité nationale s'adaptent continuellement pour suivre le rythme des nouvelles menaces, allant du terrorisme et de l'extrémisme violent aux campagnes de désinformation pendant la saison électorale, en passant par les cyberattaques ciblant les bases de données du gouvernement.

Ministères et organismes responsables de la sécurité nationale au Canada

Le gouvernement compte sur un certain nombre de ministères et d'organismes pour cerner et contrer les menaces à la sécurité nationale. Bien que de nombreux ministères et organismes fédéraux aient certaines responsabilités en matière de sécurité nationale, les principales institutions qui composent le milieu de la sécurité nationale du Canada sont les suivantes :

L'[Agence des services frontaliers du Canada](#) fournit des services frontaliers à l'appui des priorités liées à la sécurité nationale et à la sécurité publique et facilite la libre circulation des personnes et des marchandises.

Le [Service canadien du renseignement de sécurité](#) enquête sur les menaces présumées à l'égard de la sécurité du Canada et fait rapport au gouvernement du Canada, prenant parfois des mesures pour réduire ces menaces.

Le [Centre de la sécurité des télécommunications](#) obtient des renseignements électromagnétiques étrangers et aide à protéger les renseignements et les réseaux informatiques de grande importance pour le Canada.

Le [ministère de la Défense nationale et les Forces armées canadiennes](#) appuie les Forces armées canadiennes qui servent au sein de la Marine, de l'Armée de terre, de l'Aviation et des Forces d'opérations spéciales pour défendre les intérêts canadiens au pays et à l'étranger.

[Affaires mondiales Canada](#) s'occupe de la politique étrangère, de la représentation diplomatique et du renseignement étranger et fournit des rapports sur un éventail de questions liées à la sécurité internationale.

Le [Centre intégré d'évaluation du terrorisme](#) analyse les menaces terroristes qui pèsent sur le Canada et sur les intérêts canadiens et recommande le niveau de la menace terroriste au Canada.

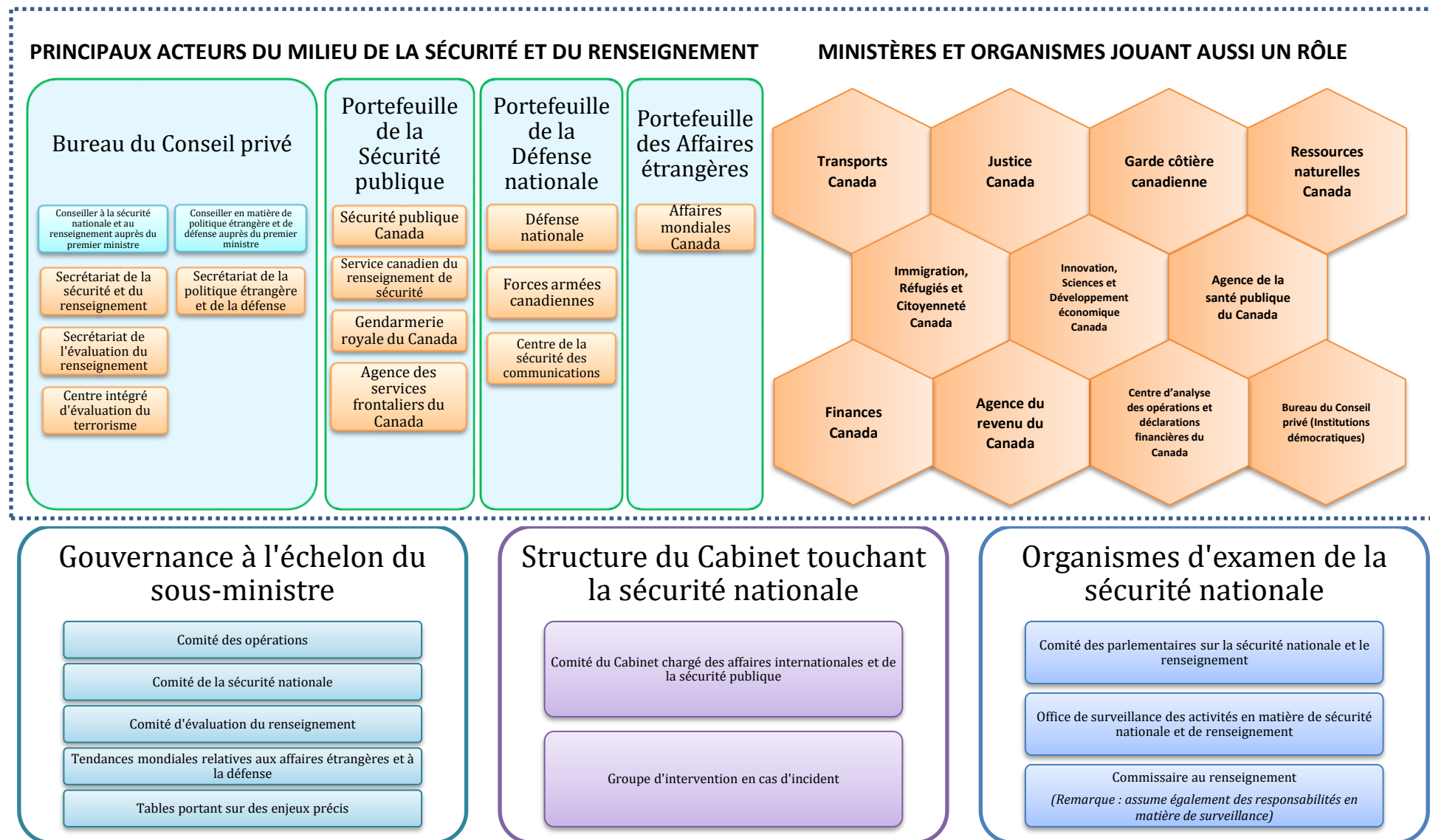
[Sécurité publique Canada](#) coordonne la politique de sécurité nationale (criminalité, terrorisme, cybersécurité, infrastructures essentielles) et les interventions en cas d'urgence et est responsable des organismes du portefeuille – GRC, SCRS, ASFC, Service correctionnel.

[Bureau du Conseil privé](#) : Le Secrétariat de la sécurité et du renseignement, le Secrétariat du renseignement et le Secrétariat de la politique étrangère et de la défense font partie du Bureau du Conseil privé et jouent un rôle important dans la coordination de la prise de décisions stratégiques en matière de sécurité nationale.

La [Gendarmerie royale du Canada](#) prévient la criminalité et mène des enquêtes sur les crimes, applique la loi et s'efforce d'assurer la sécurité du public à l'échelle communautaire, provinciale, territoriale et fédérale.

Architecture du milieu de la sécurité nationale à l'échelle fédérale

REMARQUE IMPORTANTE : LES INFORMATIONS CONTENUES DANS CE GRAPHIQUE SONT SUSCEPTIBLES DE CHANGER. DANS LE CADRE DU RAPPORT, ELLES NE SERONT PAS MIS À JOUR.



Annexe 4 : Points saillants des réunions du GCT-SN, d'août 2019 à septembre 2020

Réunion 1 – 22 et 23 août 2019, Ottawa

Thème/sujet : Discussion interne

- Séances d'information sur l'engagement de transparence en matière de sécurité nationale (ETSN).
- Discussion sur la création d'une source en ligne d'information sur la sécurité nationale accessible au public qui est intéressante, utile et accessible aux Canadiens.
- Besoin d'un changement de culture au sein du gouvernement pour appuyer les futurs efforts en matière de transparence.
- Discussion sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, le Sommet mondial 2019 du Partenariat pour un gouvernement ouvert et les pratiques de transparence de la sécurité nationale dans le Groupe des cinq.

Thème/sujet : Discussion avec le sous-ministre de la Sécurité publique

- Des efforts accrus pour expliquer les activités canadiennes en matière de sécurité nationale et de renseignement contribueraient à dissiper les mythes et la désinformation au sein de la population au sujet de ces activités.

Thème/sujet : Discussion sur le gouvernement ouvert

- Importance de la participation du public aux décisions du gouvernement, tant en personne qu'en ligne.
- Aperçu du cycle de réunions du Forum multi-intervenants sur le gouvernement ouvert, des indicateurs de rendement et des mécanismes de rapport, ainsi que de la façon dont la mobilisation et les discussions continues sont nécessaires pour soutenir ces types d'organismes consultatifs.

Thème/sujet : Discussion avec le SCRS et le CST

- Accroître la transparence au sein du SCRS et du CST en réponse aux besoins du public et afin de mieux combler les lacunes en matière d'information.
- Discussion sur la culture organisationnelle au sein du CST et du SCRS, le rôle des médias dans la communication des questions de sécurité nationale, les lacunes actuelles en matière de connaissances sur les questions de sécurité nationale et la perception et l'expérience du public à l'égard des activités de sécurité nationale du Canada.

Réunion 2 – 1^{er} et 2 décembre 2019, Ottawa

Thème/sujet : Discussion interne

- Conseils sur le recrutement d'un nouveau membre à la suite de la récente démission de Michel Fortmann.
- Examen de la création de sous-groupes pour l'exécution des tâches à venir.
- Rédaction d'un rapport après la quatrième réunion, en mars 2020.

Thème/sujet : Discussion sur l'analyse comparative entre les sexes plus (ACS+) avec des représentants d'Affaires mondiales Canada, du ministère de la Défense nationale (MDN), du ministère des Femmes et de l'Égalité des genres et de Sécurité publique Canada

- Séances d'information portant sur leur expérience et leur expertise respectives en matière de sensibilisation communautaire et d'ACS+.
- Discussions sur le genre, le terrorisme et la lutte contre le terrorisme; l'intersection de l'ACS+ avec la politique de défense du MDN « Protection, Sécurité et Engagement » (PSE); et les répercussions sur le terrain de l'utilisation de l'ACS+.
- Discussion sur l'utilisation de l'ACS+ dans le contexte de la sécurité nationale et du renseignement au Canada, y compris le rôle qu'elle peut jouer dans l'évaluation de potentiels biais de logique employés dans l'intelligence artificielle et les algorithmes.

Thème/sujet : Discussion avec le secrétaire adjoint du Cabinet, Sécurité et renseignement

- Rôle du conseiller à la sécurité nationale et au renseignement au sein du milieu de la sécurité nationale et du renseignement.
- Détermination des publics cibles des rapports antérieurs produits par les organismes d'examen et discussion sur la façon dont le GCT-SN peut choisir de viser un auditoire particulier pour ses propres rapports à l'avenir.

Thème/sujet : Discussion avec le Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)

- Suggestion selon laquelle, dans le cadre de la planification de son premier rapport, le GCT-SN établisse ses priorités en fonction de ce que les Canadiens veulent savoir et de ce qui n'est pas déjà couvert par d'autres comités ou rapports.

Réunion 3 – 2 et 3 février 2020, Ottawa

Thème/sujet : Discussion avec la commissaire à l'information et le commissaire à la protection de la vie privée

- Protection de la vie privée à l'ère numérique et accès public aux renseignements détenus par le gouvernement.
- Programmes de déclassification.
- Accès du gouvernement à des renseignements personnels de citoyens pour des raisons de sécurité nationale (p. ex. par l'entremise des médias sociaux).

Thème/sujet : Discussion avec la chef adjointe du renseignement de la Défense du ministère de la Défense nationale

- Discussion sur les initiatives qui pourraient être organisées à l'avenir pour accroître la transparence au ministère de la Défense nationale, y compris la formation des employés.

Thème/sujet : Discussion avec les représentants de la société civile

- Allégations d'inconduite mettant en cause des organismes chargés de la sécurité nationale.
- Importance d'accroître la compréhension du public concernant le travail de ces organismes au moyen de la responsabilisation et de la transparence, de mobiliser régulièrement

diverses collectivités et de régler les problèmes liés à la culture en milieu de travail au sein du gouvernement.

- Transparence pour ce qui touche les décisions judiciaires, les instructions du ministre et les décrets.

Thème/sujet : Discussion avec un groupe de journalistes

- Difficulté à accéder à des données classifiées antérieures par l'entremise du mécanisme de la *Loi sur l'accès à l'information*.
- Le manque de communication d'information par le gouvernement après des incidents touchant la sécurité nationale peut avoir des répercussions négatives sur les groupes et les collectivités marginalisés. De plus, lors de tels incidents, les lacunes dans les communications laissent place à des entités nuisibles qui peuvent s'y faufiler pour compromettre nos valeurs et nos institutions démocratiques.
- Recommandations visant à améliorer les liens entre le gouvernement et les médias. Par exemple, participer à des entrevues en personne ou par téléphone; fournir en temps opportun de l'information importante dans le cadre de conférences de presse et de séances d'information techniques; et diffuser de manière proactive aux médias et au public canadien de l'information sur des incidents touchant la sécurité nationale.

Réunion informelle – 20 mai 2020, virtuelle

Thème/sujet : Discussion interne

- Discussion informelle du GCT-SN sur la planification des prochaines réunions du GCT-SN à la lumière de la pandémie de COVID-19.

Réunion 4.1 – 10 juin 2020, virtuelle

Thème/sujet : Discussion avec des conférenciers invités : La protection de la confidentialité, l'intelligence artificielle, le monde numérique et la cybersécurité : les attentes et les besoins des Canadiens en matière d'information sont-ils respectés?

- Rétablir la confiance que les Canadiens portent envers les organismes responsables de la sécurité nationale au moyen de la transparence et de la responsabilisation.
- Il n'y a pas suffisamment de normes d'évaluation qui peuvent être appliquées et évaluées de manière uniforme et rigoureuse par les organismes d'examen de la sécurité nationale.
- Les institutions de sécurité nationale devraient fournir plus de renseignements sur l'interprétation des pouvoirs juridiques.
- Amélioration de la communication et de l'éducation afin de renforcer le discours public et les débats parlementaires sur les sujets suivants : collecte, utilisation et stockage des données; précision sur la façon dont les lois sont interprétées; amélioration du processus de publication des ministères et organismes fédéraux responsables de la sécurité nationale.
- Amélioration des débats publics et des activités de sensibilisation inclusives pour améliorer la capacité du gouvernement d'approfondir les enjeux auprès du public.
- Le gouvernement doit fournir des directives claires et de meilleures possibilités de partenariat au secteur privé dans le domaine de l'intelligence artificielle.

Réunion 4.2 – 10 juillet 2020, virtuelle

Thème/sujet : Discussion avec les invités : Sécurité nationale et droits de la personne : comment les droits individuels des Canadiens influencent-ils les initiatives de transparence connexes?

- Besoin de responsabilisation là où nous disposons du niveau de transparence requis à cette fin.
- Suggestions de mesures concrètes possibles pour combler l'écart et établir un lien de confiance entre les ministères et organismes responsables de la sécurité nationale et les collectivités qui se sentent ciblées par leur travail.
- Sentiment d'aliénation du public en raison de l'utilisation de listes prescrites par la loi et du recours à des procédures judiciaires à deux volets, à des processus ex parte et à des avocats spécialisés en sécurité nationale.
- Les gens sont réticents à divulguer des renseignements lorsqu'ils ne connaissent pas la finalité du processus de collecte.
- Les Canadiens doivent avoir accès aux outils et aux renseignements de base qui leur permettent de gérer leurs interactions avec les institutions de sécurité nationale.
- Il est important de traiter les signalements de discrimination et de harcèlement au sein des institutions de sécurité nationale.
- Il faut réexaminer les façons de joindre les Canadiens et de communiquer avec eux et veiller à inclure les intervenants pertinents qui n'ont peut-être pas l'occasion de participer à des discussions à huis clos.

Réunion 4.3 – 22 juillet 2020, virtuelle

Thème/sujet : Rôle de l'ASFC et de la GRC en matière de sécurité nationale et de renseignement

- Discussions sur le rôle, le mandat et le milieu opérationnel de l'ASFC et de la GRC, la façon dont leurs ministères respectifs cadrent dans le milieu élargi de la sécurité nationale et du renseignement et la façon dont les deux organisations mobilisent les Canadiens et communiquent avec eux.
- Discussions sur les initiatives de transparence et de reddition de comptes, le rôle provincial et fédéral de la GRC en matière de services de police, la diversité et l'inclusion et les répercussions d'un monde numérique en rapide évolution sur les activités de l'ASFC et de la GRC.

Thème/sujet : Rôle de la Commission de services policiers de Toronto (CSPT) en matière de surveillance et d'examen de la sécurité nationale et à l'échelle municipale

- Discussion sur le rôle et les responsabilités de la CSPT.
- Discussion sur des exemples de collaboration intergouvernementale entre les divers ordres de gouvernement.
- Pratiques exemplaires et méthodes de la Ville pour réussir à mobiliser le public.
- Principales pratiques de transparence, notamment en ce qui concerne l'accès du public à des données pertinentes.

Réunion informelle – 9 septembre 2020, virtuelle

Thème/sujet : Discussion interne

- Travaux internes du GCT-SN sur la rédaction du premier rapport annuel et le traitement des questions en suspens.
- Les membres conviennent de poursuivre l'élaboration du rapport hors ligne.
- Planification des activités du groupe pour la deuxième année, y compris les thèmes des réunions et les rapports.

Annexe 5.1 : Analyse internationale de la transparence de la sécurité nationale

IMPORTANT : LA PRÉSENTE ANNEXE ET LES RENSEIGNEMENTS QU'ELLE CONTIENT ONT ÉTÉ VÉRIFIÉS POUR LA DERNIÈRE FOIS LE 20 OCTOBRE 2020 ET SONT SUSCEPTIBLES DE CHANGER. DANS LE CADRE DU PRÉSENT RAPPORT, ILS NE SERONT PAS MIS À JOUR. DE PLUS, CERTAINES INFORMATIONS NE SONT PAS DISPONIBLES EN FRANÇAIS.

Le tableau ci-dessous donne un aperçu des politiques relatives à la transparence de la sécurité nationale et du renseignement (SNR) et des caractéristiques des institutions de SNR dans sept pays. Puisque le mandat du GCT-SN consiste à conseiller le sous-ministre de Sécurité publique Canada sur l'amélioration des politiques sur la transparence en matière de SNR, ce tableau fournit des points de vue comparatifs pour faciliter un examen critique du contexte canadien.

Aux fins du présent tableau, la « transparence » désigne les politiques et les programmes des organismes de sécurité nationale et de renseignement qui divulguent à leurs citoyens, de façon proactive ou réactive, des renseignements sur leurs activités, politiques, programmes et recherches. Toute l'information fournie ci-dessous est fondée sur des renseignements accessibles au public. Chaque pays est examiné selon sept aspects :

- Initiatives actuelles relatives à la transparence de la sécurité nationale et du renseignement
- Organismes de surveillance et d'examen des activités en matière de sécurité nationale et de renseignement
- Lois sur l'accès à l'information
- Système et politique de déclassification
- Données tirées de rapports accessibles au public et de leurs sites Web correspondants
- Instituts de recherche sur les politiques (ou groupes de réflexion) dans le domaine de la sécurité nationale et du renseignement
- Société civile et groupes de défense des intérêts

Pour une lecture plus approfondie, une analyse détaillée de la relation entre les pays du Groupe des cinq et leurs organismes correspondants de surveillance des activités en matière de SNR peut être consultée à la [Bibliothèque du Parlement](#).

Notes importantes concernant le tableau qui suit :

¹ Veuillez noter qu'il ne s'agit pas d'une liste exhaustive de toutes les initiatives de transparence possibles dans les pays comparés.

² Veuillez également noter qu'il ne s'agit pas d'une liste exhaustive de toutes les données et de tous les renseignements disponibles sur le site Web des activités de SNR de chaque pays.

³ Il ne s'agit pas d'une liste exhaustive de tous les groupes de réflexion de chaque pays. Le tableau vise à dresser la liste des plus importants groupes de réflexion qui mènent des recherches sur la sécurité nationale, la défense, le renseignement, la cybersécurité et la protection de la vie privée. Les rapports annuels des principaux groupes de réflexion se trouvent à l'adresse suivante : https://repository.upenn.edu/think_tanks/.

⁴ Il ne s'agit pas d'une liste exhaustive de tous les groupes de défense en matière de SNR.

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
CANADA	Sécurité publique Canada - Engagement de transparence en matière de sécurité nationale (ETSN) - Rapports publics sur la menace terroriste pour le Canada (RPMPT) - Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères, 2019 - Plan fédéral d'intervention en cas d'acte terroriste (PFIAT) - Renforcer la résilience face au terrorisme : Stratégie antiterroriste du Canada (2013) - Centre de coordination stratégique sur la communication d'information Service canadien du renseignement de sécurité (SCRS) - Rapport public de 2018 Ministère de la Défense nationale (MDN) - Accroître la transparence et la rapidité des communications aux associations des industries de la défense Centre de la sécurité des télécommunications (CST)	Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) - Rapports classifiés aux ministres concernés. - Les rapports annuels non classifiés au premier ministre doivent être déposés au Parlement. Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) – Examine le cadre du milieu de la sécurité nationale et du renseignement du Canada, ainsi que les ministères qui n'étaient pas auparavant soumis à un examen externe. - Rapport annuels du CPSNR (caviardé) - Rapports spéciaux Le Bureau du commissaire au renseignement (aucun rapport publié) – Le Bureau effectue un examen quasi judiciaire des autorisations et des décisions ministérielles touchant le Centre de la sécurité des télécommunications	<i>Loi sur l'accès à l'information</i> (1983) En 1983, la <i>Loi</i> a établi le Commissariat à l'information du Canada. La <i>Loi</i> prévoit des exemptions pour refuser l'accès à l'information, y compris la défense et la sécurité du Canada et de tout État allié ou associé avec le Canada.	Système de déclassification - Pas de système de déclassification automatique des documents. Directive sur la gestion de la sécurité du Conseil du Trésor (2019) - Directives pour gérer la sécurité du gouvernement afin d'appuyer la prestation des programmes et des services du gouvernement fédéral et la protection de l'information, des personnes et des biens. Portail du gouvernement ouvert – Demandes d'accès à l'information complétées - Permet de rechercher des résumés de demandes d'accès à l'information complétées. - Des copies des dossiers doivent être demandées, sans frais.	Commissariat à l'information du Canada (CIC) - Le rapport concernant l'administration de la <i>Loi sur l'accès à l'information</i> donne un aperçu du nombre total de demandes, du nombre de pages traitées, du nombre de demandes traitées dans les délais prévus et du temps moyen de traitement. - Les rapports annuels du CIC fournissent des statistiques sur le traitement des plaintes de 24 institutions. Rapports annuel du CPSNR (caviardé) - Permet d'examiner le cadre du milieu de la sécurité nationale et du renseignement du Canada - Comprend l'examen du CPSNR à l'égard de l'Agence des services frontaliers du Canada, de la diversité et de l'inclusion dans le milieu de la sécurité et du renseignement du Canada, etc. Rapport public de 2018 du SCRS - Rapport sur l'évaluation des menaces à la sécurité au Canada - Statistiques sur les programmes d'immigration et de filtrage du gouvernement.	Instituts de recherche en matière de SNR du gouvernement fédéral - Innovation pour la défense, l'excellence et la sécurité (MDN) - Institut Tutte - Horizons de politiques Canada Recherches propres à la SNR : - Canadian Network For Research On Terrorism, Security And Society - Centre for International and Defence Policy - The Citizen Lab - Association canadienne pour l'OTAN - Vanguard Instituts de recherche sur les politiques ayant comme domaine d'intérêt la SN : - Institut canadien des affaires mondiales - Clinique d'intérêt public et de politique d'Internet du Canada - Centre for International Governance Innovation - Conference Board du Canada	Groupes nationaux : - Conseil canadien des affaires - Association canadienne des libertés civiles - Canadian Anti-Hate Network - Fondation canadienne des relations raciales - Coalition pour la surveillance internationale des libertés civiles (cliquez sur le lien pour obtenir la liste des organisations membres) - International Human Rights Watch - No Fly List Kids Groupes régionaux : - BC Freedom of Information And Privacy Association Sections provinciales de l'ACLIC à Moncton, Montréal, Kingston, Regina, Saint John, Vancouver, Timmins, Fredericton, London

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
	- Rapports annuels - Divulgateur proactive - Centre canadien pour la cybersécurité - Alertes et avis - Collaboration avec le secteur privé - Relations avec le milieu universitaire - Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) - Directives sur les politiques et les lois, notamment les publications techniques - Évaluation des risques de financement d'activités terroristes 2018 - Produits de renseignements stratégiques	(CST) et le Service canadien du renseignement de sécurité (SCRS).			Autres rapports à considérer (peuvent ne pas contenir de données précises) : - Rapport public sur la menace terroriste pour le Canada. - Rapport annuel du Centre de la sécurité des télécommunications.	- Macdonald Laurier Institute Autres instituts de recherche sur les politiques dignes de mention ayant des projets à court terme liés à la SN : - Fondation Asie Pacifique du Canada - Institut Broadbent - Conseil international du Canada/Open Canada - Institut Fraser - IRPP/Options politiques - Forum des politiques publiques	- Digital Justice Lab - Ligue des droits et libertés
ÉTATS-UNIS	Office of the Director of National Intelligence (ODNI) - Site Web centralisé qui sert de portail aux organisations du milieu de la SNR aux États-Unis. - Dirige l'intégration et la coordination du milieu du renseignement du pays. - En 2015, l'ODNI a publié le document intitulé Principles of Intelligence Transparency et le Transparency Implementation Plan à	ODNI - Statistical Transparency Report Regarding National Security Authorities - National Intelligence Strategy - The ICOTR Transparency Tracker - Annual Report on Security Clearance Determinations - Interagency Security Classification	<i>Freedom of Information Act</i> (FOIA, 1966) Aucun commissaire à l'information officiel, mais la Federal Trade Commission (FTC), a pris des mesures relativement à des atteintes à la sécurité des données et à la vie privée. La FOIA comprend neuf exemptions, y	Système de déclassification – L' EO 13526 (2009) établit les mécanismes pour la plupart des activités de déclassification. - L'organisme d'origine attribue une date de déclassification (10 ans par défaut). - Examen automatique de la déclassification après 25 ans, à moins que les documents ne correspondent à l'une des neuf exceptions.	Statistical Transparency Report Regarding National Security Authorities - Fournit au public des statistiques sur la fréquence à laquelle le gouvernement exerce des pouvoirs essentiels en matière de SN (p. ex. FISA) et une explication de la façon dont le milieu du renseignement exerce ces pouvoirs.	Instituts de recherche en matière de SNR parrainés par le gouvernement fédéral : - Arroyo Center (R et D) - Center for Communications and Computing - Center for Naval Analyses - Defense Advanced Research Projects Agency (R et D)	Groupes nationaux : - American Civil Liberties Group - Americans for Prosperity - Amnesty International – États-Unis - The Brennan Center for Justice (Université de New York)

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
	l'intention du milieu du renseignement des États-Unis afin d'améliorer la compréhension du public à l'égard de ce milieu et d'institutionnaliser la transparence. - National Intelligence Council (NIC) – agit à titre de groupe de réflexion de l'ODNI; produit les évaluations du milieu du renseignement sur les questions de SN et les tendances mondiales. Cybersecurity and Infrastructure Security Agency (CISA) - Échange d'information : Ressource vitale pour la sécurité et la résilience des infrastructures essentielles - National Infrastructure Coordinating Center - Critical Infrastructure Cyber Community C³ Voluntary Program Sécurité intérieure - Homeland Security Information Network Open Government Plan (PDF) – décrit les initiatives nouvelles ou élargies visant à accroître la transparence, ainsi que les initiatives en cours.	Appeals Panel (ISCAP) – Organisme interagences qui fournit au public et aux utilisateurs du système de classification une tribune pour examiner de manière plus approfondie les décisions de classification. - L'organisme s'est prononcé en faveur de la divulgation des documents de la CIA dans plus de 60 % des cas. - Le registre des documents communiqués et des appels de l'ISCAP est disponible sur le site Web. Congrès des É-U U.S. House Oversight Subcommittee on National Security - La compétence comprend la surveillance de la sécurité nationale, de la sécurité intérieure et de la politique étrangère (y compris les relations des États-Unis avec d'autres pays; l'immigration; la défense; les questions touchant les anciens combattants; et la surveillance de la politique d'acquisition fédérale liée à la sécurité nationale et la compétence législative connexe).	compris le refus de répondre à des demandes afin de protéger la sécurité nationale. La CIA tire parti des exemptions en vertu de la FOIA pour protéger les sources, les méthodes et les renseignements relatifs à la sécurité nationale. Loi sur la biométrie (à l'échelle des États) : - L'Illinois, le Texas et l'État de Washington ont adopté des lois sur la protection des renseignements personnels biométriques qui visent à réglementer la collecte, la conservation et l'utilisation des données biométriques. - D'autres États (Arizona, Floride et Massachusetts) envisagent également des propositions semblables. - « The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States » - Analyse des lois étatiques sur la biométrie par le	- À 50 ans, il y a deux exceptions. - La classification au-delà de 75 ans nécessite des autorisations spéciales. National Archives and Records Administration (NARA) - National Declassification Centre - Interagency Security Classification Appeals Panel ODNI - IC on the Record (ICOTR) - Créé en 2013 pour fournir au public un accès direct à des renseignements factuels liés aux activités licites de surveillance à l'étranger menées par le milieu du renseignement. - Le site Tumblr affiche l'emplacement des documents précédemment publiés. Déclassification et transparence de la NSA - Liens vers les documents, y compris les rapports et les communiqués liés à la FOIA, les documents historiques, les publications internes de la NSA, etc.	National Intelligence Strategy - Décrit les activités et les résultats nécessaires pour que le milieu du renseignement puisse fournir en temps opportun des renseignements, éclairés, objectifs et pertinents. - Fournit un objectif pour le milieu du renseignement. - Facteurs influant sur le rendement du milieu du renseignement (réalisations, risques, défis). - Fournit un diagramme et des explications concernant tous les éléments du milieu du renseignement. ICOTR Transparency Tracker - Statistiques sur les documents publiés, y compris les documents déclassifiés antérieurement. Report on Security Clearance Determinations – rapport annuel - Rapport annuel sur l'état actuel des autorisations de sécurité du gouvernement américain. - Statistiques sur le nombre total de personnes dans l'ensemble du gouvernement qui sont admissibles à avoir accès à l'information classifiée, qui y ont accès et qui y sont admissibles, mais qui n'y ont pas accès.	- MIT Lincoln Laboratory - National Institute of Standards and Technology Recherches propres à la SNR : - Carnegie Endowment for International Peace - Center for a New American Security - Center for Security and Emerging Technology - Center for Strategic and Budgetary Assessments - Federation of American Scientists - GW Cyber and Homeland Security Programs - James Martin Center for Nonproliferation Studies - National Consortium for the Study of Terrorism and Responses to Terrorism Instituts de recherche sur les politiques ayant comme domaine d'intérêt la SN : - The Atlantic Council - Belfar Center	- Center for Democracy and Technology - Constitutional Alliance - Defending Rights & Dissent - Demand Progress - Digital Welfare State and Human Rights Project - Electronic Privacy Information Center - Human Rights Watch - Project on Government Oversight - U.S. Global Leadership Coalition Groupes régionaux : - Sections de l'ACLU dans chaque État, à Washington (D.C.) et à Porto Rico

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
		<u>U.S. Senate Select Committee on Intelligence</u> - Superviser et effectuer des études continues des activités et des programmes de renseignement du gouvernement des États-Unis. - Soumettre au Sénat des propositions législatives appropriées et lui faire rapport de ces activités et programmes de renseignement. - Effectuer une surveillance législative attentive des activités de renseignement des États-Unis afin de s'assurer que ces activités sont conformes à la Constitution et aux lois des États-Unis. <u>U.S. Senate Committee on Homeland Security and Governmental Affairs</u> - Compétence étendue relative aux opérations gouvernementales en général et au département de la Sécurité intérieure en particulier. - Étudie l'efficacité, l'économie et l'efficacité de tous les organismes et ministères du gouvernement fédéral.	National Law Review			- <u>Brookings Institution</u> - <u>Cato Institute</u> - <u>Center for Strategic and International Studies</u> - <u>Council on Foreign Relations</u> - <u>Hudson Institute</u> - <u>Rand Corporation</u>	

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
ROYAUME-UNI	<i>Investigatory Powers Act</i>, 2016 Fournit un nouveau cadre pour régir l'utilisation et la surveillance des pouvoirs d'enquête par les organismes d'application de la loi et les organismes de sécurité et de surveillance. Intelligence and Security Committee of Parliament - Liens accessibles vers les rapports, la liste des organisations surveillées par le Comité, les organismes de surveillance du renseignement et les lois pertinentes.	Intelligence and Security Committee of Parliament (ISC) – Comité du Parlement ayant la responsabilité légale de surveiller le milieu du renseignement du R.-U. - Rapports annuels (de 1995 à aujourd'hui) - Réponses du gouvernement et déclarations ministérielles écrites - Rapports spéciaux Independent Reviewer of Terrorism Legislation – éclaire le débat public et politique sur la loi antiterroriste. - Relève du Secrétaire de l'Intérieur et du Parlement. - Témoignages devant les comités parlementaires - Articles et discours Investigatory Powers Commissioner's Office (IPCO) – surveille de façon indépendante et autorise l'utilisation de pouvoirs d'enquête par les organismes de renseignement, les forces policières et d'autres autorités publiques	<i>Freedom of Information Act</i> (FOI, 2000) L'Information Commissioner's Office a été créé en 1984 à titre de registraire de la protection des données. L'ICO s'est vu confier la responsabilité supplémentaire de la FOI en 2001 et a changé son nom pour Information Commissioner's Office. La FOI du R.-U. comprend 23 exemptions, divisées en 2 types : absolues et non absolues. Les questions de sécurité sont classées comme l'une des exemptions absolues. Par conséquent, tous les organismes de sécurité (p. ex. MI5, MI6, GCHQ) sont exemptés des demandes de divulgation. Data Protection Act (2018) – fondée sur le <i>Règlement général sur la protection des données</i> de l'Union européenne; remplace la <i>Data</i>	Système de déclassification - Aucun système de déclassification automatique des documents. - La FOI exige la communication de l'information, sauf dans les cas où il y a des motifs de confidentialité. National Cyber Security Centre (NCSC) – indicateurs de compromission - Déclassifier les documents de nature délicate au moyen d'un système automatisé capable de déterminer ce qui peut être communiqué en quelques secondes. - Defence and Security Media Advisory (DSMA) Committee dirigé par le ministère de la Défense. - Le système d'avis du DSMA est un moyen de fournir des conseils et des directives aux médias au sujet de l'information sur la défense et la sécurité dont la publication pourrait compromettre la sécurité nationale. Il s'agit d'un moyen volontaire d'encourager les médias à ne pas publier certains renseignements.	Rapports annuels de l'ISC - Description détaillée des travaux du comité, des évaluations du renseignement portant sur des menaces spécifiques et des dépenses (documents caviardés). NCSC - Fiche d'information sur les indicateurs de compromission, qui permet aux organisations d'obtenir rapidement des renseignements sur les activités numériques malveillantes à des points centraux du réseau. Les organisations peuvent utiliser les indicateurs de compromission pour retracer le système infecté. Investigatory Powers Tribunal - Fait le suivi du volume de plaintes au fil du temps, du nombre de plaintes par organisation, du nombre d'audiences publiques et des résultats des audiences par année - Publication des décisions par le Tribunal. IPCO - Le rapport annuel fournit la méthode d'inspection en fonction de l'expertise des inspecteurs de l'IPCO. Il décrit également comment l'approche a changé.	Instituts de recherche en matière de SNR du gouvernement fédéral : - Defence and Security Accelerator - Defence Science and Technology Laboratory Recherches propres à la SNR : - International Institute for Strategic Studies - The Royal Institute of International Affairs (Chatham House) - The Royal United Services Institute - United Kingdom National Defence Association Instituts de recherche sur les politiques ayant comme domaine d'intérêt la SN : - Future of Humanity - Google DeepMind (accent mis sur l'IA) Instituts généraux de recherche sur les politiques ayant des projets à court terme liés à la SN : - Civitas : Institute for the Study of Civil Society - Equality and Human Rights Commission	Groupes nationaux : - Amnesty International - R.-U. - Big Brother Watch - Centre for Policy Studies - Defend the Right to Protest - Liberty - Open Rights Group - Privacy International

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
		- Rapports annuels de l'PCO Investigatory Powers Tribunal – Instance judiciaire qui enquête sur les plaintes relatives à la conduite des acteurs du milieu du renseignement du R.-U., du MI5, du SIS et du GCHQ. Biometrics Commissioner – poste établi en vertu de la <i>Protection of Freedoms Act</i> de 2012; le commissaire est un conseiller indépendant du gouvernement. Il examine la conservation et l'utilisation des données biométriques par la police.	<i>Protection Act</i> de 1998.			- Institute for Public Policy Research - New Local Government Network	
AUSTRALIE	Office of National Intelligence (ONI) - L'ONI est un élément clé de la formation de la National Intelligence Community (NIC). - L'ONI est responsable de la gestion organisationnelle de la NIC et agit comme point de responsabilité unique devant le premier ministre et le National Security Committee of Cabinet. Office of National Assessments (ONA)	Inspector-General of Intelligence and Security (IGIS) – Bureau indépendant établi en vertu de la loi qui veille à la légalité et au bien-fondé des mesures prises par le milieu du renseignement de l'Australie, enquête sur les plaintes et mène des examens concernant les organismes de l'AIC et d'autres ministères du Commonwealth responsables de la sécurité nationale.	<i>Freedom of Information Act</i> (FOI, 1982), gouvernement fédéral. La FOI a été modifiée en 2010 pour créer l'Office of the Information Commissioner. La FOI prévoit 10 exemptions, y compris en ce qui concerne les documents qui touchent la sécurité nationale, la défense	Système de déclassification - L'organisme d'origine de l'information demeure responsable du contrôle du nettoyage, de la reclassification ou de la déclassification de son information. - L'organisme d'origine peut définir une date ou un événement particulier en vue de la déclassification automatique.	Rapports annuels de l'IGIS - Cela comprend l'énoncé de rendement annuel, y compris l'objectif, les programmes pertinents, les résultats et l'analyse. - Indicateurs de rendement concernant les enquêtes, les inspections et les enquêtes sur les plaintes - Données sur les divulgations d'intérêt public par organisme et par source.	Instituts de recherche en matière de SNR du gouvernement fédéral : - National Security Science and Technology Centre Recherches propres à la SNR : - Air Power Australia - Australia Defence Association - Australian Strategic Policy Institute - SAGE International Australia	Groupes nationaux : - Australian Council For International Development - Australia Privacy Foundation - Digital Rights Watch - Human Rights Law Centre - Refugee Council of Australia

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
	- Open Source Centre (OSC) – recueille, interprète et diffuse de l'information relative à des questions ayant une importance politique, stratégique ou économique pour appuyer les priorités du gouvernement en matière de renseignement et le travail de la NIC. Australia-New Zealand Counter-Terrorism Committee - Accord entre les deux pays pour assurer la coordination des activités de lutte contre le terrorisme. - Tient à jour les documents portant sur le National Counter-Terrorism Plan et facilite l'échange d'information entre les organismes et les administrations.	- L'IGIS produit un rapport annuel, mais celui-ci n'est pas disponible actuellement. Parliamentary Joint Committee on Intelligence and Security – mène des enquêtes sur des questions qui lui sont renvoyées par le Sénat, la Chambre des représentants ou un ministre du gouvernement du Commonwealth. - Enquêtes et rapports pour chaque législature.	ou les relations internationales.			- Strategic & Defence Studies Centre Autres instituts de recherche sur les politiques dignes de mention ayant des projets liés à la SN : - The Centre for Independent Studies - Institute for Government	
NOUVELLE-ZÉLANDE	Government Communications Security Bureau (GCSB) - Examen de la conformité au GCSB - Rapport annuel - Mécanismes externes de surveillance New Zealand Security Intelligence Service (NZIC) - À l'instar du GCSB, le NZIC a rendu accessibles son propre mécanisme de	Inspector-General of Intelligence and Security (IGIS) – Assure une surveillance indépendante du New Zealand Security Intelligence Service et du Government Communications Security Bureau. L'IGIS peut mener des enquêtes et des examens touchant les organismes de renseignement. - Rapports de l'IGIS - rapports d'enquête,	<i>The Official Information Act (OIA, 1982)</i> Le Bureau de l'ombudsman, créé en 1962, est un organisme semblable au Commissariat à l'information du Canada. L'ombudsman du pays enquête sur les plaintes visant des organismes gouvernementaux.	Politique de déclassification - L'organisme d'origine devrait établir des procédures d'examen de la classification. - Processus de déclassification ponctuel en fonction des demandes traitées en vertu de l'OIA. - La déclassification systématique dépend du ministère. - Le Ministry of Foreign Affairs and Trade (MFAT) dispose d'un vaste programme	Publication de l'IGIS - Mandats liés au renseignement délivré. - Rapports publics sur des enquêtes précises comprenant des pratiques exemplaires et des recommandations. - Étude longitudinale des plaintes relatives aux activités de renseignement à l'étranger. Programme de déclassification du MFAT - Dossier des documents communiqués à ce jour.	Recherches propres à la SNR : - Centre for Strategic Studies New Zealand	Groupes nationaux : - Amnesty International - N.-Z. - Human Rights Foundation

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
	surveillance et ses rapports annuels . Australia-New Zealand Counter-Terrorism Committee (consultez la section sur l'Australie pour obtenir de plus amples renseignements)	examens, pratiques exemplaires. - Rapports annuels - Enquêtes en cours - Discours et publications	L'OIA énonce les conditions à respecter pour refuser l'accès à l'information, y compris la sécurité nationale et la défense de la N.-Z. (OIA, partie 1, article 6).	permanent d'examen et de communication de documents classifiés depuis au moins 25 ans.			
ALLEMAGNE	Le ministère fédéral de l'Intérieur, de la Construction et du Territoire publie divers rapports sur son site Web. - Rapports annuels sur la prévention de la corruption dans l'administration fédérale. - Indique explicitement que le rapport exclut les organismes de renseignement fédéraux allemands pour éviter de révéler des renseignements de nature délicate. Service de renseignement national de l'Allemagne (BfV) - Fournit des renseignements au Federal Ministry of the Interior, Building and Community dans le cadre de son rapport annuel. - Publication de rapports annuels et de rapports sommaires sur l'extrémisme de droite, l'islamisme, la cybersécurité et la protection contre l'espionnage industriel	Commission de contrôle parlementaire (la Commission) – La <i>Parliamentary Scrutiny of Federal Intelligence Activities Act</i> permet à la Commission d'enquêter sur le Bureau fédéral de protection de la Constitution (BfV), le service de contre-espionnage militaire (MAD) et le service fédéral de renseignement (BND). La Commission enquête sur l'obligation de divulgation du gouvernement fédéral, puisque le gouvernement fédéral est tenu de fournir volontairement les renseignements suivants : - Activités générales des organismes de renseignement. - Surveillance des communications privées.	<i>Freedom of Information Act</i> (FOI, 2006) Le commissaire fédéral à la protection des données et au droit à l'information (BfDI) est l'organisme chargé de superviser la protection des données. La FOI de 2006 lui a ajouté une fonction d'ombudsman. En 2016, le BfDI est devenu un organisme indépendant. Les services de renseignement étrangers de l'Allemagne et certaines activités des services de police fédéraux sont exemptés de la divulgation dans le cadre des demandes d'information.	Politique de déclassification - Les documents classifiés sont déclassifiés par les archives fédérales allemandes après 30 ans, sauf indication contraire. La durée de la classification ne peut être prolongée qu'une seule fois, pour 30 années supplémentaires. - Des exceptions s'appliquent aux renseignements personnels, qui ne sont déclassifiés que 10 ans après le décès de la personne. - Aucun examen périodique des documents classifiés. - Des documents liés à l'ancienne République démocratique allemande ont été rendus accessibles dans un délai minimal.	Ministère fédéral de l'Intérieur, de la Construction et du Territoire - Rapports annuels présentant des données et des tendances relatives à la criminalité, à l'extrémisme, au terrorisme et à l'espionnage. Le rapport est fondé sur les renseignements recueillis par le BfV. - Statistiques sur la criminalité policière Commission de contrôle parlementaire - Rapports annuels sur ses activités, rapports d'évaluation, rapport sur les mesures prises en vertu de la <i>Counter Terrorism Act</i>. Service de renseignement national de l'Allemagne - Rapports dressant la liste des groupes faisant l'objet d'une surveillance et donnant une vue d'ensemble de ceux-ci. Commissaire fédéral à la protection des données et au droit à l'information (BfDI)	Instituts de recherche en matière de SNR du gouvernement fédéral : - High-Tech Strategy 2025 Recherches propres à la SNR : - George C. Marshall European Center for Security Studies - German Institute for International and Security Affairs - Initiative européenne pour la stabilité – ESI - Federal Academy for Security Policy Instituts de recherche sur les politiques dignes de mention ayant comme domaine d'intérêt la SN : - Fondation Friedrich Ebert - German Council on Foreign Relations - Transparency International	Groupes nationaux : - Algorithm Watch - German League for Human Rights - Society for Threatened Peoples International

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
	- Ligne d'aide pour la lutte contre le terrorisme - Aperçu des domaines d'activité du BfV Enquête de la commission parlementaire allemande sur le scandale d'espionnage de la NSA - En 2014, la commission a commencé à enquêter sur les services secrets américains qui espionnaient l'Allemagne et à élaborer une stratégie sur la façon de protéger les télécommunications allemandes. - Présentation des conclusions au Parlement. Le rapport fournit également des renseignements sur les activités d'espionnage de l'Allemagne visant ses alliés.	- Collecte secrète de données, y compris les demandes d'information des organismes de renseignement présentées à d'autres organisations. La Commission peut obliger les services de renseignement à lui remettre des éléments de preuve. Toutefois, les organismes de renseignement peuvent refuser de divulguer des renseignements à la Commission dans certaines circonstances (p. ex. protection des sources, atteinte aux droits d'une personne). La Commission fait également régulièrement rapport au Parlement fédéral. Commission G10 du Parlement - La Commission examine et autorise les demandes du gouvernement fédéral pour permettre aux organismes de renseignement d'intercepter des communications privées. Elle a le pouvoir de mettre fin aux mesures de surveillance qu'elle juge illégales. - Elle peut également enquêter sur des			- Rapports annuels qui évaluent la protection des données et l'accès à l'information dans tous les ministères, de l'IA à la défense, en passant par la sécurité (aucune version française n'est disponible).		

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
		plaintes concernant des demandes d'information.					
PAYS-BAS	General Intelligence and Security Service (GISS) - Publication de divers renseignements, y compris des rapports annuels, des extraits audio, des vidéos et des Q et R - Intelligence and Security Services Review Committee (CTIVD) - Principal organisme de surveillance externe des services de renseignement et de sécurité. - Surveillance des activités du GISS et du Defence Intelligence and Security Service (DISS). - A accès à tous les renseignements pertinents requis pour une enquête et peut écouter les témoignages faits sous serment et faire appel à des experts. - Agit à titre de comité consultatif interne sur les plaintes – conseille les ministres sur les décisions relatives aux plaintes contre le GISS et le DISS. Les ministres sont libres de prendre leurs propres décisions, mais les conseils du CTIVD doivent être publiés.	Intelligence and Security Services Review Committee (CTIVD) - Rapports annuels - Rapports d'examen des services de surveillance du CTIVD - Procédure de traitement des plaintes, protocole de traitement des plaintes et décisions rendues dans le cadre d'audiences portant sur les éventuelles fautes commises par les organismes de renseignement. - Mène des activités de surveillance systémiques au moyen d'inspections aléatoires afin d'obtenir une vue d'ensemble des principales activités des services de renseignement. - Peut exercer son autorité à l'égard de la CT Infobox. - Comités parlementaires de surveillance (ne mènent pas d'enquêtes et ne produisent pas de rapports) - Committee on the Intelligence and Security Services (ISS)	<i>Government Information (Public Access) Act</i> ou <i>Wet Openbaarheid van Bestuur (Wob)</i> (1980) La loi néerlandaise sur l'accès public fait la distinction entre la divulgation <i>passive</i> et <i>proactive</i> d'information. Toutefois, contrairement à la divulgation passive, la divulgation proactive n'est pas exécutoire. La loi sur l'accès public prévoit 11 exemptions. On ne s'attend pas à ce que les autorités du Parlement et de la magistrature et certaines autorités de l'exécutif, comme l'Intelligence and Security Services Review Committee (CTIVD) divulguent des renseignements sur demande. De même, les renseignements traités par les services de renseignement ou à l'appui de ceux-ci sont exemptés.	Politique de déclassification - Selon la réglementation, la classification est temporaire, à moins qu'il n'y ait des exemptions spéciales. Par conséquent, la durée de la classification est fixée à 10 ans ou à un moment précis, selon la nature délicate du document. - Les documents classifiés pendant plus de 10 ans peuvent faire l'objet d'un examen après 20 ans.	Publications du CTVID - En ce qui concerne la fonction de surveillance du CTVID, le comité a publié des rapports sur le secret et la transparence, les enquêtes sur les activités des organismes de SNR, l'échange de données et la coopération, ainsi que les enquêtes en cours. - Aperçu du processus de traitement des plaintes contre les organismes de SNR. - Publication du GISS - Rapports sur l'espionnage, y compris des conseils pour les entreprises afin qu'elles enquêtent sur les activités d'espionnage et des moyens de limiter les risques. - Information sur le terrorisme accessible au public, activités de l'organisme et nouvelles sur les activités terroristes. - Renseignements sur l'islam radical et l'extrémisme, y compris différents types de mouvements fondamentalistes et extrémistes et un rapport sur le salafisme aux Pays-Bas. - National Coordinator for Counterterrorism and Security (NCTV)	Instituts de recherche en matière de SNR du gouvernement fédéral : - Scientific Council for Government Policy - Netherlands Bureau for Economic Policy Analysis Recherches propres à la SNR : - International Centre for Counter-Terrorism Instituts de recherche sur les politiques dignes de mention ayant comme domaine d'intérêt la SN : - Clingendael, Netherlands Institute of International Relations - Hague Institute for Global Justice	Groupes nationaux : - Bits Of Freedom - Cordaid - Justice and Peace Netherlands - Netherlands Institute for Human Rights - Netherlands Network for Human Rights Research

PAYS	INITIATIVES ACTUELLES RELATIVES À LA TRANSPARENCE DE LA SNR ¹	ORGANISMES DE SURVEILLANCE ET D'EXAMEN	LOIS SUR L'ACCÈS À L'INFORMATION	SYSTÈME ET POLITIQUE DE DÉCLASSIFICATION	DONNÉES TIRÉES DE RAPPORTS PUBLICS ET DE SITES WEB ²	INSTITUTS DE RECHERCHE SUR LES POLITIQUES EN MATIÈRE DE SNR ³	GROUPES DE DÉFENSE EN MATIÈRE DE SNR ⁴
	Counter-Terrorism Infobox (CT Infobox) Groupe de coopération composé de représentants de la sécurité nationale, du renseignement et d'un certain nombre d'autres organismes mis sur pied après les attentats terroristes de 2004 à Madrid pour échanger de l'information afin de lutter contre le terrorisme et la radicalisation et de permettre la prise de mesures appropriées.	Committee) – surveille le GISS. - Committee on Defence – composé de tous les experts en la matière de tous les partis politiques de la Deuxième Chambre, traite des questions relevant du mandat du ministre de l'Intérieur et des Relations au sein du Royaume, y compris le GISS.	Il n'y a pas de commissaire à l'information officiel, mais il existe une autorité néerlandaise de protection des données (semblable au commissaire à la protection de la vie privée). Les appels concernant les décisions relatives aux demandes d'accès public d'un organisme gouvernemental sont présentés directement à l'organisme gouvernemental, ce qui comprend le processus d'appel supérieur.		- Rapports d'évaluation des menaces à la cybersécurité et des menaces terroristes . - Information sur les différents types d'infrastructures essentielles aux Pays-Bas.		

Annexe 5.2 : Politiques relatives à la transparence de la sécurité nationale et du renseignement dans certaines organisations gouvernementales à l'échelle internationale

IMPORTANT : LA PRÉSENTE ANNEXE ET LES RENSEIGNEMENTS QU'ELLE CONTIENT ONT ÉTÉ VÉRIFIÉS POUR LA DERNIÈRE FOIS LE 20 OCTOBRE 2020 ET SONT SUSCEPTIBLES DE CHANGER. DANS LE CADRE DU PRÉSENT RAPPORT, CES RENSEIGNEMENTS NE SERONT PAS MIS À JOUR. DE PLUS, CERTAINES INFORMATIONS NE SONT PAS DISPONIBLES EN FRANÇAIS.

Les tableaux ci-dessous fournissent des renseignements sur les politiques et les initiatives relatives à la transparence de la sécurité nationale et du renseignement (SNR) dans quatre organisations gouvernementales à l'échelle internationale. Ces organisations ont des répercussions directes ou indirectes sur le Canada en matière de SNR.

Tous les renseignements fournis ci-dessous sont fondés sur l'information accessible au public et ne constituent pas une liste exhaustive de toutes les données et de tous les renseignements disponibles.

TABEAU 5.2.1 : UNION EUROPÉENNE

UNION EUROPÉENNE
<i>Règlement général sur la protection des données (RGPD)</i> • Le RGPD a été ratifié par le Parlement européen en 2016 et est entré en vigueur le 25 mai 2018. Il a eu et continue d'avoir une incidence importante sur la réglementation du marché mondial des données. • Le cadre s'appuie sur la directive de 1998 sur la protection des données. Il vise à améliorer et à harmoniser la réglementation et les pratiques organisationnelles en matière de protection des renseignements personnels. Le RGPD fournit également des directives sur la façon dont les entreprises devraient traiter les renseignements de leurs clients. Chaque pays européen au sein de l'UE peut adapter le RGPD en fonction de ses besoins contextuels. • Les données à caractère personnel peuvent comprendre des renseignements sur le nom et l'emplacement d'une personne, les adresses IP et les témoins, ainsi que le nom d'utilisateur en ligne. Il y a aussi des catégories particulières de données à caractère personnel qui bénéficient d'une meilleure protection. Ces catégories particulières peuvent comprendre des données génétiques et biométriques, des renseignements concernant la santé, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses et l'orientation sexuelle. • Le RGPD comprend des sections sur les principes (articles 5-11) ainsi que sur les droits des personnes concernées (articles 12-23). • Les principes fondamentaux du RGPD comprennent les suivants : « <i>licéité, loyauté, transparence</i> », « <i>intégrité et confidentialité</i> » et « <i>responsabilité</i> ». • Les droits des personnes comprennent le droit à l'information, le droit d'accès, le droit à la portabilité des données et les droits liés aux décisions automatisées et au profilage.

- Bien que le RGPD ne définisse pas explicitement la transparence, les articles 12 à 14 énoncent des exigences précises pour les responsables du traitement et les sous-traitants :
 - [Article 12](#) : Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée (fournit des règles générales sur la transparence).
 - [Article 13](#) : Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée (communications concises, transparentes et intelligibles avec les personnes concernées au sujet de leurs droits).
 - [Article 14](#) : Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée (communications concises, transparentes et intelligibles avec la personne concernée en cas d'atteinte à la protection des données).
- Restrictions : Le degré d'obligation de fournir des renseignements aux personnes concernées, décrit aux articles 13 et 14, peut être réduit en fonction des mesures nationales prises par chaque pays, conformément à leurs libertés et droits fondamentaux respectifs. L'[article 23](#) énumère les restrictions du RGPD, y compris la protection de la sécurité nationale, de la défense et de la sécurité publique.
- Répercussions du RGPD sur le Canada :
 - Le RGPD s'applique à toutes les organisations qui stockent ou traitent les données à caractère personnel des citoyens de l'UE, quel que soit leur niveau de protection de la vie privée. Le RGPD exige que ces entreprises et organisations prennent des mesures pour se conformer au RGPD, comme la création de postes de délégué à la protection des données, la mise en œuvre des principes de la protection de la vie privée dès la conception des nouveaux processus et des nouvelles technologies et la tenue à jour des dossiers de traitement des données.
 - De lourdes sanctions financières et sanctions touchant la réputation sont imposées en cas de non-conformité ou d'inaction.
- Décision automatisée et profilage :
 - L'[article 22](#) comprend des dispositions sur le profilage et les systèmes de décision automatisée fondés sur l'intelligence artificielle (IA). Il vise à veiller à ce que la technologie de l'IA ne puisse pas être utilisée comme seul décideur dans les cas qui ont une incidence sur les droits et les libertés des personnes.
- Données biométriques
 - Le RGPD classe les données biométriques en deux catégories, selon les caractéristiques physiques et les caractéristiques comportementales.
 - Comme il a été mentionné précédemment, les données biométriques utilisées pour identifier une personne sont classées comme des « données sensibles » dans le RGPD. Ainsi, l'utilisation des données biométriques des citoyens de l'UE est restreinte et assujettie à la réglementation.
 - Les organisations qui recueillent et utilisent des données biométriques devront entreprendre des évaluations des facteurs relatifs à la vie privée (EFVP).
 - En ce qui concerne la reconnaissance faciale, le vice-président exécutif de la Commission européenne pour les affaires numériques a déclaré que la reconnaissance faciale était

contraire au RGPD parce que la technologie ne répondait pas aux exigences relatives au consentement de l'utilisateur.

Accord entre l'UE et le Canada sur les dossiers passagers (DP)

- Les dossiers passagers font l'objet d'un accord relatif à l'échange de données entre l'UE et le Canada en ce qui a trait « [à la prévention ou à la détection d'infractions de terrorisme ou de crimes transnationaux graves, à des enquêtes ou à des poursuites relativement à celles-ci](#) ».
- Les DP contiennent des données sur les détails du vol qui sont stockées dans la base de données des transporteurs aériens, ce qui comprend l'itinéraire du passager, ses coordonnées, les modes de paiement et les invités.
- La Cour de justice de l'Union européenne (CJUE) a rejeté le projet d'accord sur les dossiers passagers (DP) avec le Canada. Selon l'[avis](#) de la CJUE, l'accord entre l'UE et le Canada sur les DP n'est pas compatible avec la Charte des droits fondamentaux de l'UE dans sa forme actuelle. Les droits garantis par la Charte ne sont pas absolus. Un accord sur les DP peut être établi pour permettre la communication et la conservation des données afin de protéger la sécurité nationale et la sécurité publique, malgré une atteinte grave à la vie privée et à la protection des données à caractère personnel. Toutefois, une telle atteinte devrait reposer sur des règles claires et précises régissant sa portée et son application (section VI, A.39), être strictement nécessaire (section VI, B.41) et proportionnelle (section VII, C.54).
- À l'heure actuelle, l'UE a conclu des accords sur les DP avec les [États-Unis](#) (conservation des données des DP pendant un maximum de 15 ans) et l'[Australie](#) (conservation des données des DP pendant un maximum de cinq ans et demi). L'UE a également adopté son propre cadre interne en matière de DP qui permet la conservation de ces données pendant un maximum de cinq ans.

Coopération structurée permanente (PESCO) en matière de sécurité et de défense

- Dans le cadre de la politique relative à la sécurité et à la défense de l'UE, la Stratégie globale pour la politique étrangère et de sécurité de l'UE (SGUE) a permis de constituer la Coopération structurée permanente (PESCO). Il s'agit d'un cadre fondé sur un traité conclu entre 25 États membres de l'UE qui vise à promouvoir une coopération plus étroite entre les États membres et à accroître leurs investissements pour faire face aux menaces à la sécurité et renforcer les capacités de sécurité et de défense.
- Plus précisément, la PESCO se concentre sur trois domaines :
 - approfondissement de la collaboration : la collaboration entre les États membres participants est officielle et contraignante et n'est plus ponctuelle;
 - la majorité des projets de la PESCO sont liés aux besoins opérationnels;
 - la PESCO peut être utilisée de concert avec d'autres outils pour cerner les lacunes et les possibilités de nouvelles initiatives. Elle vise à éviter le double emploi et à rationaliser les ressources.
- Voici les États membres participants : Autriche, Belgique, Bulgarie, Croatie, Chypre, République tchèque, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Irlande, Italie,

Lettonie, Lituanie, Luxembourg, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Espagne et Suède.

Examen annuel coordonné en matière de défense (CARD)

- En 2016, la Stratégie globale pour la politique étrangère et de sécurité de l'UE (SGUE) a permis de créer l'examen annuel coordonné en matière de défense (CARD) afin de favoriser le renforcement des capacités par l'entremise d'analyses et d'évaluations des plans et des capacités de l'UE en matière de défense et de sécurité.
- Son objectif est « [de développer \[sur une base volontaire\] une méthode plus structurée pour assurer la disponibilité des capacités \[...\] nécessaires \[...\], fondée sur une transparence, une visibilité politique et un engagement accrus de la part des États membres](#) » (traduction). L'examen vise à renforcer la coopération entre les États membres et à assurer l'utilisation optimale des dépenses en matière de défense en collaboration avec la PESCO.

RESSOURCES :

- [Règlement général sur la protection des données](#)
- [DP : Avis 1/15 de la Cour](#)
- [Fiche d'information sur la PESCO](#)
- [Coopération structurée permanente \(PESCO\) en matière de défense](#)
- [Examen annuel coordonné en matière de défense \(CARD\)](#)

TABLEAU 5.2.2 : PAYS DU GROUPE DES CINQ

PAYS DU GROUPE DES CINQ
• Alliance multilatérale du renseignement entre cinq pays anglophones, soit l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis. Il s'agit d'un accord conclu entre les cinq pays pour communiquer par défaut les renseignements électromagnétiques qu'ils recueillent. • Il y a très peu d'information sur le cadre juridique qui sous-tend l'échange de renseignements et la façon dont celui-ci se fait. Les plus récents renseignements accessibles au public remontent à 1955. • En juillet 2017, Privacy International et la Media Freedom & Information Access Clinic (École de droit de Yale) ont intenté une poursuite contre la National Security Agency, l'Office of the Director of National Intelligence, le département d'État et la National Archives and Records Administration. La poursuite visait à obtenir des renseignements et un accès aux dossiers liés aux activités du Groupe des cinq. En réponse, la NSA et le département d'État ont communiqué des renseignements limités. • Divulgations : – 1959-61 Appendices to the United Kingdom-United States Communication Intelligence (UKUSA) Agreement – 1961 General Security Agreement between the Government of the United States and the Government of the United Kingdom (accord général de sécurité)

- [1998 Agreement to Extend the 1966 Agreement between the Government of Australia and the Government of the United States of America relating to the Establishment of a Joint Defence Facility at Pine Gap](#) (accord de Pine Gap)

Remarque : L'information fournie ci-dessus est fondée sur des sources de renseignements secondaires.

Five Eyes Intelligence Oversight and Review Council (FIORC)

- La portée et l'objet du FIORC, les réunions, les lignes directrices opérationnelles et les éléments administratifs sont énoncés dans la charte.
- Le FIORC est composé d'organisations non politiques de renseignement, de surveillance, d'examen et de sécurité des pays du Groupe des cinq :
 - Office of the Inspector-General of Intelligence and Security de l'Australie
 - Office de surveillance des activités en matière de sécurité nationale et de renseignement du Canada
 - Commissariat au renseignement du Canada
 - Commissioner of Intelligence Warrants et Office of the Inspector-General of Intelligence and Security de la Nouvelle-Zélande
 - Investigatory Powers Commissioner's Office du Royaume-Uni
 - Office of the Inspector General of the Intelligence Community des États-Unis
- Le conseil se réunit en personne pour discuter de préoccupations et d'intérêts mutuels, comparer les pratiques exemplaires en ce qui concerne les méthodes d'examen et de surveillance, examiner de nouvelles possibilités de coopération pour les examens et l'échange d'information et encourager la transparence afin d'accroître la confiance du public.
- Les résumés des réunions annuelles sont accessibles au public.

RESSOURCES :

- [Article de Lawfareblog.com : « Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements »](#)
- [Article de Justsecurity.org : « The “Backdoor Search Loophole” Isn't Our Only Problem: The Dangers of Global Information Sharing »](#)
- ODNI – [Five Eyes Intelligence Oversight and Review Council \(FIORC\)](#)
- [Charte du FIORC \(PDF\)](#)

TABEAU 5.2.3 : ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE)
Principes de l'OCDE sur l'intelligence artificielle (IA) • En 2018, le Comité de la politique de l'économie numérique de l'OCDE a créé un Groupe d'experts sur l'IA (GEIA) chargé de fournir des directives sur les principes d'établissement de la portée de l'intégration de l'IA dans la société et l'économie. Le groupe comprenait des experts des pays membres de l'OCDE. Le Canada comptait sur un représentant de l'Institut canadien de recherches avancées (ICRA) au sein du GEIA.

• Les principes servent de normes internationales sur l'IA, « visant à assurer la conception de systèmes d'IA robustes, sûrs, équitables et dignes de confiance ». Ils ont été adoptés le 21 mai 2019. En tout, 42 pays ont adopté les principes, dont le Canada. • La Commission européenne appuie les principes. • Répercussions au Canada – Stratégie pancanadienne en matière d'intelligence artificielle : En 2017, le gouvernement du Canada a prévu 125 millions de dollars pour la Stratégie pancanadienne en matière d'intelligence artificielle et a nommé un institut de recherche sans but lucratif, l'ICRA, pour élaborer et diriger une stratégie nationale en matière d'IA. L'ICRA collabore avec trois des instituts nationaux d'IA du Canada (Institut Vector, Mila, Amii), des universités, des hôpitaux et d'autres organisations. Le programme IA et société de l'ICRA constitue un pilier clé de la Stratégie pancanadienne en matière d'IA. Il vise à mettre en relation des experts de divers secteurs (universités, industrie, droit, éthique, soins de santé, gouvernement, etc.) afin de mener des discussions approfondies sur les enjeux et les défis actuels. – Groupe international d'experts en intelligence artificielle Canada-France – En juillet 2018, les gouvernements du Canada et de la France ont annoncé qu'ils travailleraient à la création d'un Groupe international d'experts en IA. L'objectif est de créer un point de référence mondial pour l'échange de recherches sur les questions et les pratiques exemplaires liées à l'IA. L'objectif est de « promouvoir une vision de l'intelligence artificielle centrée sur l'humain ».	
RESSOURCES :	• Principes de l'OCDE sur l'IA • L'intelligence artificielle dans la société • Recommandation du Conseil sur l'intelligence artificielle • Stratégie pancanadienne en matière d'intelligence artificielle de l'ICRA • Rapport sur les stratégies nationales et régionales en matière d'IA de l'ICRA • Mandat pour le Groupe international d'experts en intelligence artificielle • Communiqué de presse

TABEAU 5.2.4 : ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD (OTAN)
• L'OTAN est une alliance militaire intergouvernementale entre 30 pays. Le Canada est un membre fondateur de l'OTAN depuis 1949. Il compte actuellement sur une délégation conjointe à l'OTAN, composée de représentants des sections politiques, militaires et de soutien à la défense. • Transparence financière – L'OTAN est financée par ses pays membres et doit donc rendre des comptes aux gouvernements de ces derniers.

- L'OTAN publie le budget civil total annuel (coûts administratifs pour le siège social de l'OTAN) et le budget militaire total (coûts de la structure de commandement intégrée), le budget du Programme OTAN d'investissement au service de la sécurité (capacités militaires) et le compendium annuel des données financières et économiques et des données sur les effectifs de tous les pays membres.

Unified Vision

- Chaque année, l'OTAN entreprend un essai majeur géré par le Commandement allié Transformation et le siège de l'OTAN dans le contexte du renseignement, de la surveillance et de la reconnaissance interarmées (JISR) de l'OTAN. L'essai JISR offre aux décideurs et aux exploitants clés une meilleure connaissance de la situation sur le terrain afin de faciliter la prise de décisions éclairées en temps opportun. Les alliés partagent le fardeau de la collecte, de l'analyse et de la communication de l'information. L'essai JISR permet de réunir des données sur la surveillance et la reconnaissance recueillies dans le cadre de divers projets.
- Par exemple, l'essai Unified Vision 2016 visait à améliorer la capacité de l'Alliance d'échanger et de traiter du renseignement complexe. Selon l'organisation, l'essai a permis d'améliorer la façon dont l'Alliance réagit aux opérations multinationales et à la guerre hybride et tire parti de la nouvelle capacité de surveillance au sol de l'Alliance.

Politique de l'OTAN pour le développement de l'intégrité

- La politique de l'OTAN pour le développement de l'intégrité a été approuvée au Sommet de l'OTAN de 2016.
- Le plan d'action et la politique pour le développement de l'intégrité aident les pays membres à favoriser la bonne gouvernance et à mettre en œuvre les principes d'intégrité, de transparence et de redevabilité dans la politique de l'OTAN. La politique pour le développement de l'intégrité vise à prévenir, grâce à de bonnes pratiques de gouvernance, l'insécurité, l'extrémisme et le terrorisme auxquels sont confrontés les partenaires et d'autres pays.
- La politique de l'OTAN pour le développement de l'intégrité contribue aux trois principales tâches de l'OTAN, soit la défense collective, la gestion de crise et la sécurité coopérative.
- La politique de l'OTAN pour le développement de l'intégrité aide les Nations Unies, la Banque mondiale et l'Union européenne à favoriser de bonnes pratiques de gouvernance et est appuyée par des experts de tous les secteurs.

RESSOURCES :

- [Organisation du Traité de l'Atlantique Nord \(OTAN\)](#)
- [Transparence et obligation de rendre compte](#)
- [Le Canada et l'Organisation du Traité de l'Atlantique Nord](#)
- [Unified Vision 2016](#)
- [Unified Vision 2018](#)
- [Politique OTAN pour le développement de l'intégrité](#)
- [Développement de l'intégrité](#)